Polytopes in the Fiat-Shamir with Aborts Paradigm

Henry Bambury, **Hugo Beguinet,**
Thomas Ricosset, Eric Sageloli

Eprint : 2024/411

INTRODUCTION

Fiat-Shamir Transform and its definition in the lattice setting.

FIAT-SHAMIR TRANSFORMATION

Prover / Signer		Verifier
$\mathbf{sk}$	message: μ	$\mathbf{vk}$
$\boldsymbol{y} \leftarrow \text{Random}$		
$\boldsymbol{w} = \text{Commit}(\boldsymbol{vk}, \boldsymbol{y})$	$\boldsymbol{w}$ $\longrightarrow$	
$c = H(\boldsymbol{w}, \mu)$	c $\longleftarrow$	$c \in \text{Chall}$
$\boldsymbol{z} = \text{Prove}(\mathbf{sk}, \boldsymbol{y}, c)$	$c/\boldsymbol{w}, \boldsymbol{z}$ $\longrightarrow$	$\text{Verify}(\mathbf{vk}, \boldsymbol{z}, c/\boldsymbol{w})$

FIAT-SHAMIR with ABORTS

Using uniform distributions

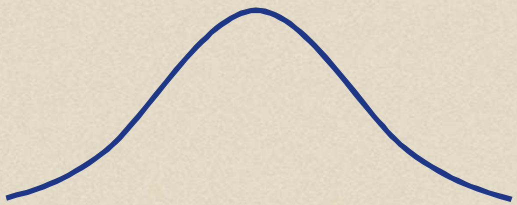
Notation: V_x is the set in which x lives.

Signer		**Verifier**
$\mathbf{sk} = \boldsymbol{S}, \mu$		$\mathbf{vk} = \boldsymbol{AS}$
$\boldsymbol{y} \leftarrow V_{\boldsymbol{y}}$		
$\boldsymbol{w} = \boldsymbol{Ay}$		
$c = \mathrm{H}(\boldsymbol{w}, \mu)$		
➢ $\boldsymbol{z} = \boldsymbol{y} + \boldsymbol{S}c$		
If $\boldsymbol{z} \in V_{\boldsymbol{z}}$	$\xrightarrow{c,\ \boldsymbol{z}}$	$c == \mathrm{H}(\boldsymbol{Az} - \mathrm{vk} \cdot c, \mu)$
else		

Goal: Obtaining the shape of $V_{\boldsymbol{z}}$

EXISTING DISTRIBUTIONS

Gaussian / Uniform



Gaussian & Bimodal

- [Lyu12]
- [DDLL13]

Hypercube Uniform

- [Lyu09, DLK+21]

Hypersphere & Bimodal Uniform

- [CCD+23]

PRACTICAL CHOICES

Trade-off in image

Unattractive

Attractive

Dilithium
[DKL+21]

Haetae
[CCD+23]

Signature size

Public key size

Sampler

01

NOVEL FRAMEWORK

Introduction of a novel framework for Fiat-Shamir with Aborts using convex bodies.

02

FOR A NEW APPROACH

Building an enticing polytope for this new framework.

03

SAMPLER STUDY

Uniform sampler definition within the previously defined polytopes, with its performances.

04

PATRONUS

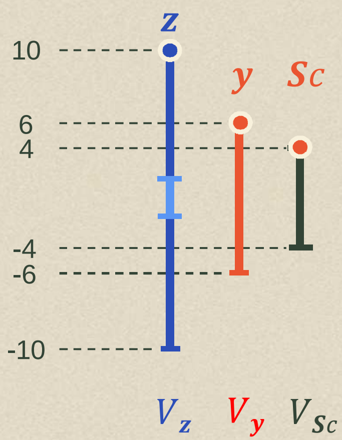
In a nutshell, a competitive Fiat-Shamir signature.

01
Novel Framework

Rejection Sampling

REJECTION SAMPLING

Motivation



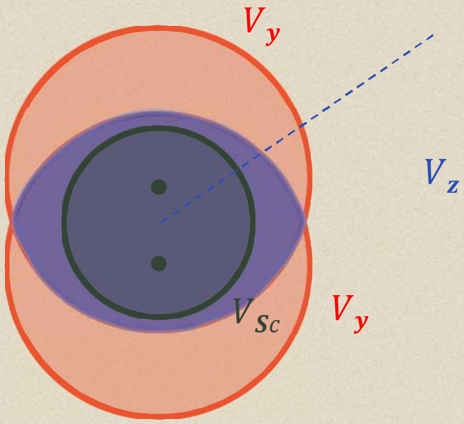
- z, V_z, V_y, V_{Sc} are all public. y, Sc are private.
- $z = y + Sc$.

z should reveal no information on y and Sc

Given V_y and V_{Sc} : How should V_z be?

REJECTION SAMPLING

Geometrical behavior



- Desirable z are in the blue area.
- Leakage is prevented on z if and only if:

$$V_z \subseteq \bigcap_{u \in V_{Sc}} V_y + u$$

The bigger V_z is, the lower the signature size becomes at fixed rejection rate:

$$V_z = \bigcap_{u \in V_{Sc}} V_y + u$$

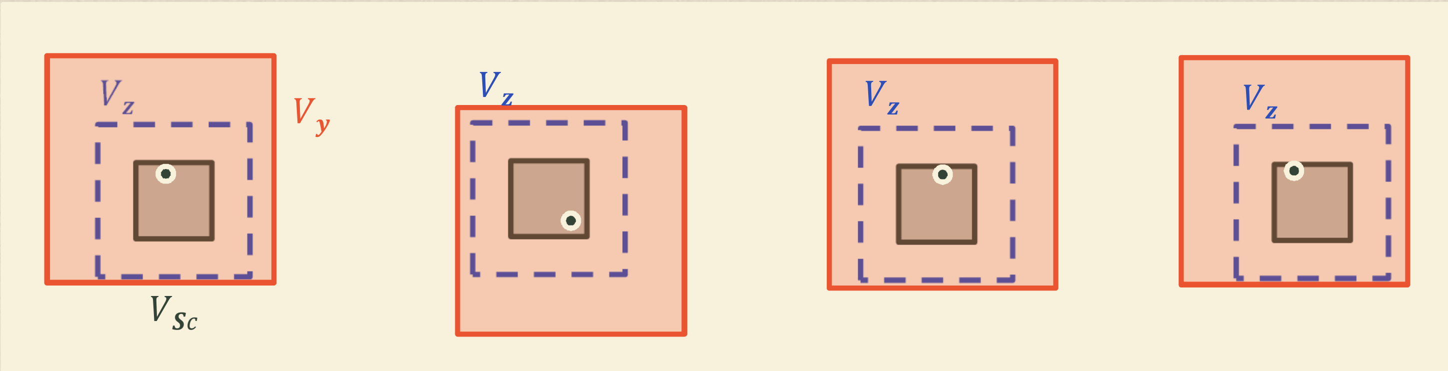
NOVEL FRAMEWORK

P-CEPTION

Theorem *(P-ception: Intersection of Polytopes)*

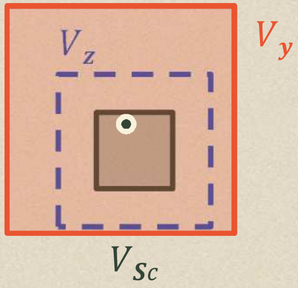
Let P be a symmetric inscriptible and circumscriptible polytope. Let $r, R \in \mathbb{R}$ such that $R > r$ and $P_r = r \cdot P$. Then:

$$\bigcap_{\boldsymbol{u} \in Pr} P_R + \boldsymbol{u} = P_{R-r}$$



P-CEPTION

IMPLICATION

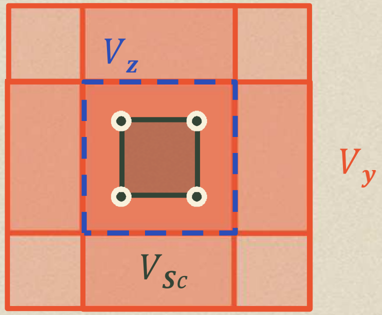


Rejection Probability: $\frac{\mathrm{Vol}(V_z)}{\mathrm{Vol}(V_y)}$

Theorem Application

$\frac{\mathrm{Vol}(V_z)}{\mathrm{Vol}(V_y)} = \frac{(R-r)^n}{R^n}$ with n being the dimension.

P-CEPTION EXTENDED



- Equal result for V_z shape using vertices of V_{Sc}.
.
- But why does it matter?

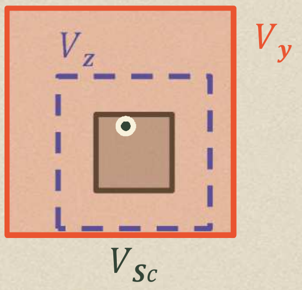
Theorem *(P-ception: Extension 1)*

Additionally, if P_r is an integral polytope then:

$$\bigcap_{\boldsymbol{u} \in Pr \cap \mathbb{Z}^n} P_R \cap \mathbb{Z}^n + \boldsymbol{u} = P_{R-r} \cap \mathbb{Z}^n$$

P-CEPTION EXTENDED

IMPLICATION

$\mathbb{Z}^n \cap$ 

Rejection Probability: $\dfrac{\mathrm{Card}(V_z)}{\mathrm{Card}(V_y)}$

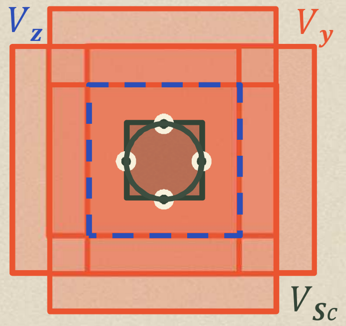
It is usually hard to compute the cardinal of a polytope…

$$\frac{\mathrm{Card}(V_z)}{\mathrm{Card}(V_y)} = \frac{\mathrm{Vol}(V_z)}{\mathrm{Vol}(V_y)} \cdot \frac{\mathrm{Card}(V_z)}{\mathrm{Vol}(V_z)} \cdot \frac{\mathrm{Vol}(V_y)}{\mathrm{Card}(V_y)} = \frac{(R-r)^n}{R^n} \cdot \frac{1+\epsilon_R}{1+\epsilon_{R-r}}.$$

Approximation using counting algorithms.

P-CEPTION EXTENDED

EXTEND-CEPTION



- Equal result for V_z shape using one point on each facet of V_{Sc}.
- Again, why does it matter?
- No change on rejection rate !

Theorem *(P-ception: Extension 2)*

If S is the inscribed sphere of P_r, then:

$$\bigcap_{\boldsymbol{u} \in S} P_R + \boldsymbol{u} = P_{R-r}$$

02
FOR A NEW APPROACH

[BBR+24]

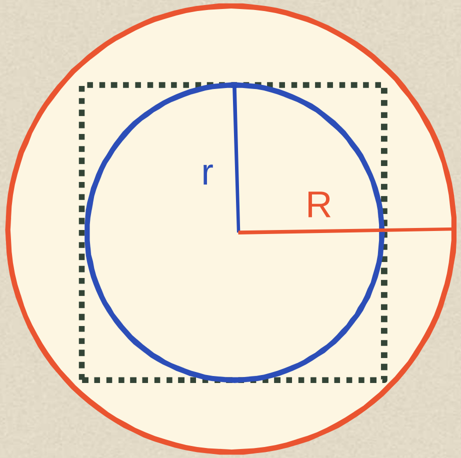
CUTTING A RARE GEM

Prerequisite - Properties

Aim to build a new P

To verify hypotheses:
- Symmetric
- Inscriptible/Circumscriptibile
- Integral vertices

To be efficient:
- Fast sampler
- Small approximation ratio: $\frac{R}{r}$

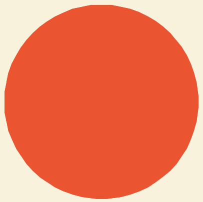


R - proof of knowledge size.

r - best size (fixed security).

CUTTING A RARE GEM

Recapitulative Table

	Signature	Sampler	Bimodal	Ratio
	✖ ✖	✔ ✔	✖	$\sqrt{n}$
	✔ ✔	✖	✔	1

INTERLUDE

Hypercube

Definition $(Hypercube)$

$$B_\infty(R) = \{\, \boldsymbol{x} \in \mathbb{R}^n : \forall i, |xi| \leq R \,\}.$$

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

INTERLUDE

Cross-Polytope

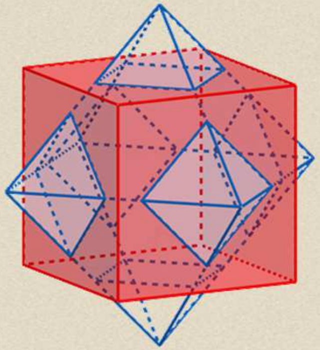
Definition *(Cross Polytope)*

$$B_1(R) = \{\, \boldsymbol{x} \in \mathbb{R}^n : |\textstyle\sum xi| \leq R \,\}.$$

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

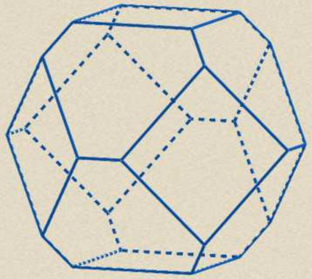
THE POLYTOPE H

An Intersection of Dual



Definition (H)

$$H_R^n = B_\infty(R) \cap B_1(\sqrt{n}R).$$



THE POLYTOPE H

In a nutshell

- Symmetric,
- Inscriptible and circumscriptible,
- Can be defined as an integral polytope through a little trick

- Radius ratio: $\sqrt[4]{n}$,
- Sampler … ?

03

SAMPLER

Step by step

[BBR+24]

SAMPLING WITHIN H

Steps

Sampling within a cross-polytope

1 - Sampling within the positive quadrant,

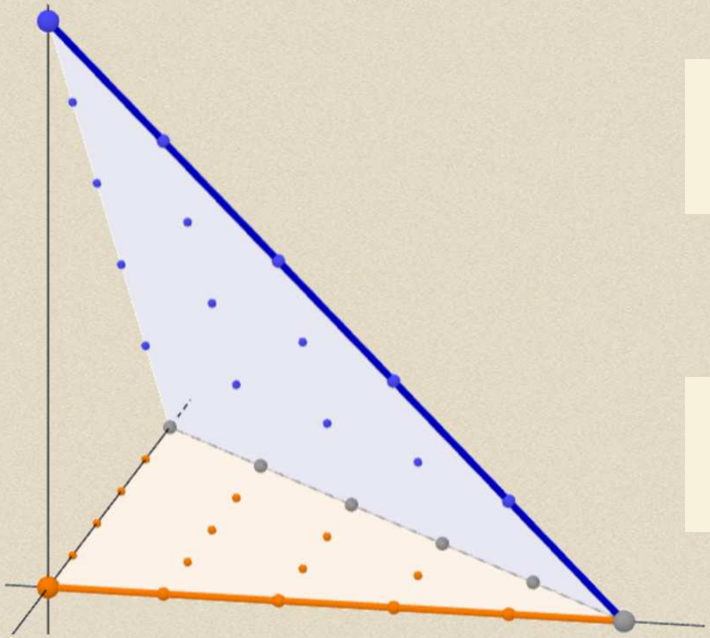
2 - Applying a sign approprietly.

Concluding for a sampler within H

1 - Using a statistical argument.

SAMPLING WITHIN H

positive quadrant



$$S_{1,\mathbb{N}} = \{\, \boldsymbol{y} \in \mathbb{N} : \|\boldsymbol{y}\|_1 = r\sqrt{n} \,\}$$

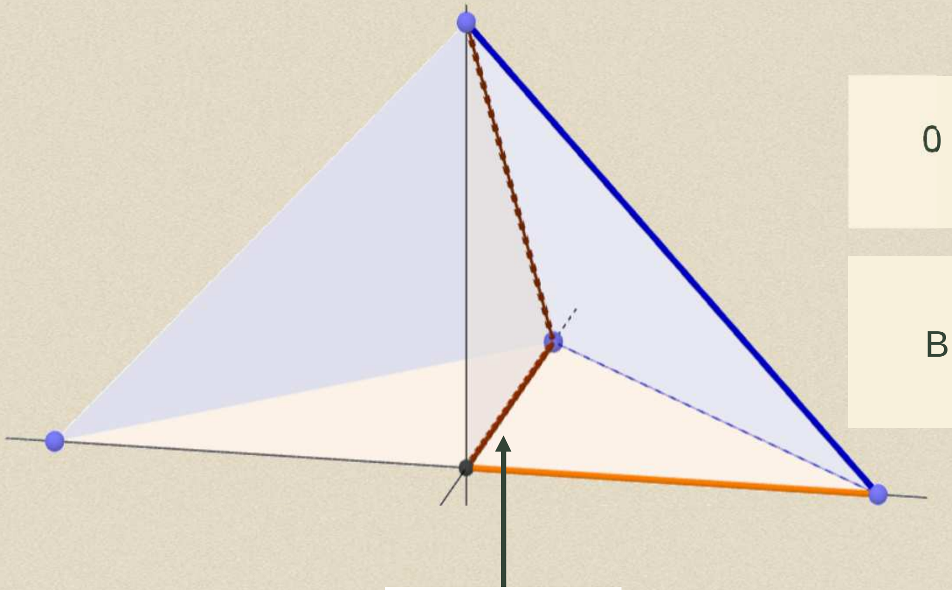
$\updownarrow$ Bijection

$$B_{1,\mathbb{N}} = \{\, \boldsymbol{y} \in \mathbb{N} : \|\boldsymbol{y}\|_1 \leq r\sqrt{n} \,\}$$

Part of a broader theorem on l_p norms

SAMPLING WITHIN H

Applying a sign



Bias !

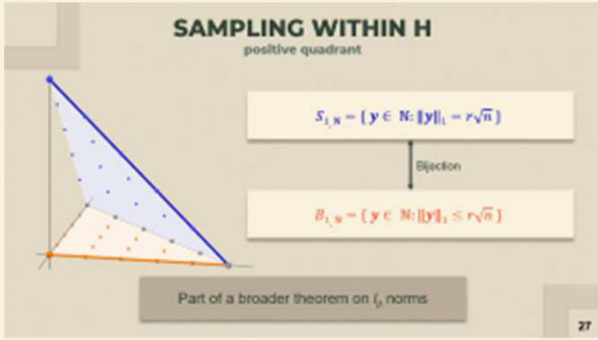
Applying a sign leads to bias!

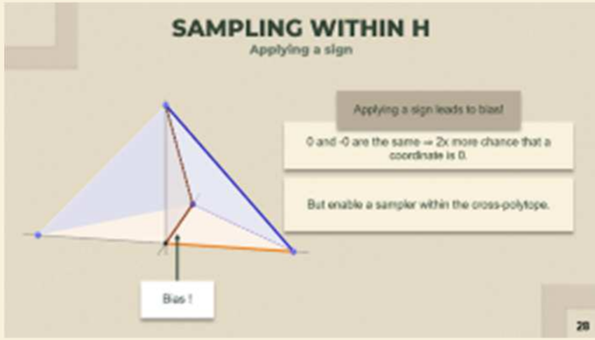
0 and -0 are the same ⇒ 2x more chance that a coordinate is 0.

But enable a sampler within the cross-polytope.

SAMPLING WITHIN H

Applying a sign





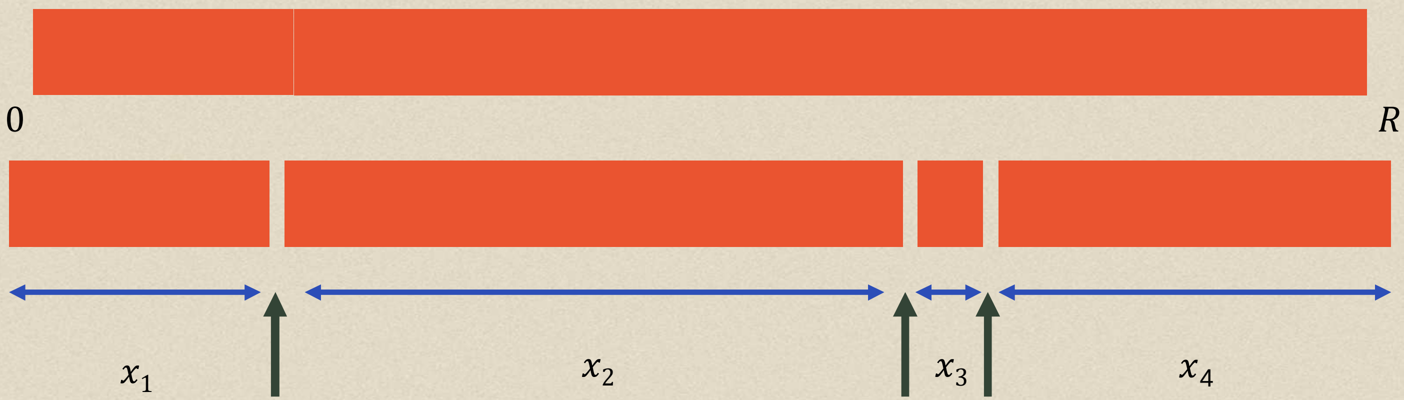
- How to sample on the positive quadrant?
- How to remove bias?

While being Constant-Time or Isochronous!

SAMPLING ON THE SIMPLEX

on reals

Recall the simplex: $S_1 = \{\, \boldsymbol{y} : \|\boldsymbol{y}\|_1 = R \,\}$



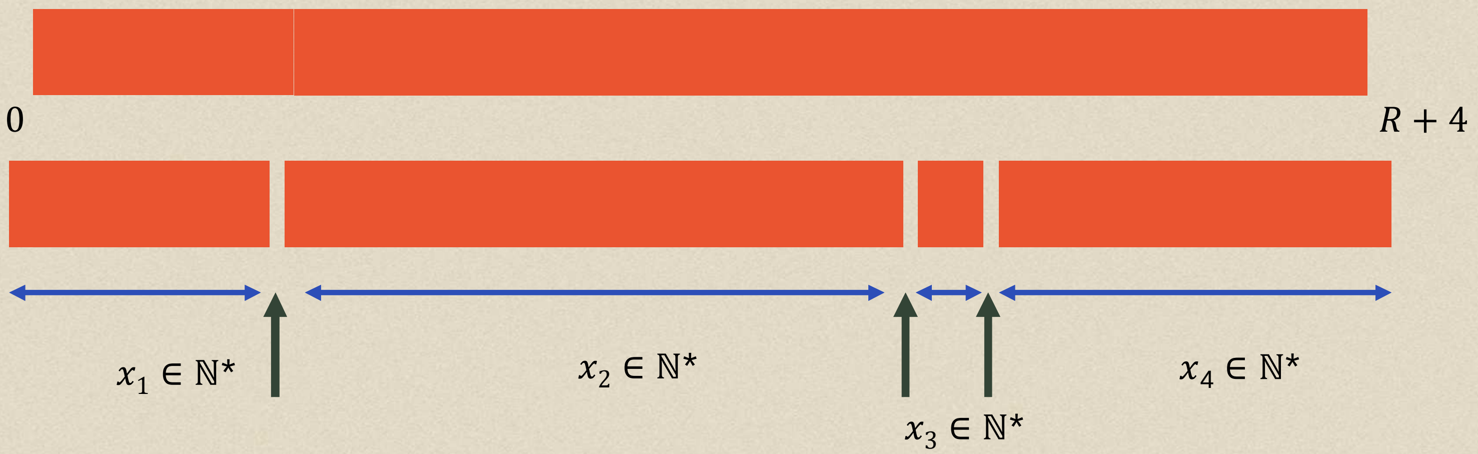
$$\boldsymbol{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

Remove one coordinate to obtain a uniform sampling on the positive quadrant.

SAMPLING ON THE SIMPLEX

on integers

Recall the simplex: $S_{1,\mathbb{N}} = \{ \boldsymbol{y} \in \mathbb{N}^n : \|\boldsymbol{y}\|_1 = R \}$



$$\boldsymbol{x} = \begin{pmatrix} x_1 - 1 \\ x_2 - 1 \\ x_3 - 1 \\ x_4 - 1 \end{pmatrix}$$

Remove one coordinate to obtain a uniform sampling on the positive quadrant.

REMOVING BIAS

Removing bias is easy …

… except when being isochronous is important.

When a 0 coefficient appears, restart with probability 0.5!

Works perfectly for big radius R.
Ex: This application.

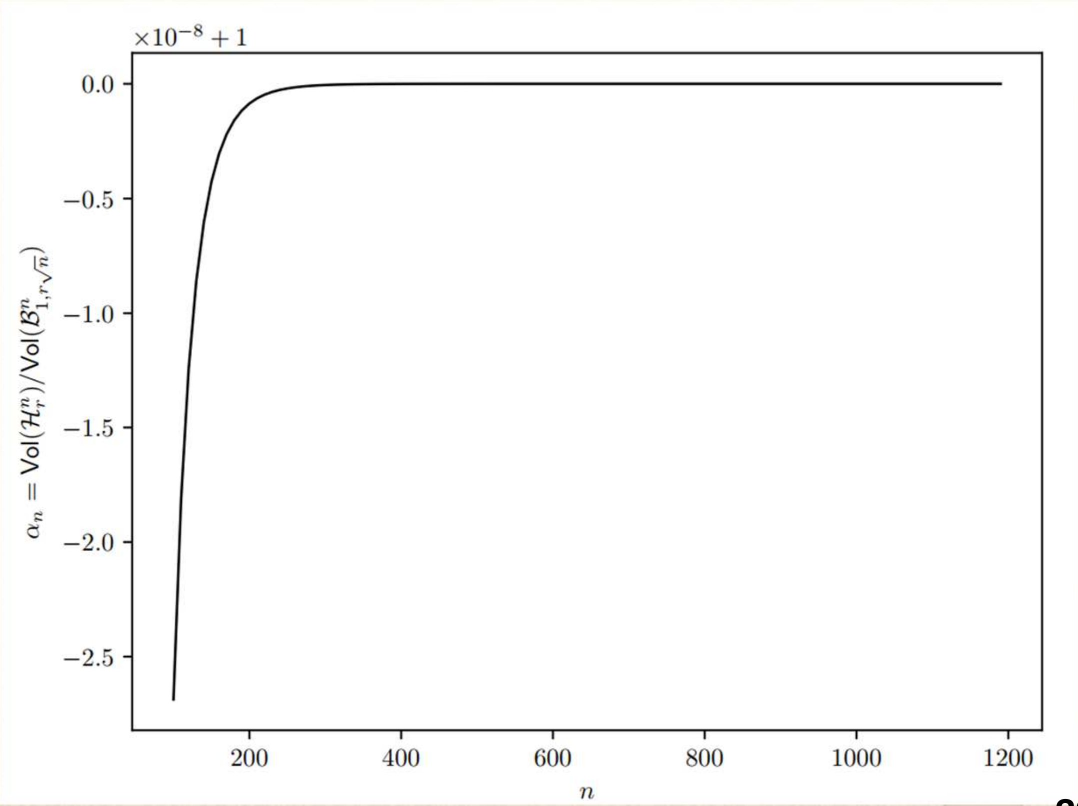
Exponential number of reject for short radius R.
Ex: Sampling short LWE secrets.

SAMPLING ON THE SIMPLEX

on integers

- ➢ Uniform sampler on the n+1 simplex.
- ➢ Uniform sampler within the positive quadrant of the cross-polytope.
- ➢ Adding sign + removing bias isochronously.

Isochronous uniform sampler within H !



SAMPLER PERFORMANCES

i5-1021U CPU

This sampler

NIST Level	II	III	V
Speed(cycle)			
Median	420,721	575,430	1,028,036
Average	453,294	594,168	1,111,171
Randomness(bits)			
Median	16,048	10,064	24,208
Average	16,827	11,087	25,221

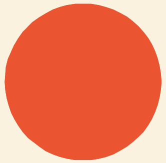
Dilithium sampler

NIST Level	II	III	V
Speed			
Median	24,152	29,732	42,262
Average	24,173	29,943	41,968
Randomness			
Median	-	-	-
Average	2,700	3,400	4,760

With simple tests, Haetae sampler is around the x10 compared to this sampler.

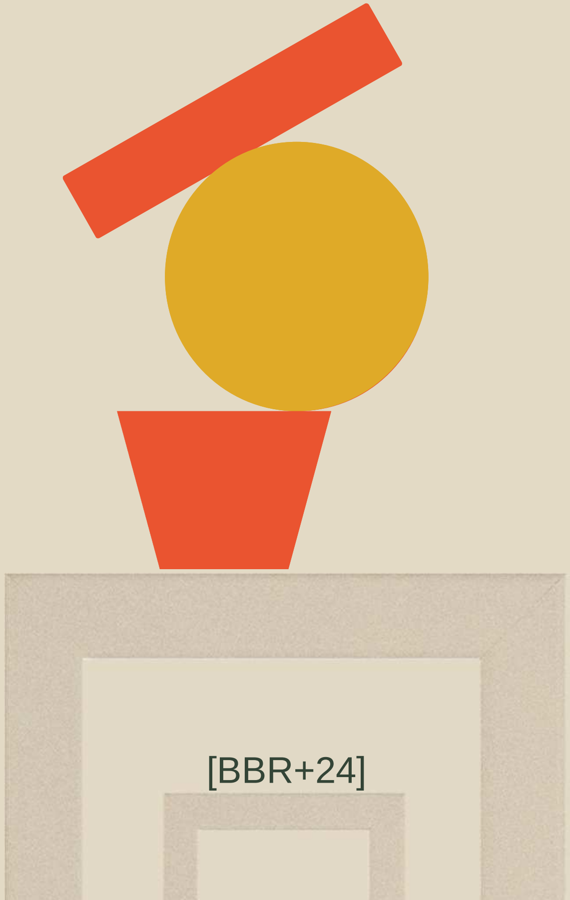
CUTTING A RARE GEM

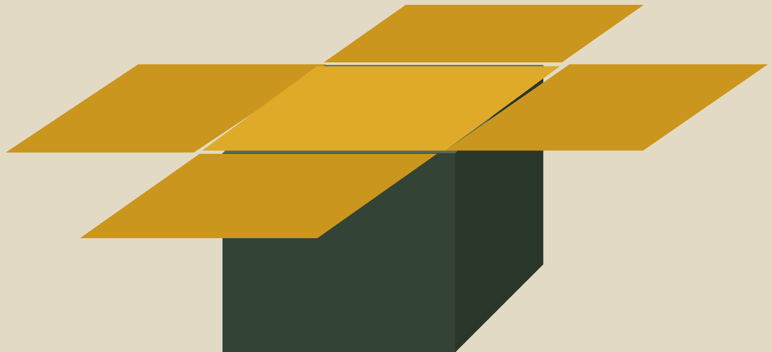
Recapitulative Table Completed

	Signature	Sampler	Bimodal	Ratio
	✗ ✗	✓ ✓	✗	$\sqrt{n}$
	✓	✓	✗	$\sqrt[4]{n}$
	✓ ✓	✗	✓	1

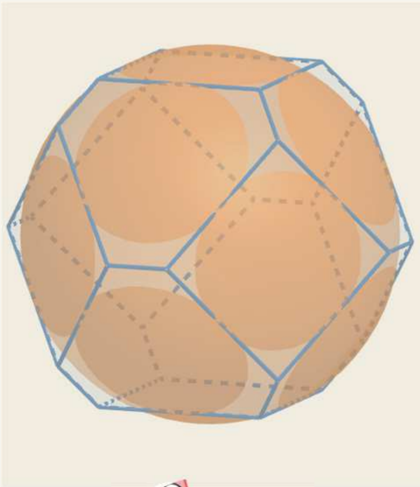
04

PATRONUS





A LAST MINUTE IMPROVEMENT



Definition (C)

$$C_{\theta,r}^{n} = H_{r}^{n} \cap B_2(\theta \cdot r) \text{ with } \theta \approx 1.5.$$

- Low rejection rate,
- θ decreases as (n,r) grows,
- **WARNING:** Not a polytope!

- Radius ratio: $\sqrt[4]{n} \rightarrow 1.5$

PATRONUS PERFORMANCES

Signature size (bytes)			
Security target (bits)	**120**	**180**	**260**
Haetae	1,463	2,337	2,908
Patronus	2,038	2,543	3,689
Dilithium	2,420	3,293	4,595

Verification key size (bytes)			
Haetae	992	1,472	2,080
Patronus	992	1,152	1,952
Dilithium	1,312	1,952	2,592

Rejection rate			
Haetae	6	5	6
Patronus	3	4.25	3
Dilithium	4.25	5,1	3,850

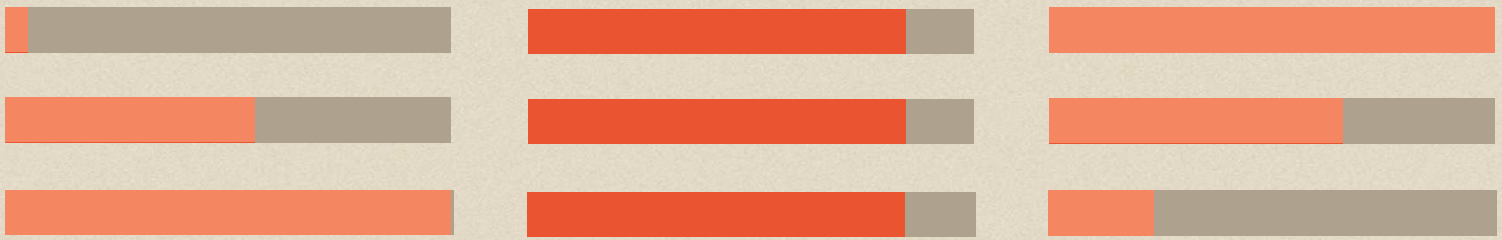
PRACTICAL CHOICES

Trade-off Comparison

Dilithium
[DKL+21]

Patronus
[BBR+24]

Haetae
[CCD+23]



Bonus

BIMODAL

[BBR+24]

THE CASE OF BIMODAL

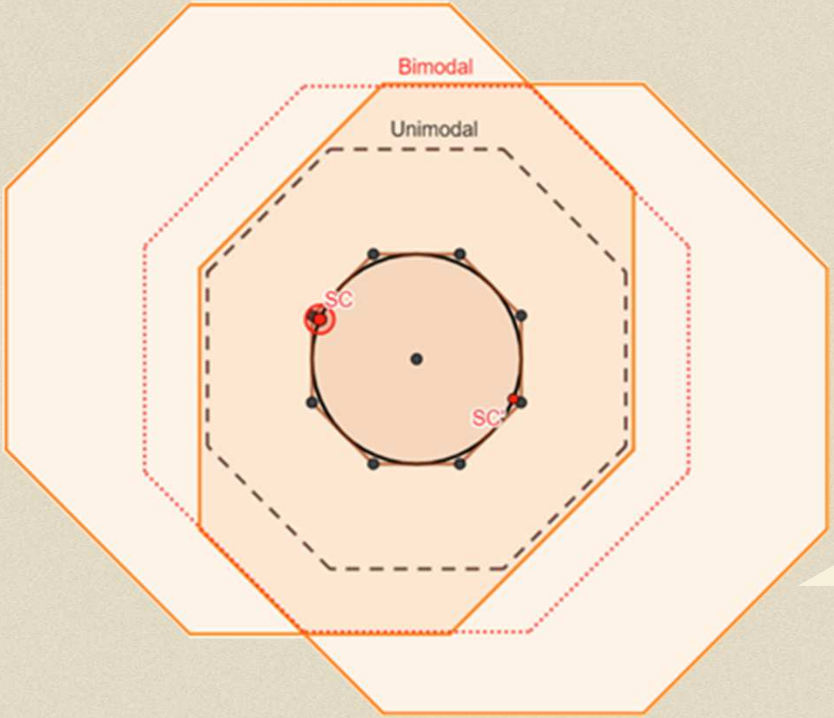
Notation: $V_{\boldsymbol{x}}$ is the set in which $\boldsymbol{x}$ lives.

Signer		Verifier
$\mathrm{sk} = \boldsymbol{S}, \mu$		$\mathrm{vk} = \boldsymbol{AS}$
$\boldsymbol{y} \leftarrow V_{\boldsymbol{y}}$		
$\boldsymbol{w} = \boldsymbol{Ay}$		
$c = \mathrm{H}(\boldsymbol{w}, \mu)$		
➤ $\boldsymbol{z} = \boldsymbol{y} \pm \boldsymbol{S}c$		
$\boxed{\textit{If } \boldsymbol{z} \in V_{\boldsymbol{z}}}$	$\xrightarrow{c,\ \boldsymbol{z}}$	$c == \mathrm{H}(\boldsymbol{Az} - \mathrm{vk} \cdot c, \mu)$

else

Goal: Obtaining the shape of $V_{\boldsymbol{z}}$

BIMODAL CASE

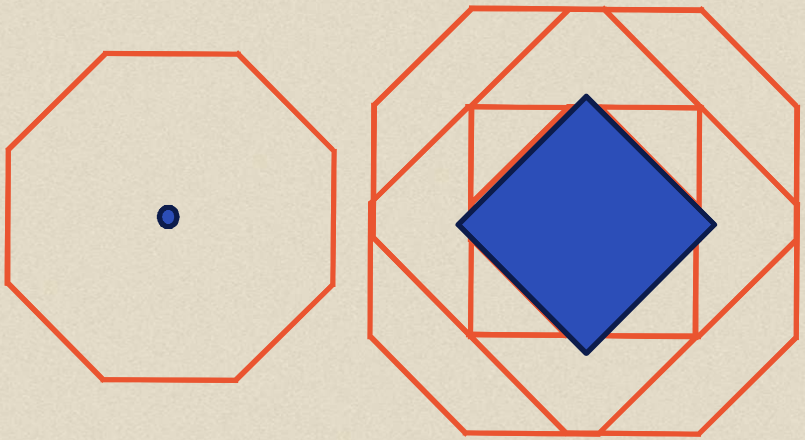


$$\bigcap_{\boldsymbol{u} \in Pr} (\mathrm{P}_R + \boldsymbol{u}) \cup (PR \ - \boldsymbol{u})$$

Does not work in high dimension...

But… Approximate Rejection Sampling?

INTERSECTION OF DUALS



Duality and intersections of Duals might have more intricate behaviors!

Can it be exploited in unstructured lattice based signatures?

CONCLUSION

SUMMARY

Signatures

- A general FSwA framework for convex bodies,
- Its discrete extension with polytopes.

- Introduction of the polytope H verifying the necessary properties,
- With an enticing isochronous sampler (still lacking compared to Dilithium).

- Leading to a competitive signature called Patronus compared to its peers: Dilithium and Haetae.

TO GO FURTHER

Bimodal

- Prove that perfect rejection sampling on polytopes + bimodal is impossible,
- Can it work with approximate rejection sampling ?
- Can bimodal be instanciated with different approaches?

Unstructured Lattice Assumptions

- Corollary of P-ception: Intersection of duals around one of the dual.
- Finer study **S**c: improving its entropy without changing the signature size.

Personal

- Can we find a better « cut » for signature algorithms?!

Thank you for listening!

Any questions ?

REFERENCES

BBR+24: Bambury, H., Beguinet, H., Ricosset, T., Sageloli, É. (2024). Polytopes in the Fiat-Shamir with Aborts Paradigm. In: Reyzin, L., Stebila, D. (eds) Advances in Cryptology – CRYPTO 2024. CRYPTO 2024. Lecture Notes in Computer Science, vol 14920. Springer, Cham.

BCP+23: Beguinet, H., Chevalier, C., Pointcheval, D., Ricosset, T., Rossi, M.: GeT a CAKE: Generic transformations from key encaspulation mechanisms to pass- word authenticated key exchanges. In: Tibouchi, M., Wang, X. (eds.) ACNS 23, Part II. LNCS, vol. 13906, pp. 516–538. Springer, Heidelberg (Jun 2023).

BM92: Steven M. Bellovin and Michael Merritt. Encrypted key exchange: Password-based protocols secure against dictionary attacks. In 1992 IEEE Symposium on Security and Privacy, pages 72–84. IEEE Computer Society Press, May 1992.

CCD+23: 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.

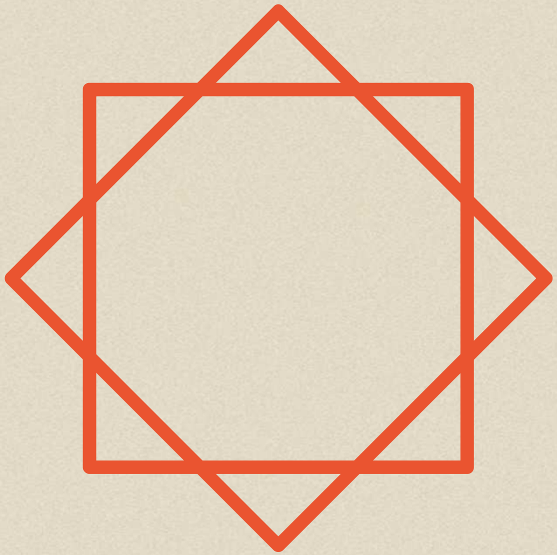
DDLL13: Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal Gaussians. In Ran Canetti and Juan A. Garay, editors, CRYPTO 2013, Part I, volume 8042 of LNCS, pages 40–56. Springer, Heidelberg, August 2013.

DKL+21: 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.

Lyu09: 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.

Lyu12: 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.

BETTER POLYTOPES



It looks like the same as the previous one…

But nop !
There are some nice results on intersections of cross-polytopes ! [Kas77]

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

01

NOVEL FRAMEWORK

Introduction of a novel framework for Fiat-Shamir with Aborts using convex bodies.

02

FOR A NEW APPROACH

Building an enticing polytope for this new framework.

03

SAMPLER STUDY

Uniform sampler definition within the previously defined polytopes, with its performances.

04

PATRONUS

In a nutshell, a competitive Fiat-Shamir signature.

01

NOVEL FRAMEWORK

Introduction of a novel framework for Fiat-Shamir with Aborts using convex bodies.

02

FOR A NEW APPROACH

Building an enticing polytope for this new framework.

03

SAMPLER STUDY

Uniform sampler definition within the previously defined polytopes, with its performances.

04

PATRONUS

In a nutshell, a competitive Fiat-Shamir signature.