Polytopes in the Fiat-Shamir with Aborts Paradigm

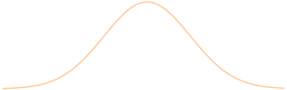
Crypto 2024

Henry Bambury [1,2], **Hugo Beguinet** [1,3], Thomas Ricosset [3], Éric Sageloli [1,3,4]

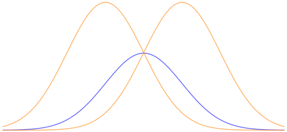
[1]DIENS, Inria Team CASCADE [2]DGA [3]Thales [4]École polytechnique

21st of August 2024

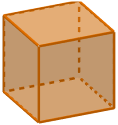
Rejection Sampling: A Brief History of Distributions



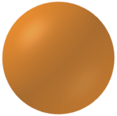
[Lyu12]



[DDLL13, CCD^{+}23]

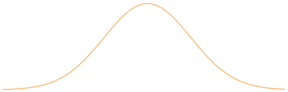


[Lyu09, DKL^{+}21]

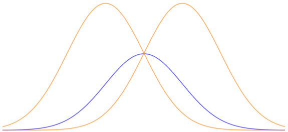


[CCD^{+}23]

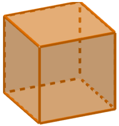
Rejection Sampling: A Brief History of Distributions



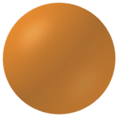
[Lyu12]



[DDLL13, CCD+23]

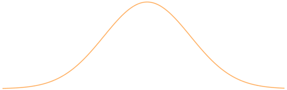


[Lyu09, DKL+21]

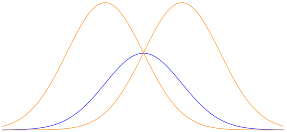


[CCD+23]

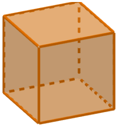
Rejection Sampling: A Brief History of Distributions



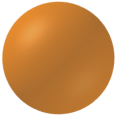
[Lyu12]



[DDLL13, CCD^{+}23]



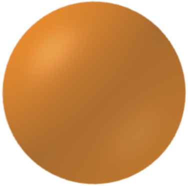
[Lyu09, DKL^{+}21]



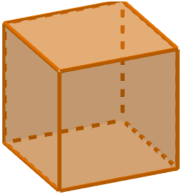
[CCD^{+}23]

Focus on uniform distributions.

Lattice-based FSwA Signatures: Haetae and Dilithium



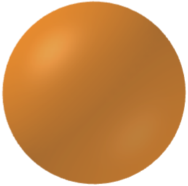
$\longleftrightarrow$

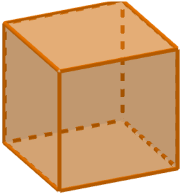


Signature size	✔ ✔
Verification key	✔
Sampler	✘

Signature size	✘ ✘
Verification key	✔
Sampler	✔✔

Lattice-based FSwA Signatures: Haetae and Dilithium





Signature size	✔ ✔	Signature size	✘ ✘
Verification key	✔	Verification key	✔
Sampler	✘	Sampler	✔✔

Is there a shape embracing the best of both?

Outline

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

III. Choosing a Polytope $\mathcal{H}$

IV. In Application

Outline

Fiat-Shamir (with Aborts) on Lattice Assumptions.

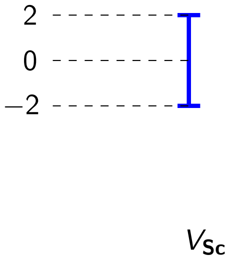
Notation: $V_{\mathbf{x}}$ the support of the distribution from which $\mathbf{x}$ is taken.

Signer		**Verifier**
$\mathsf{sk} = \mathbf{s}, \mu$		$\mathsf{vk} = \mathbf{As}$
$\mathbf{y} \leftarrow \mathcal{C}$		
$\mathbf{w} = \mathbf{Ay}$		
$c = \mathtt{H}(\mathbf{w}, \mu)$		
$\mathbf{z} = \mathbf{y} + \mathbf{S}c$		
$\boxed{\text{if } \mathbf{z} \in V_{\mathbf{z}}}$	$\xrightarrow{c, \mathbf{z}}$	$c == \mathtt{H}(\mathbf{Az} - \mathsf{vk} \cdot c)$

Goal: obtaining the shape of $V_{\mathbf{z}}$.

Rejection Sampling: Motivation

1D Example:

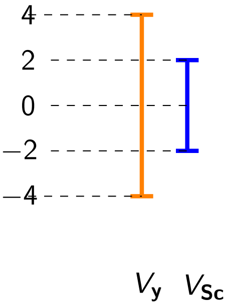


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

Rejection Sampling: Motivation

1D Example:

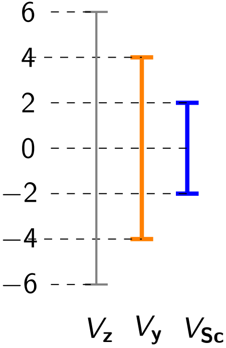


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

Rejection Sampling: Motivation

1D Example:

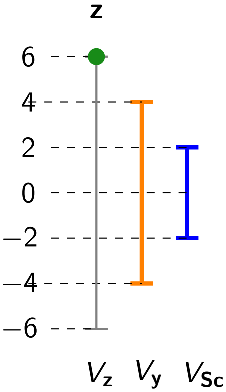


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

Rejection Sampling: Motivation

1D Example:

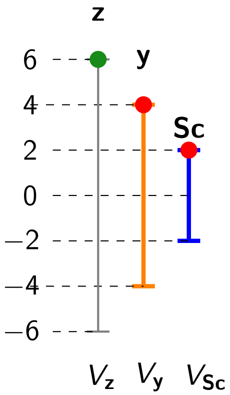


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

Rejection Sampling: Motivation

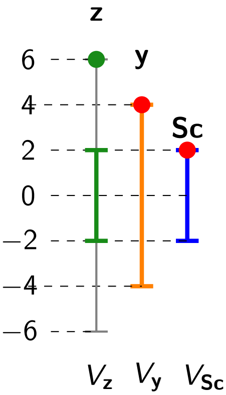
1D Example:



Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

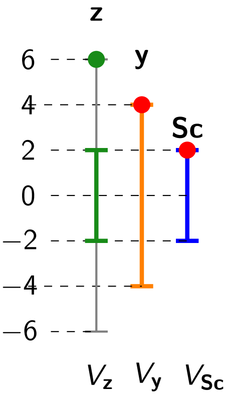
1D Example:



Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

1D Example:

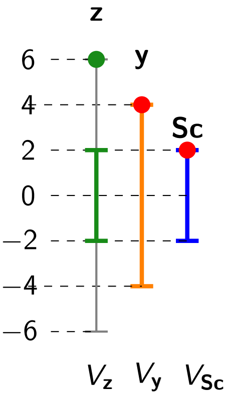


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

$\mathbf{z}$ should reveal **no information** on $\mathbf{y}$ and $\mathbf{Sc}$.

1D Example:

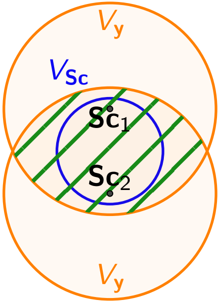


Remark:

- $V_{\mathbf{z}}$, $V_{\mathbf{y}}$ and $V_{\mathbf{Sc}}$ are all public.
- $\mathbf{z} = \mathbf{y} + \mathbf{Sc}$

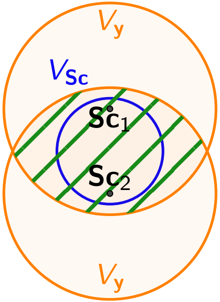
z should reveal **no information** on **y** and **Sc**.

How should $V_{\mathbf{z}}$ be?



- Possible $\mathbf{z}$ are in the green area.

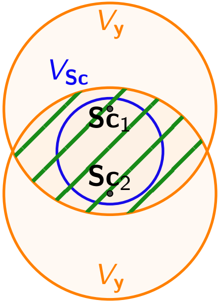
From V_z to ...



- Possible z are in the green area.
- z avoids information leakage if and only if:

$$V_z \subseteq \bigcap_{c \in V_{Sc}} (V_y + c).$$

From $V_{\mathbf{z}}$ to ...



- Possible $\mathbf{z}$ are in the green area.
- $\mathbf{z}$ avoids information leakage if and only if:

$$V_{\mathbf{z}} \subseteq \bigcap_{\mathbf{c} \in V_{\mathbf{Sc}}} (V_{\mathbf{y}} + \mathbf{c}).$$

The bigger $V_{\mathbf{z}}$ is, the lower the signature size becomes (at equal rejection rate):

$$V_{\mathbf{z}} = \bigcap_{\mathbf{c} \in V_{\mathbf{Sc}}} (V_{\mathbf{y}} + \mathbf{c}).$$

Roadmap

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

III. Choosing a Polytope $\mathcal{H}$

IV. In Application

Polytope intersection: a useful tool

Theorem ($\mathcal{P}$-ception: Intersection of polytopes)

Let $\mathcal{P}$ be a symmetric inscriptible and circumscriptible polytope. Let $r, R \in \mathbb{R}_{>0}$ such that $R > r$ and $\mathcal{P}_r := r \cdot \mathcal{P}$. Then:

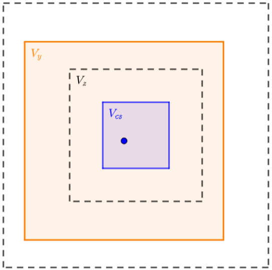
$$\bigcap_{\mathbf{c} \in \mathcal{P}_r} \mathcal{P}_R + \mathbf{c} = \mathcal{P}_{R-r}.$$

Polytope intersection: a useful tool

Theorem ($\mathcal{P}$-ception: Intersection of polytopes)

Let $\mathcal{P}$ be a symmetric inscriptible and circumscriptible polytope. Let $r, R \in \mathbb{R}_{>0}$ such that $R > r$ and $\mathcal{P}_r := r \cdot \mathcal{P}$. Then:

$$\bigcap_{\mathbf{c} \in \mathcal{P}_r} \mathcal{P}_R + \mathbf{c} = \mathcal{P}_{R-r}.$$

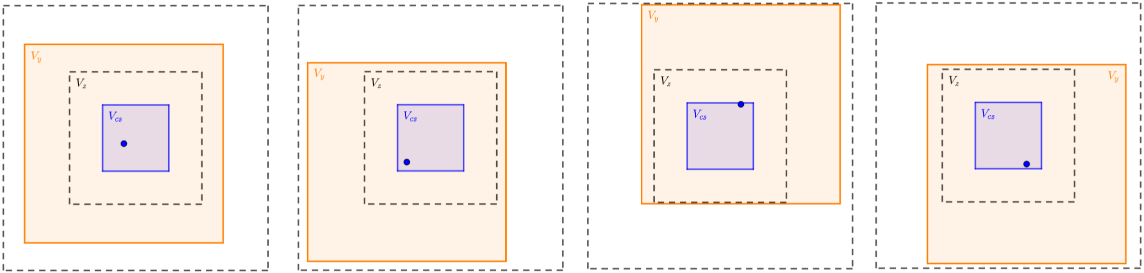


Polytope intersection: a useful tool

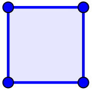
Theorem ($\mathcal{P}$-ception: Intersection of polytopes)

Let $\mathcal{P}$ be a symmetric inscriptible and circumscriptible polytope. Let $r, R \in \mathbb{R}_{>0}$ such that $R > r$ and $\mathcal{P}_r := r \cdot \mathcal{P}$. Then:

$$\bigcap_{\mathbf{c} \in \mathcal{P}_r} \mathcal{P}_R + \mathbf{c} = \mathcal{P}_{R-r}.$$

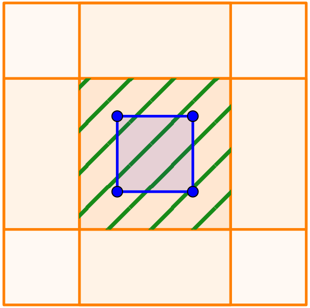


$\mathcal{P}$-ception case 1: Restriction to integral points



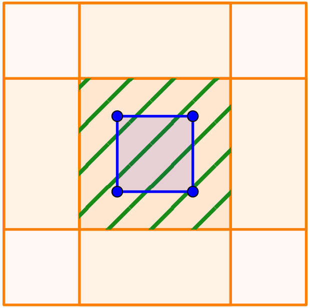
- Same result using only the vertices of $V_{\mathbf{Sc}}$.

$\mathcal{P}$-ception case 1: Restriction to integral points



- Same result using only the vertices of $V_{\mathbf{Sc}}$.
- Yes and?

$\mathcal{P}$-ception case 1: Restriction to integral points



- Same result using only the vertices of $V_{\mathbf{Sc}}$.
- Yes and?

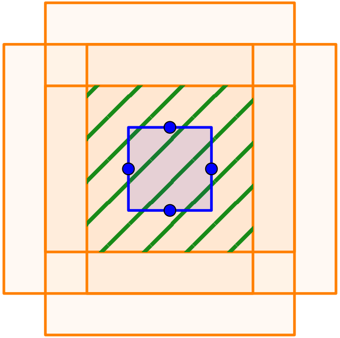
Wait, is it not better to work directly on integers?

Theorem ($\mathcal{P}$-ception: Generalization 1)

If $\mathcal{P}_r$ is an integral polytope, then:

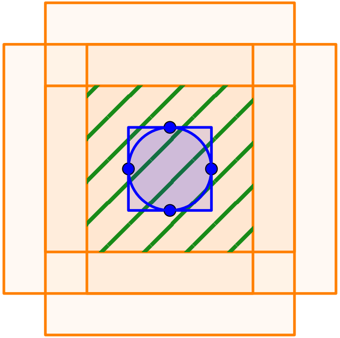
$$\bigcap_{\mathbf{c} \in \mathcal{P}_r \cap \mathbb{Z}^n} \mathcal{P}_R \cap \mathbb{Z}^n + \mathbf{c} = \mathcal{P}_{R-r} \cap \mathbb{Z}^n.$$

$\mathcal{P}$-ception case 2: Different shape for $V_{\mathbf{Sc}}$



- Same result using only one point on each facet of $V_{\mathbf{Sc}}$.
- Again, yes and?

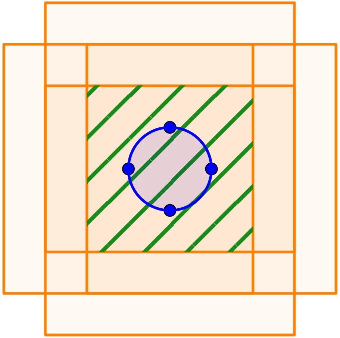
$\mathcal{P}$-ception case 2: Different shape for $V_{\mathbf{Sc}}$



- Same result using only one point on each facet of $V_{\mathbf{Sc}}$.
- Again, yes and?

In practice $V_{\mathbf{Sc}}$ is not a square but a sphere...

$\mathcal{P}$-ception case 2: Different shape for $V_{\mathbf{Sc}}$



- Same result using only one point on each facet of $V_{\mathbf{Sc}}$.
- Again, yes and?

> In practice $V_{\mathbf{Sc}}$ is not a square but a sphere...

Theorem ($\mathcal{P}$-ception: Generalization 2)

If $\mathcal{S}$ is the inscribed sphere of $\mathcal{P}_r$, then:

$$\bigcap_{\boxed{\mathbf{c} \in \mathcal{S}}} \mathcal{P}_R + \mathbf{c} = \mathcal{P}_{R-r}.$$

Roadmap

Polytope Choice: Cutting a Rare Gem

What we want for $\mathcal{P}$:

- Verifies simple assumptions
- Integral vertices
- Efficiently samplable
- Small ratio

Definition (Ratio ρ)

Given the circumradius R of $\mathcal{P}$ and its in radius r:

$$\rho := \frac{R}{r}$$

Polytope Choice: Cutting a Rare Gem

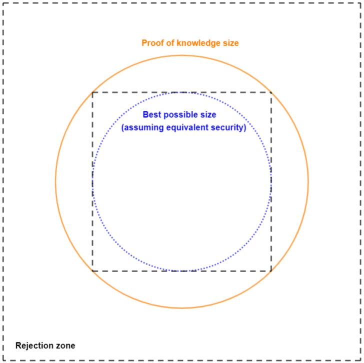
What we want for $\mathcal{P}$:

- Verifies simple assumptions
- Integral vertices
- Efficiently samplable
- Small ratio

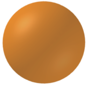
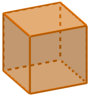
Definition (Ratio ρ)

Given the circumradius R of $\mathcal{P}$ and its in radius r:

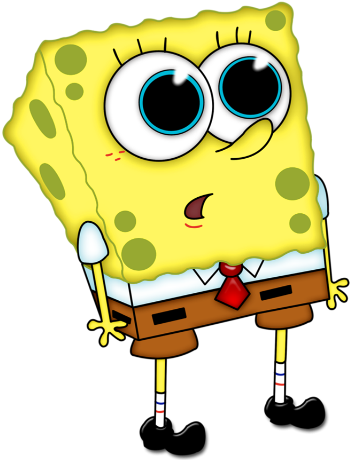
$$\rho := \frac{R}{r}$$



Where Should It Be?

	Signature	Verification Key	Sampling Method	Bimodal	Ratio
	✔✔	✔	✘✘	✔	1
					
	✘✘	✔	✔✔	✘	$\sqrt{n}$

Interlude: High-dimensional Balls



The Hypercube:

$$\mathcal{B}_\infty(R) = \{\mathbf{x} \in \mathbb{R}^n : \forall i, |x_i| \le R\}.$$

- Volume: $(2R)^n$.
- Radius ratio: $\sqrt{n}$.
- Mass concentrates: at the corners.

Interlude: High-dimensional Balls

The Cross-polytope[1]:

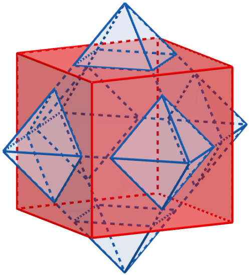
$$\mathcal{B}_1(R\sqrt{n}) = \{\mathbf{x} \in \mathbb{R}^n : \sum |x_i| \leq R\sqrt{n}\}.$$

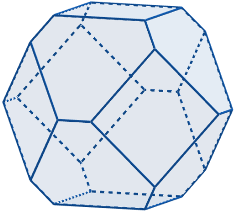
- Volume: $\frac{(2\sqrt{n}R)^n}{n!}$.
- Radius ratio: $\sqrt{n}$.
- Mass concentrates: at the center.

[1] also called Hyperoctahedron, Orthoplex, or Cocube.

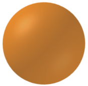
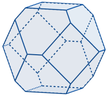
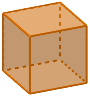
The Polytope $\mathcal{H}$

$$\mathcal{H}_r^n = \mathcal{B}_\infty^n(r) \cap \mathcal{B}_1^n(r\sqrt{n})$$





Recap Table

	Signature	Verification Key	Sampling Method	Bimodal	Ratio
	✔✔	✔	✘✘	✔	1
			✔	✘	$\sqrt[4]{n}$
	✘✘	✔	✔✔	✘	$\sqrt{n}$

Roadmap

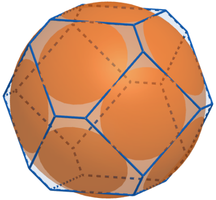
I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

III. Choosing a Polytope $\mathcal{H}$

IV. In Application

Reject More for Better Performances



$$\mathcal{C}^n_{\theta,r} = \mathcal{H}^n_r \cap \mathcal{B}_2(\theta \cdot r) \text{ with } \theta \approx 1.5$$

- Low rejection rate.
- Ratio: from $n^{1/4}$ to θ.
- θ decreases as (n, r) grows.
- **Warning**: not a polytope anymore.

A new Fiat-Shamir with Aborts Signature Scheme: PATRONUS

- **Signature sizes:** (in bytes)

Security target (bits)	120	180	260
HAETAE	1,463	2,337	2,908
PATRONUS (this work)	**2,070**	**2,575**	**3,721**
DILITHIUM	2,420	3,293	4,595

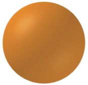
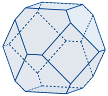
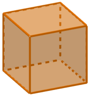
- **Verification key sizes:** (in bytes)

HAETAE	992	1,472	2,080
PATRONUS (this work)	**832**	**1,152**	**1,632**
DILITHIUM	1,312	1,952	2,592

- **Rejection rate:**

HAETAE	6	5	6
PATRONUS (this work)	**3**	**4.250**	**3**
DILITHIUM	4.250	5.1	3.850

Recap Table

	Signature	Verification Key	Sampling Method	Bimodal	Ratio
	✔✔	✔	✘✘	✔	1
	✔	✔✔	✔	✘	$\sqrt[4]{n} \to 1.5$
	✘✘	✔	✔✔	✘	$\sqrt{n}$

Takeaway

What you should remember:

- We propose a new framework for rejection sampling in polytopes.
- This allows for rigorous analysis of perfect rejection in Fiat-Shamir.
- Our polytope $\mathcal{H}$ uses L_1 and L_∞ balls to approach an optimal L_2 ball.
- It is easy to sample from $\mathcal{H}_\mathbb{Z}$.
- This leads to the signature scheme PATRONUS , an interesting tradeoff between DILITHIUM and HAETAE.

Roadmap

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

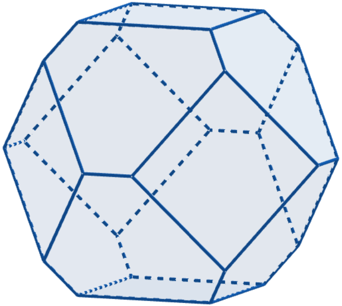
III. Choosing a Polytope $\mathcal{H}$

IV. In Application

V. Bonus: Open Questions and Perspectives

The End: Questions?

Thank you for listening!



Article: eprint.iacr.org/2024/411

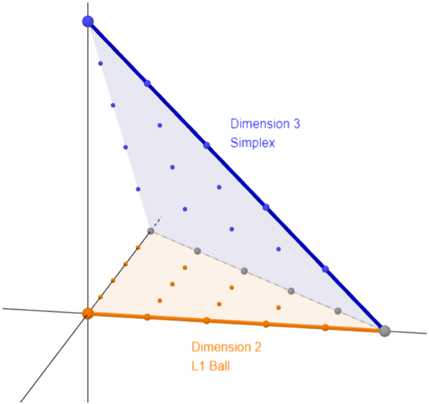
A useful projection

The following sets are isomorphic via a simple projection:

$$\mathcal{S}^{n+1}_{1,\mathbb{Z}^+}(r\sqrt{n}) = \{\mathbf{y} \in \mathbb{Z}^{n+1}_{\geq 0} : \|\mathbf{y}\|_1 = r\sqrt{n}\},$$

$$\mathcal{B}^{n}_{1,\mathbb{Z}^+}(r\sqrt{n}) = \{\mathbf{y} \in \mathbb{Z}^{n}_{\geq 0} : \|\mathbf{y}\|_1 \leq r\sqrt{n}\}.$$

Bonus trick: project away from the largest coordinate to lower $\mathbb{E}(\|\mathbf{y}\|_\infty)$.

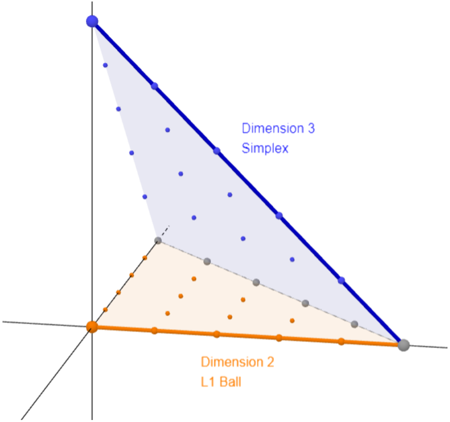


Making the Sampler Uniform and Isochronous

Mind the sides!

- Flip n coins for signs.
- Restart for each 0 coordinate, with probability $1/2$.

- Uniform: ✓
- IsoSignachronous: ✓
- Expected restarts: small if $n \ll r$.

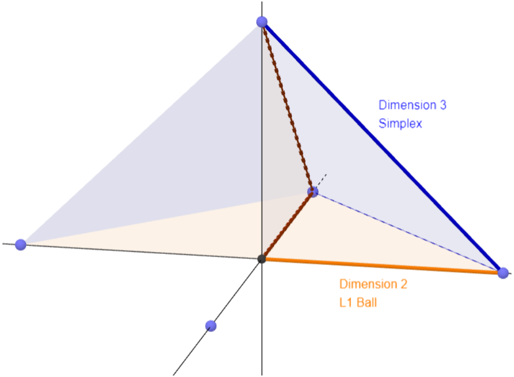


Making the Sampler Uniform and Isochronous

Mind the sides!

- Flip n coins for signs.
- Restart for each 0 coordinate, with probability $1/2$.

- Uniform: ✓
- IsoSignachronous: ✓
- Expected restarts: small if $n \ll r$.



Can we get a Better Polytope?

Theorem (From [Kas77])

There exists a constant $1 < c < 32$ such that for each n, there exists an orthogonal $U \in \mathcal{O}_n(\mathbb{R})$ such that

$$\mathcal{B}_2^n(1) \subseteq \mathcal{B}_1^n(\sqrt{n}) \cap U\mathcal{B}_1^n(\sqrt{n}) \subseteq \mathcal{B}_2^n(c).$$

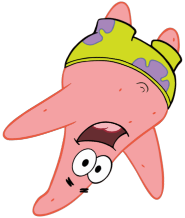
Can we get a Better Polytope?

Theorem (From [Kas77])

There exists a constant $1 < c < 32$ *such that for each* n*, there exists an orthogonal* $U \in \mathcal{O}_n(\mathbb{R})$ *such that*

$$\mathcal{B}_2^n(1) \subseteq \mathcal{B}_1^n(\sqrt{n}) \cap U\mathcal{B}_1^n(\sqrt{n}) \subseteq \mathcal{B}_2^n(c).$$

$\bigcap$



$=$

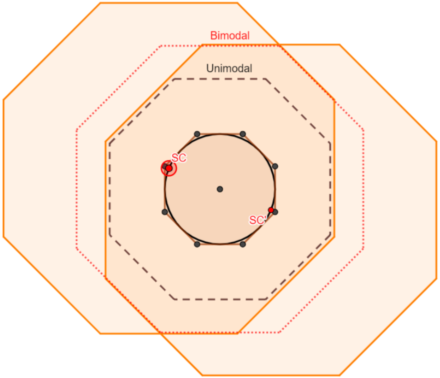
The Bimodal Situation

Objective: Use the trick by [DDLL13] for better sizes.

- We need to study

$$I = \bigcap_{\mathbf{sc} \in \mathcal{B}_2(r)} (\mathcal{P}_{R,\mathbf{sc}} \cup \mathcal{P}_{R,-\mathbf{sc}})$$

- No improvement in the Hypercube case.
- For $\mathcal{H}$, no obvious improvement after dim 4 as the largest $\mathcal{H}$ in I is $\mathcal{H}_{R-r}$.
- For $\mathcal{C}$, less unlikely.



References I

Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Junbum Shin, Damien Stehlé, and MinJune Yi.
HAETAE algorithm specifications and supporting documentation.
Submission to the NIST's post-quantum cryptography standardization process, 2023.

Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky.
Lattice signatures and bimodal Gaussians.
In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 40–56. Springer, Heidelberg, August 2013.

References II

Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé.
CRYSTALS-Dilithium: A lattice-based digital signature scheme.
Submission to the NIST's post-quantum cryptography standardization process (update from February 2021), 2021.

B. S. Kashin.
Diameters of some finite-dimensional sets and classes of smooth functions.
Izv. Akad. Nauk SSSR Ser. Mat., 41(2):334–351, 1977.
Translated in: *Math. USSR-Izv.*, **11** (1977), no. 2, 317–333.

Vadim Lyubashevsky.
Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures.
In Mitsuru Matsui, editor, *ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 598–616. Springer, Heidelberg, December 2009.

References III

Vadim Lyubashevsky.
Lattice signatures without trapdoors.
In David Pointcheval and Thomas Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 738–755. Springer, Heidelberg, April 2012.