# Polytopes in the Fiat-Shamir with Aborts Paradigm

## CWI Student Seminar

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

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

24th of April 2024

# Disclaimer

- Talk based on https://eprint.iacr.org/2024/411.pdf.

# Outline

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

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

IV. Sampling in $\mathcal{H} \cap \mathbb{Z}^n$

# Roadmap

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

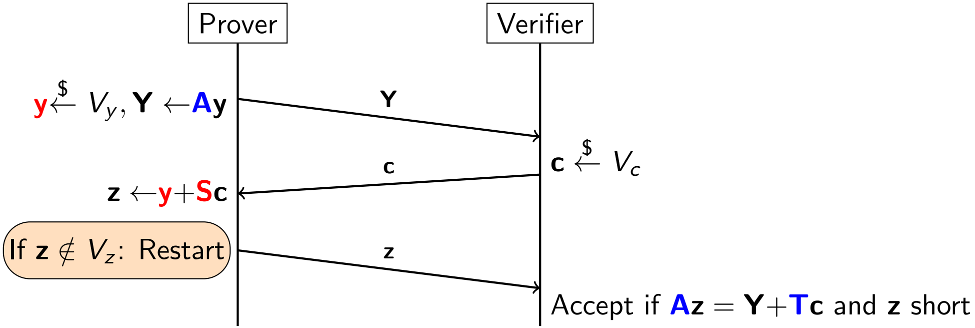
III. Choosing a Polytope $\mathcal{H}$

IV. Sampling in $\mathcal{H} \cap \mathbb{Z}^n$

# SIS-based ID protocol

Secret parameters:
short $\mathbf{S} \in \mathbb{Z}_q^{m \times k}$

Public parameters:
$\mathbf{A} \in \mathbb{Z}_q^{n \times m}, \mathbf{T} = \mathbf{A}\mathbf{S}$

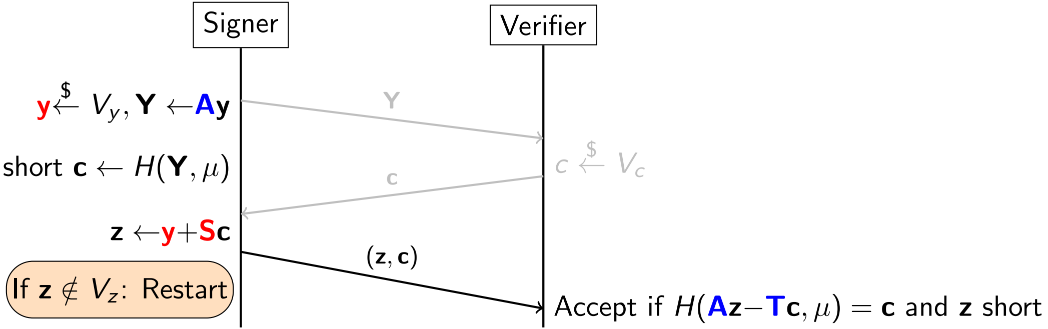


# Fiat-Shamir with Aborts

Message: $\mu$

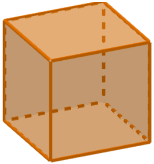
Signing Key: short $\mathbf{S} \in \mathbb{Z}_q^{m \times k}$

Public parameters: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{T} = \mathbf{A}\mathbf{S}$

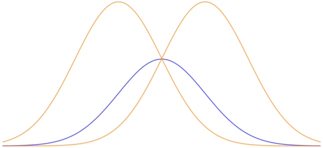


# Rejection sampling: a brief history of distributions

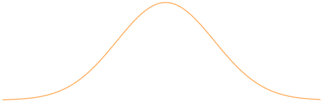
Idea: provably transform an imperfect distribution into a perfect distribution.



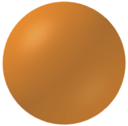
[Lyu09, DKL+21]



[DDLL13, CCD+23]



[Lyu12]



[CCD+23]

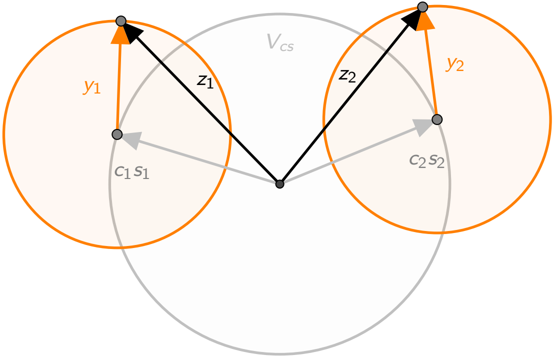
# Important remarks

Our security relies on structured variants of `SIS`:
`MLWE`, `MSIS` and `SelfTargetMSIS`.

The important metric for signature size and $\mathrm{Supp}(V_{cs})$ is the $L_2$ metric.

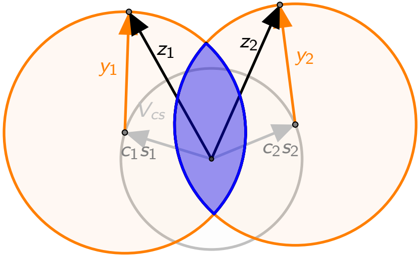
- We focus on the unimodal case (for now).
- We focus on uniform distributions.
- Notation: we identify distribution $V_y$ and set $\mathrm{Supp}(V_y)$.

# Rejection sampling: motivation



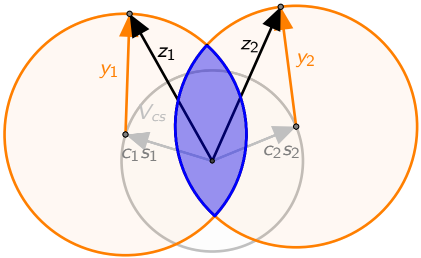

Knowing **z** should reveal **no information** on **y** and **cs**.

# Rejection sampling: motivation




**Witness-Indistinguishability:** each $\mathbf{z}$ in the blue area is equally likely to have been generated from any valid secret key.

# Rejection sampling: motivation




**Witness-Indistinguishability:** each $\mathbf{z}$ in the blue area is equally likely to have been generated from any valid secret key.

This must hold for **all** elements of $V_{\mathbf{cs}}$.

# What do we want?

Assuming uniform distributions $\mathbf{z}$ avoids information leakage if and only if:

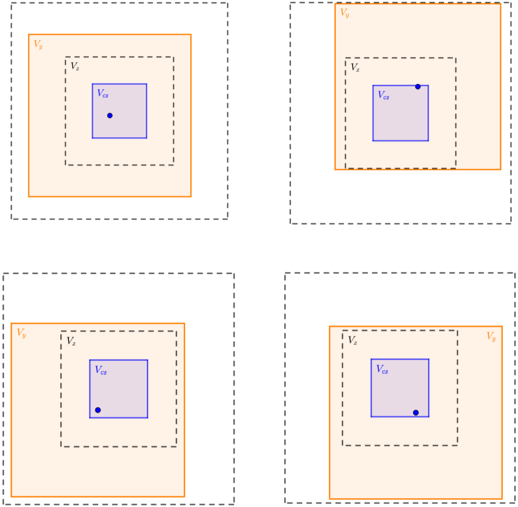
$$V_z \subseteq \bigcap_{\mathbf{x} \in V_{cs}} (V_y + \mathbf{x}).$$

Furthermore, $V_z$ minimises the number of rejects if and only if:

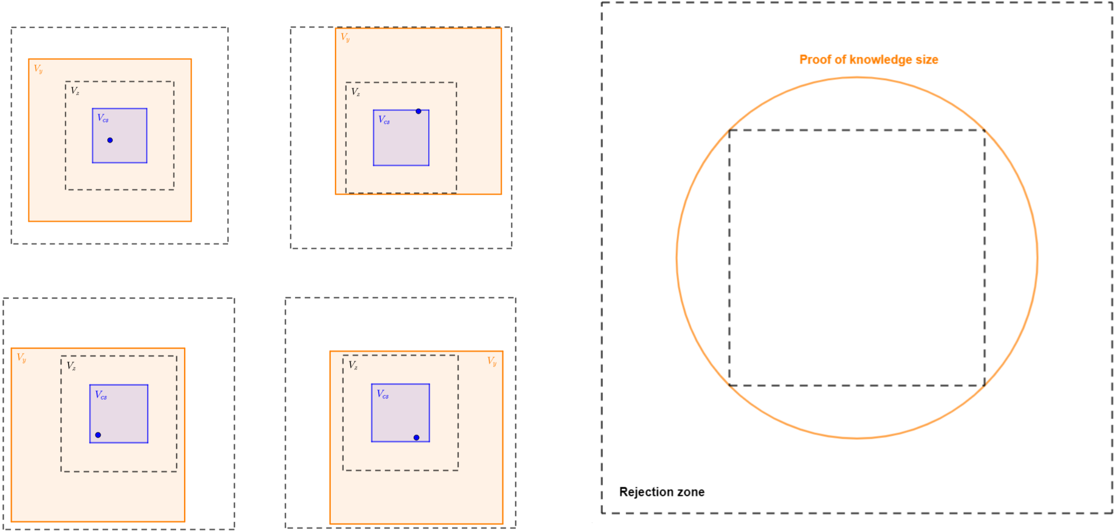
$$V_z = \bigcap_{\mathbf{x} \in V_{cs}} (V_y + \mathbf{x}).$$

- $\max_{\mathbf{z} \in V_z} \|\mathbf{z}\|_2$ conditions the signature size.
- Rejection rate depends on the tightness of the inclusion.

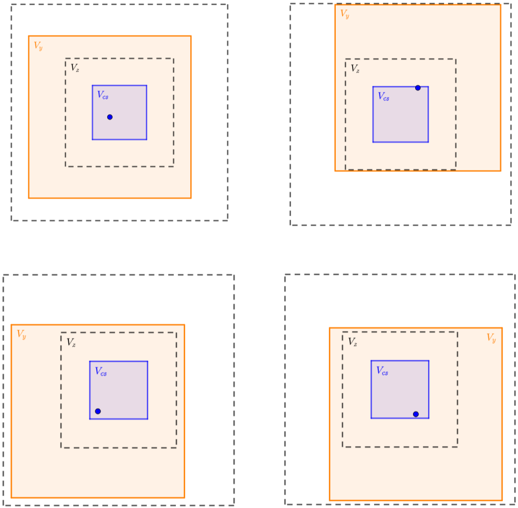
# Illustration: a Square

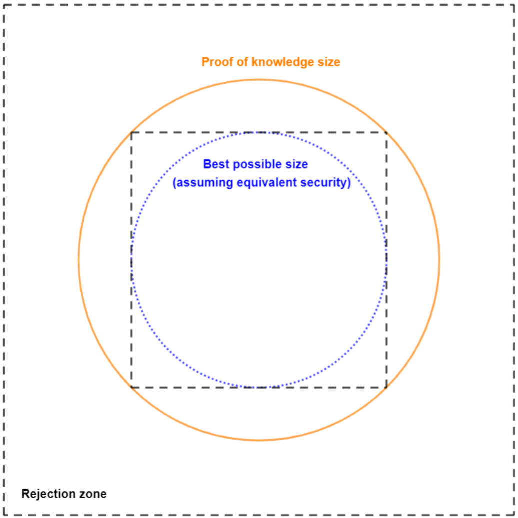


# Illustration: a Square



# Illustration: a Square



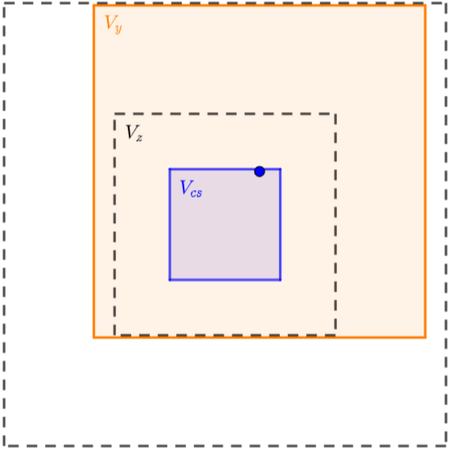



# Starting Point: DFPS22

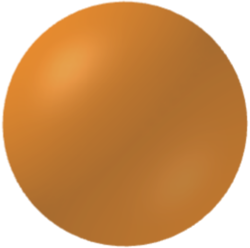
Probability of rejecting:

$$\frac{\mathrm{Vol}(V_z)}{\mathrm{Vol}(V_y)}.$$

- [DFPS22] observe that Gaussian distributions and uniform distributions in Hyperballs give optimal sizes.



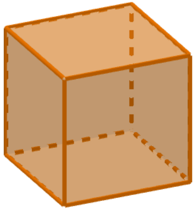
# Hyperballs: Pros and Cons



- Very small sizes (optimal according to [DFPS22]).
- Hard to mask against side channels.
- Hard to sample (Fixed point arithmetic).
- Only analysed in the continuous setting.
- Used in HAETAE [CCD+23].

# Hypercubes: Pros and Cons

- Larger sizes (in some sense hard to do worse).
- Easy to mask against side channels.
- Very simple sampler.
- Valid in the discrete setting.
- Used in DILITHIUM [DKL+21].



# Proposing a tradeoff: Objectives

**What we want:**

- Good proof sizes (better than DILITHIUM).
- A simple sampler (no FP arithmetic and no Gaussians).
- A valid analysis in the discrete setting.

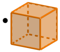
# Roadmap

# Our solution: Polytopes

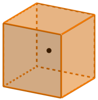
**Definition (Polytope)**

A *polytope* is the convex hull of its vertices $\mathcal{V}(\mathcal{P}) = \{\mathbf{x}_1, \dots, \mathbf{x}_v\} \in \mathbb{R}^n$.

$\mathcal{P}^n_{1,\mathbf{0}}$



$\mathcal{P}^n_{1,(2,0,0)}$



$\mathcal{P}^n_{2,\mathbf{0}}$

# 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 $R > r$. Then:*

$$\bigcap_{\mathbf{c} \in \mathcal{P}_r} \mathcal{P}_{R,\mathbf{c}} = \bigcap_{\mathbf{c} \in \mathcal{V}(\mathcal{P}_r)} \mathcal{P}_{R,\mathbf{c}} = \bigcap_{\text{one } \mathbf{c}_i \text{ per face of } \mathcal{P}_r} \mathcal{P}_{R,\mathbf{c}_i} = \mathcal{P}_{R-r}.$$

# 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 $R > r$. Then:*

$$\bigcap_{\mathbf{c}\in\mathcal{P}_r} \mathcal{P}_{R,\mathbf{c}} = \bigcap_{\mathbf{c}\in\mathcal{V}(\mathcal{P}_r)} \mathcal{P}_{R,\mathbf{c}} = \bigcap_{\text{one } \mathbf{c}_i \text{ per face of } \mathcal{P}_r} \mathcal{P}_{R,\mathbf{c}_i} = \mathcal{P}_{R-r}.$$

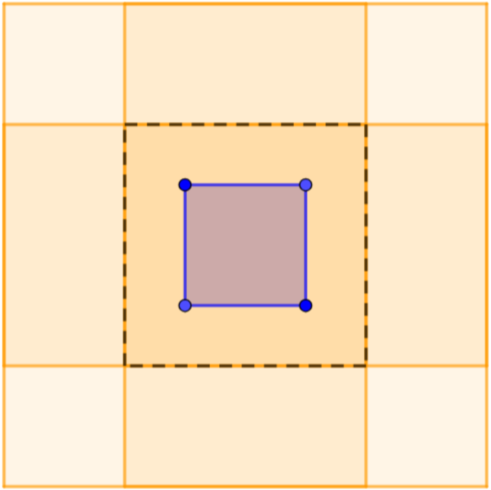
**Corollary (Discrete version)**

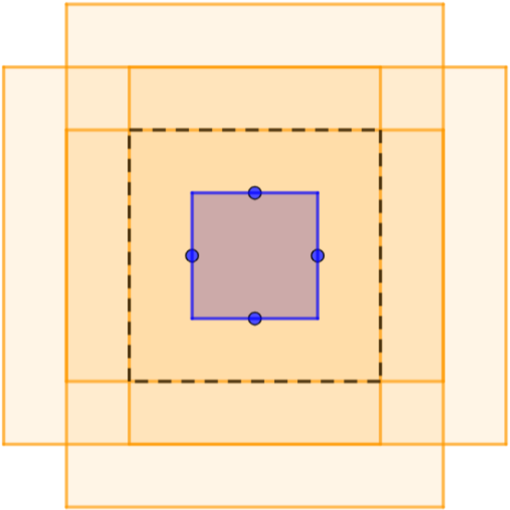
*If $\mathcal{V}(\mathcal{P}_r) \subset \mathbb{Z}^n$, then*

$$\bigcap_{\mathbf{c}\in\mathcal{P}_{r,\mathbb{Z}}} \mathcal{P}_{R,\mathbf{c}} = \bigcap_{\mathbf{c}\in\mathcal{V}(\mathcal{P}_r)} \mathcal{P}_{R,\mathbf{c},\mathbb{Z}} = \mathcal{P}_{R-r,\mathbb{Z}},$$

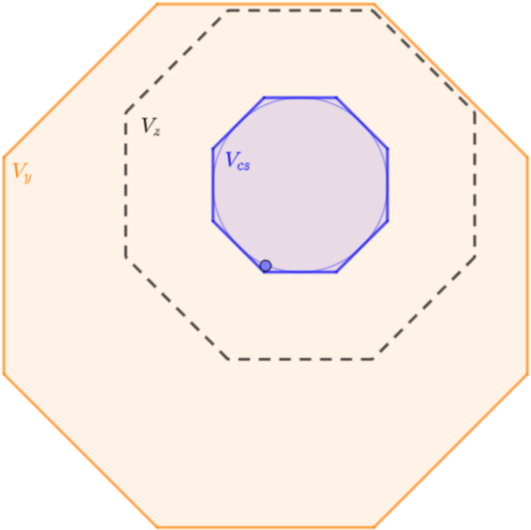
*where $\mathcal{P}_{\mathbb{Z}} = \mathcal{P} \cap \mathbb{Z}^n$.*

# $\mathcal{P}$-ception: Illustration 1





# $\mathcal{P}$-ception: Illustration 2



# Rejection Sampling with Polytopes: Continuous case

Let $\mathcal{P}^n$ be a symmetric polytope whose vertices all lie on a sphere.

**Theorem (informal)**

If $V_y = \mathcal{P}^n_R$ and $V_{cs} \subseteq \mathcal{P}^n_r$, then:

$$\frac{\mathrm{Vol}\,\mathcal{P}^n_{R-r}}{\mathrm{Vol}\,\mathcal{P}^n_R} = \left(\frac{R-r}{R}\right)^n$$

determines the rejection rate.

In practical instantiations, $r \ll R$.

# Rejection Sampling with Polytopes: Discrete case

Let $\mathcal{P}^n$ be a symmetric polytope, with integral vertices all on a sphere, then:

**Theorem (informal)**

If $V_y = \mathcal{P}^n_R \cap \mathbb{Z}^n$ and $V_{cs} \subseteq \mathcal{P}^n_r \cap \mathbb{Z}^n$, then:

$$\frac{|\mathcal{P}^n_{R-r,\mathbb{Z}}|}{|\mathcal{P}^n_{R,\mathbb{Z}}|} = \frac{\mathrm{Vol}\,\mathcal{P}^n_{R-r}}{\mathrm{Vol}\,\mathcal{P}^n_R} \cdot \frac{|\mathcal{P}^n_{R-r,\mathbb{Z}}|}{\mathrm{Vol}\,\mathcal{P}^n_{R-r}} \cdot \frac{\mathrm{Vol}\,\mathcal{P}^n_R}{|\mathcal{P}^n_{R-r,\mathbb{Z}}|} = \left(\frac{R-r}{R}\right)^n \frac{1+\varepsilon_R}{1+\varepsilon_{R-r}}$$

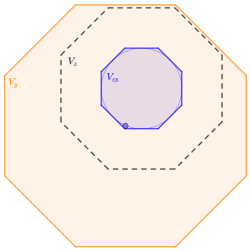
determines the rejection rate.

Computing $\varepsilon$ should be done only once, and requires:

- Volumes of integral polytopes.
- Counting integral points in polytopes.

} Efficient for well-chosen polytopes

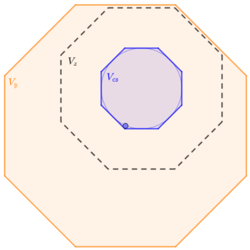
# Extra motivation: Optimality of rejection




Recall that we would like maximality of:

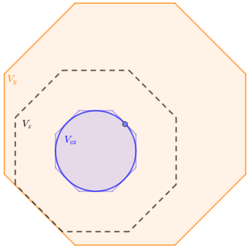
$$\bigcap_{\mathbf{x} \in V_{cs}} (V_y + \mathbf{x}).$$

# Extra motivation: Optimality of rejection

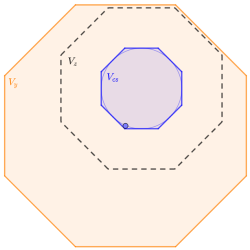



Recall that we would like maximality of:

$$\bigcap_{\mathbf{x} \in V_{cs}} (V_y + \mathbf{x}).$$

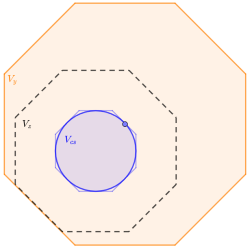


# Extra motivation: Optimality of rejection




Recall that we would like maximality of:

$$\bigcap_{\mathbf{x} \in V_{cs}} (V_y + \mathbf{x}).$$




If the support $V_y$ is a polytope, and if $\mathcal{P}$ is a symmetric polytope that admits an inscribed ball $\mathcal{B}_2$ that is tangent to all of its faces, then we can interchangeably use $\mathcal{P}$ or $\mathcal{B}_2$ for the support of **cs**.

# Roadmap

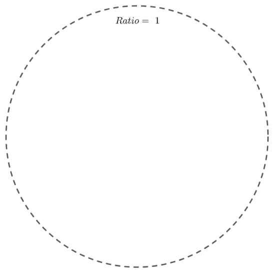
I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

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

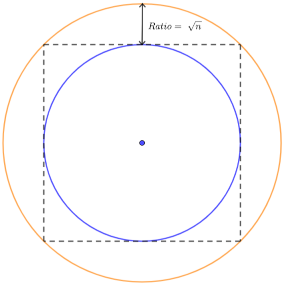
IV. Sampling in $\mathcal{H} \cap \mathbb{Z}^n$

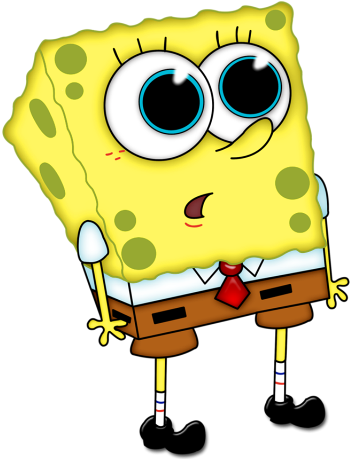
# Polytope choice: Cutting a rare gem




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

- Symmetric
- Inscriptible
- Circumscriptible
- Small ratio
- Integral vertices
- Efficiently samplable





The Hypercube:

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

- Norm: $L_\infty$.
- Volume: $(2R)^n$.
- Inradius: $R$.
- Circumradius: $\sqrt{n}R$.
- Mass concentrates: at the corners.

# Interlude: High-dimensional balls

The Cross-polytope[1]:

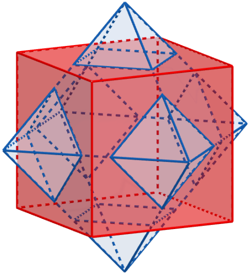
$$\mathcal{B}_1(R) = \{\mathbf{x} \in \mathbb{R}^n : \sum |x_i| \leq R\}.$$

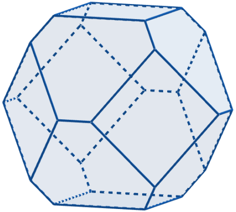
- Norm: $L_1$.
- Volume: $\frac{(2R)^n}{n!}$.
- Inradius: $\frac{1}{\sqrt{n}}R$.
- Circumradius: $R$.
- Mass concentrates: at the center.

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

# The Polytope $\mathcal{H}$

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





# Some properties of $\mathcal{H}$

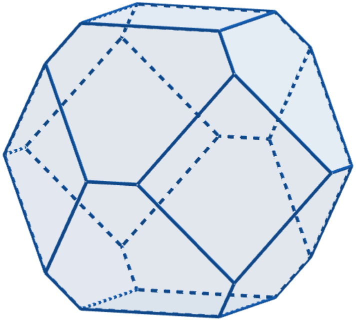
- Volume $\approx \text{Vol}(\mathcal{B}_1^n(r\sqrt{n}))$ :

$$\frac{(2r\sqrt{n})^n}{n!}\sum_{i=0}^{\lfloor\sqrt{n}\rfloor}(-1)^i\binom{n}{i}\left(1-\frac{i}{\sqrt{n}}\right)^{n+1}$$

- Inradius: $r$ (by design).
- Circumradius:

$$r\sqrt{\lfloor\sqrt{n}\rfloor+(\sqrt{n}-\lfloor\sqrt{n}\rfloor)^2}\leq r\sqrt[4]{n}.$$

$\mathcal{H}$ is symmetric, and perfectly inscriptible and circumscriptible.



# Roadmap

I. Intro: Fiat-Shamir and Rejection Sampling

II. The Polytope-based Framework

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

IV. Sampling in $\mathcal{H} \cap \mathbb{Z}^n$

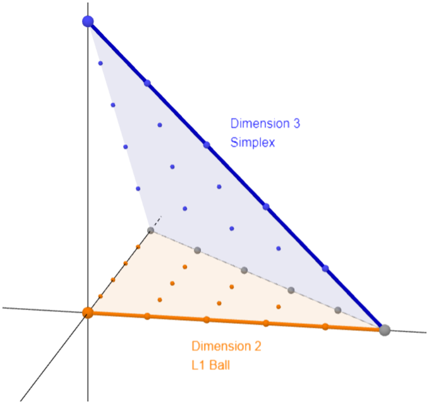
# A useful projection

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 $\mathbb{E}(\|\mathbf{y}\|_\infty)$.



# Sampling in $\mathcal{H} \cap \mathbb{Z}^n$

**$\texttt{SampleL1Sphere}(n, r)$**

$\quad /\!/ \; \mathcal{S} = \{X \subset [\![1, r+n-1]\!] : \#X = n-1\}$
$\mathbf{X} \xleftarrow{\$} \mathcal{U}(\mathcal{S})$
$\mathbf{X} \leftarrow \{0\} \cup \mathbf{X} \cup \{r+n\}$
$\mathbf{X}.\texttt{sort}()$
$\quad /\!/ \; x_0, \cdots, x_n$ the ordered elements of X
**for** $i \in [\![1, n]\!]$ :
$\quad b \xleftarrow{\$} \{0, 1\}$
$\quad y_i \leftarrow (x_i - x_{i-1} - 1)$
$\quad$ **if** $y_i + b = 0$ **then**
$\quad\quad$ **restart**
$\quad y_i \leftarrow (-1)^b y_i$
**return** $\mathbf{Y} := (y_i)_{1 \le i \le n}$

**$\texttt{SampleL1Ball}(n, r)$**

$(y_i)_{n+1} \xleftarrow{\$} \texttt{SampleL1Sphere}(n+1, r)$
**return** $(y_1, \cdots, y_n)$

**$\texttt{SampleH}(n, r)$**

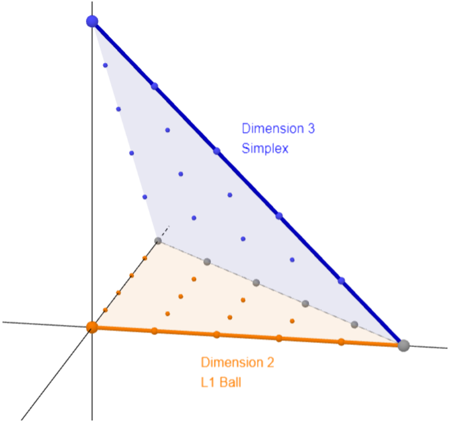
$\Delta_n \leftarrow (\sqrt{n} - \lfloor \sqrt{n} \rfloor)$
$r' \leftarrow \lfloor \sqrt{n} \rfloor r + \lfloor \Delta_n r \rfloor$
$\mathbf{Y} \leftarrow \perp$
**while** $\mathbf{Y} = \perp$ **do**
$\quad \mathbf{Y} \leftarrow \texttt{SampleL1Ball}(n, r')$
$\quad$ **if** $\|\mathbf{Y}\|_\infty > r$ **then**
$\quad\quad \mathbf{Y} \leftarrow \perp$
**return Y**

# Making the sampler Uniform and Isochronous

Mind the sides!

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

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

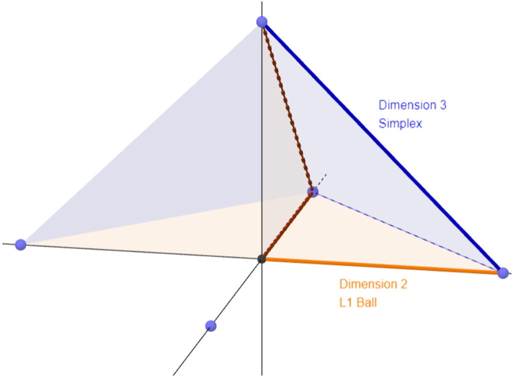


# Making the sampler Uniform and Isochronous

Mind the sides!

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

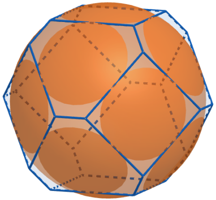
- Uniform: ✓
- Isochronous: ✓
- Expected restarts: small if $n \ll r$.



# Recap.

We have simple sampling with quality $n^{1/4}$

# Reject more for better performances



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

Key observation: for $\theta > c$,

$$1 - \exp(-\sqrt{n}) < \frac{\mathrm{Vol}\,\mathcal{C}^n_{\theta,r}}{\mathrm{Vol}\,\mathcal{H}^n_r} < 1.$$

- Ratio $n^{1/4} \to \theta$
- Trade-off between aborts and size.
- Warning: not a polytope anymore.

# A new Fiat-Shamir with Aborts signature scheme: PATRONUS

# Signature performances: Concrete (example) parameters

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

| Security target (bits) | 120 | 180 | 260 |
|---|---|---|---|
| HAETAE | 1,463 | 2,337 | 2,908 |
| PATRONUS[2] (this work) | 1,869 | 2,398 | 3,459 |
| DILITHIUM | 2,420 | 3,293 | 4,595 |

- **Verification key sizes:** Similar to DILITHIUM ✓
- **Expected rejects:** Similar to HAETAE ✓
- **Sampler randomness:** at most 1.3 times that of DILITHIUM ✓
- **Optimised sampler implementation:** Work in progress ⚠

[2] Parameters may still vary

# 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 $L_\infty$ 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

# 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*

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

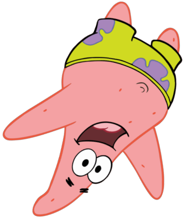
# Can we get a better polytope?

**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*

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

$\cap$



$=$

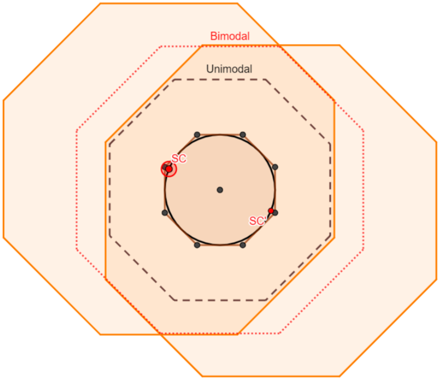
# The Bimodal situation

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

- We need to study

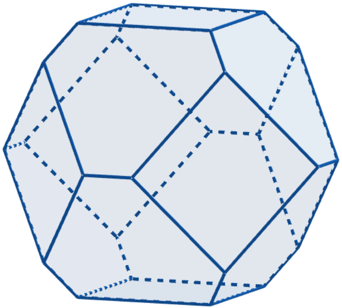
$$I = \bigcap_{\mathbf{sc} \in \mathcal{B}_2(r)} (\mathcal{P}_{R,\mathbf{sc}} \cup \mathcal{P}_{R,-\mathbf{sc}})$$

- 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.



# The End

Thank you for listening!



If you have extra questions, feel free to contact Hugo (hugo.beguinet@ens.fr)

# 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


Julien Devevey, Omar Fawzi, Alain Passelègue, and Damien Stehlé.
On rejection sampling in lyubashevsky's signature scheme.
In Shweta Agrawal and Dongdai Lin, editors, *ASIACRYPT 2022, Part IV*, volume 13794 of *LNCS*, pages 34–64. Springer, Heidelberg, December 2022.

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.

# References III


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.

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.