5th NIST PQC Standardization Conference, April 10-12, 2024

ANTRAG

SYMPLIFYING AND IMPROVING FALCON WITHOUT COMPROMISING SECURITY

Thomas Espitau, Jade Guiton, **Thi Thu Quyen Nguyen**, Chao Sun, Mehdi Tibouchi, Alexandre Wallet.

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*)

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*)

- Fast
- Short signature
- Security NIST I,V

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*) 

- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*) 

- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka (*Eurocrypt 2022*)

- More parameter choices
- Simpler implementation
- Fast

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*) 

- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka (*Eurocrypt 2022*)

- More parameter choices
- Simpler implementation
- Fast
- Signature 15% larger
- Loss of 20-30 security bits

POST-QUANTUM HASH-AND-SIGN OVER LATTICES

Falcon (*NIST 2017*)

- Restricted parameter choices
- Hard implementation
- Fast
- Short signature
- Security NIST I,V

Mitaka (*Eurocrypt 2022*)

- More parameter choices
- Simpler implementation
- Fast
- Signature 15% larger
- Loss of 20-30 security bits

ANTRAG: Make the best of both worlds

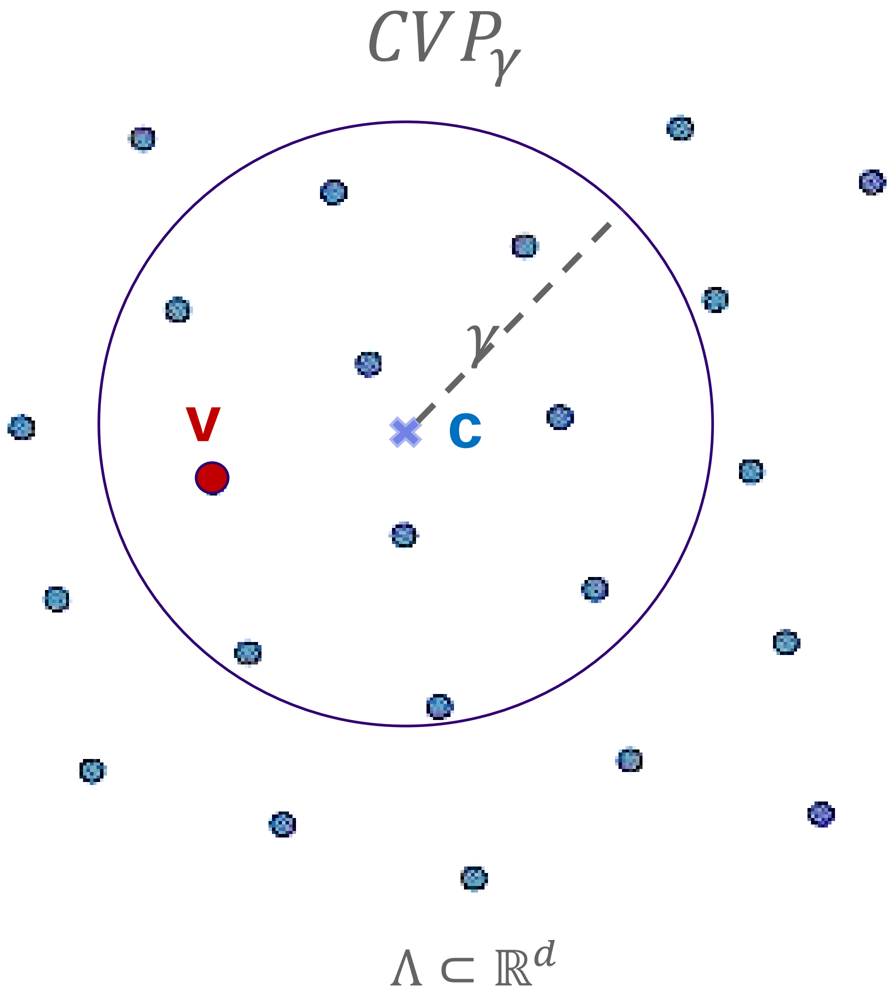
HASH-AND-SIGN OVER LATTICES

Sign($\mathbf{m}, \mathbf{sk}_\Lambda, \gamma$):

- $\mathbf{c} := H(\mathbf{m})$
- $\mathbf{v} \leftarrow \mathrm{CloseVector}_{\Lambda,\gamma}(\mathbf{c})$
- $\mathbf{s} := \mathbf{c} - \mathbf{v}$
- Return $\mathbf{sig} := \mathbf{s}$.

Verify($\mathbf{m}, \mathbf{sig}, \mathbf{pk}_\Lambda, \gamma$):

- Accept iff $\|\mathbf{sig}\| \leq \gamma$ and $H(\mathbf{m}) - \mathbf{sig} \in \Lambda$.



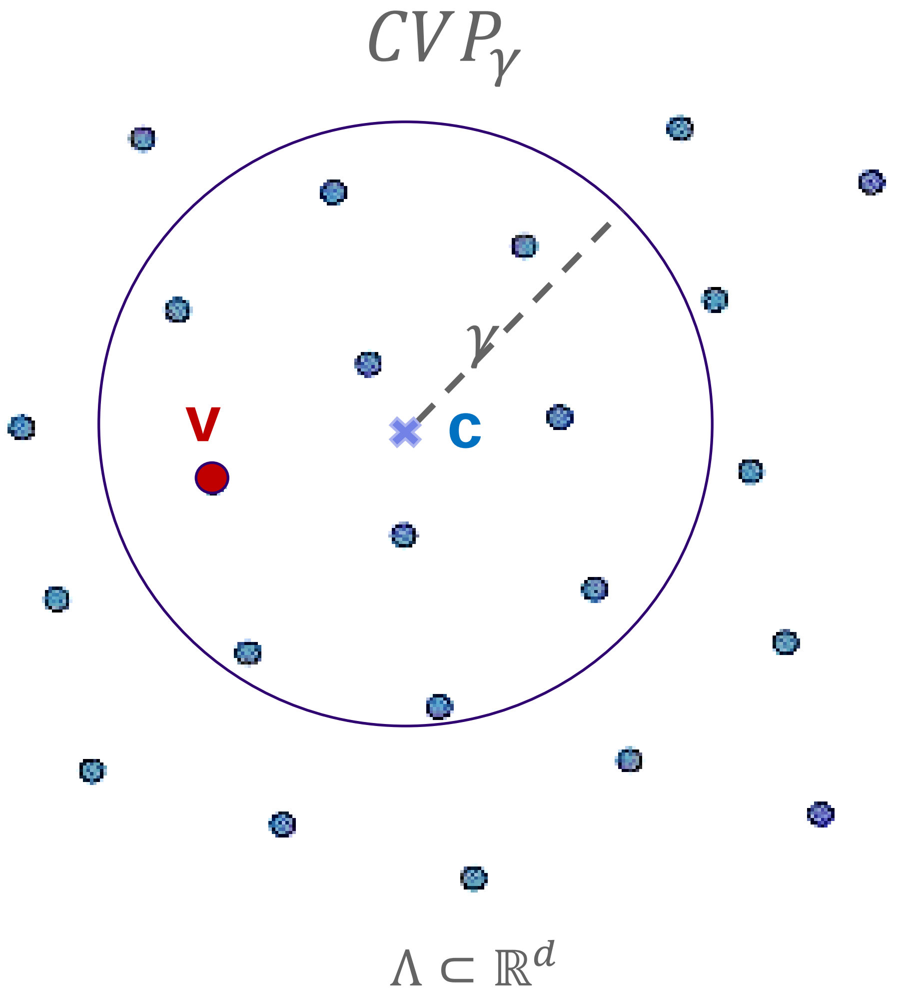
HASH-AND-SIGN OVER LATTICES

Sign$(\mathbf{m}, \mathbf{sk}_\Lambda, \gamma)$**:**

- $\mathbf{c} \coloneqq H(\mathbf{m})$
- $\mathbf{v} \leftarrow \mathrm{DiscreteGaussianSampler}(\mathbf{sk}_\Lambda, \mathbf{c})$
- $\mathbf{s} \coloneqq \mathbf{c} - \mathbf{v}$
- Return $\mathbf{sig} \coloneqq \mathbf{s}$.

Verify$(\mathbf{m}, \mathbf{sig}, \mathbf{pk}_\Lambda, \gamma)$:

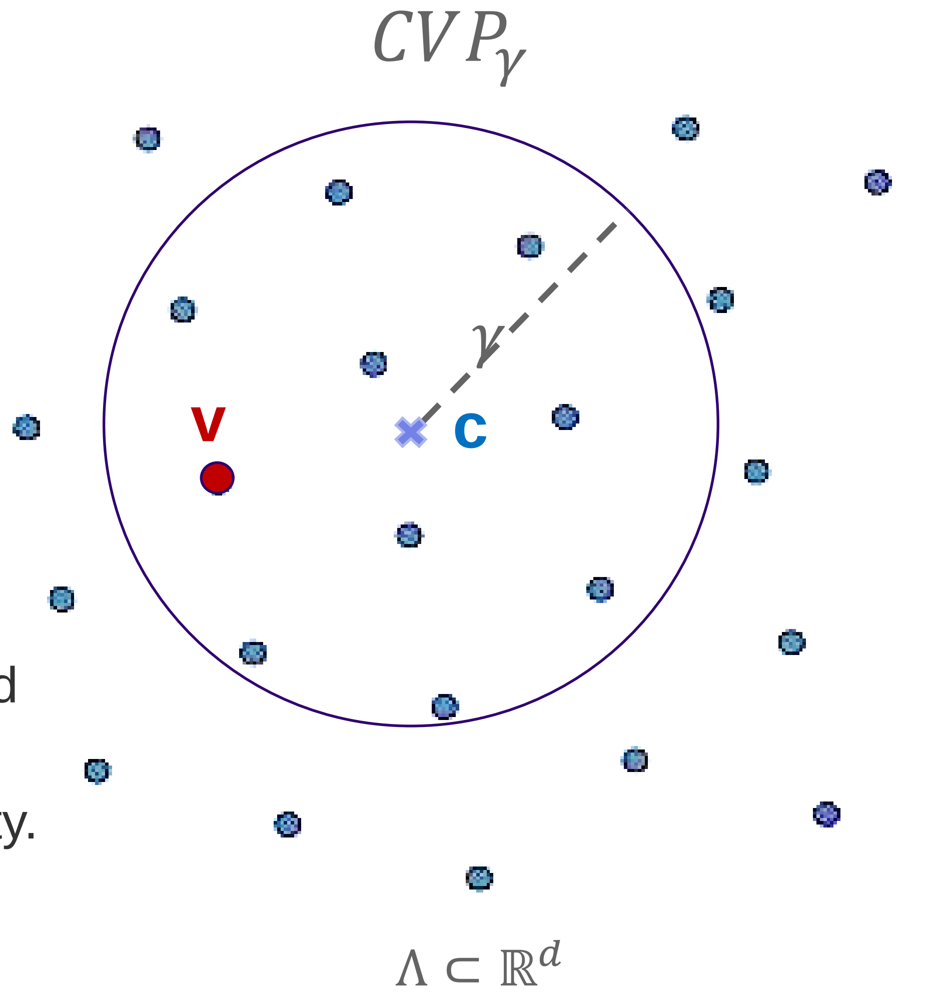
- Accept iff $\|\mathbf{sig}\| \leq \gamma$ and $H(\mathbf{m}) - \mathbf{sig} \in \Lambda$.



HASH-AND-SIGN OVER LATTICES

Sign($\mathbf{m}, \mathbf{sk}_\Lambda, \gamma$):

- $\mathbf{c} \coloneqq H(\mathbf{m})$
- $\mathbf{v} \leftarrow \mathrm{DiscreteGaussianSampler}(\mathbf{sk}_\Lambda, \mathbf{c})$
- $\mathbf{s} \coloneqq \mathbf{c} - \mathbf{v}$
- Return $\mathbf{sig} \coloneqq \mathbf{s}$.



Remarks:

- **Security** : related to Close Vector Problem (CVP) hard to solve without $\mathbf{sk}$.
- Smaller $\mathrm{DiscreteGaussianSampler}(\mathbf{sk}_\Lambda, \cdot)$: better security.

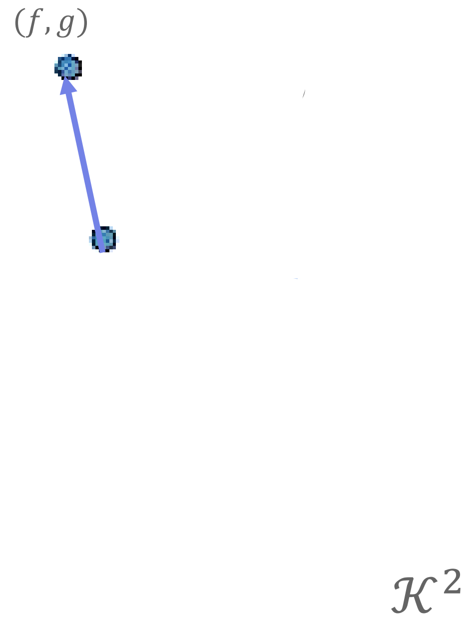
→ need $\mathbf{sk}$ of « good quality », i.e short basis.

NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime

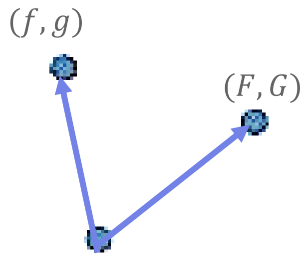
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime
- Small polynomials $f, g \in \mathcal{K}$



NTRU LATTICES

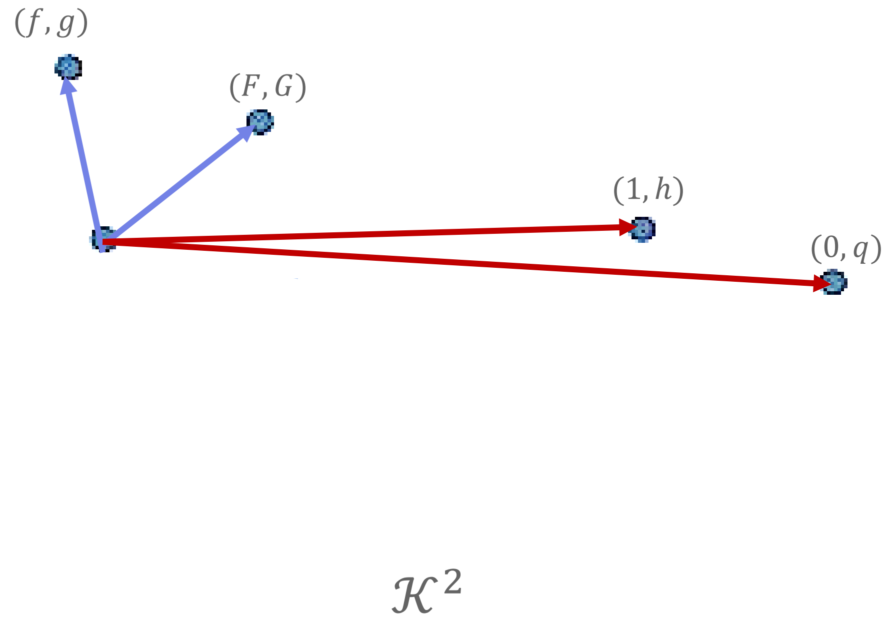
- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$



$\mathcal{K}^2$

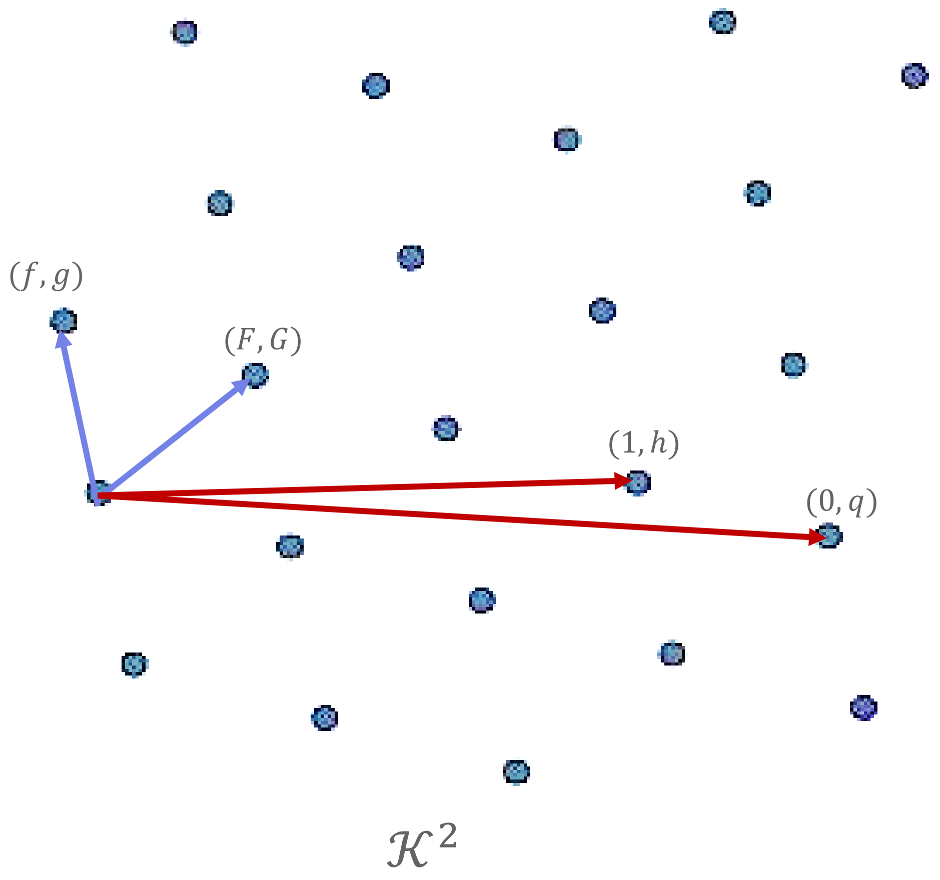
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
- Large $h := f^{-1}g \bmod q$



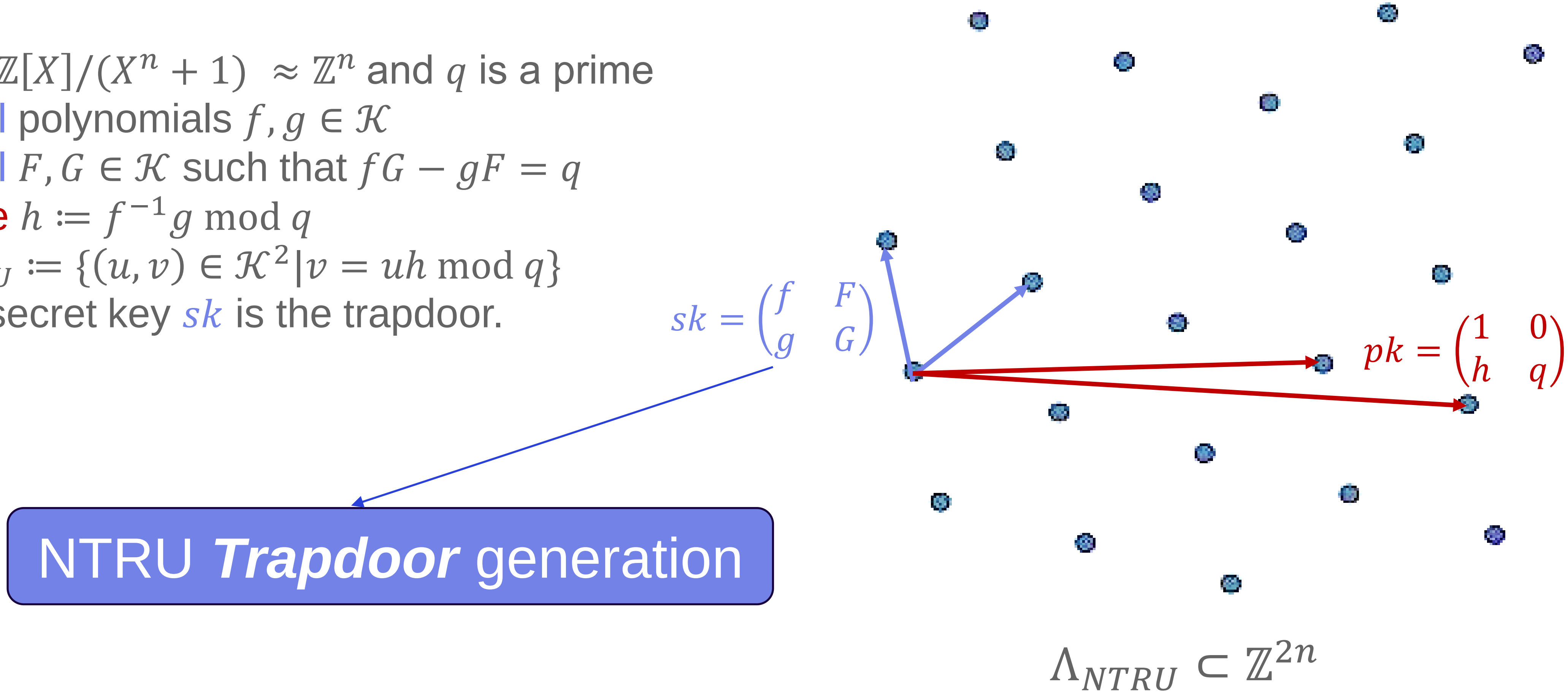
NTRU LATTICES

- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
- Large $h \coloneqq f^{-1} g \bmod q$
- $\Lambda_{NTRU} \coloneqq \{(u, v) \in \mathcal{K}^2 | v = uh \bmod q\}$



NTRU LATTICES

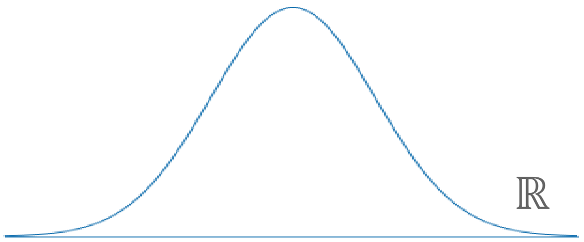
- $\mathcal{K} = \mathbb{Z}[X]/(X^n + 1) \approx \mathbb{Z}^n$ and q is a prime
- Small polynomials $f, g \in \mathcal{K}$
- Small $F, G \in \mathcal{K}$ such that $fG - gF = q$
- Large $h := f^{-1} g \bmod q$
- $\Lambda_{NTRU} := \{(u, v) \in \mathcal{K}^2 | v = uh \bmod q\}$
- The secret key sk is the trapdoor.



GAUSSIAN DISTRIBUTIONS

GAUSSIAN DISTRIBUTIONS

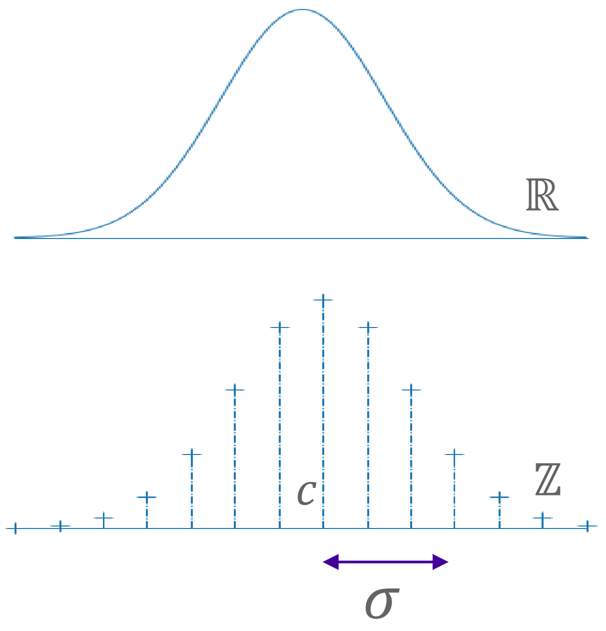
- Gaussian Distribution $\mathcal{N}_{\mathbb{R},c,\sigma}$



GAUSSIAN DISTRIBUTIONS

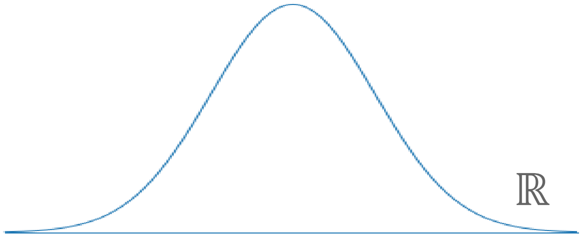
- Gaussian Distribution $\mathcal{N}_{\mathbb{R},c,\sigma}$

- Discrete Gaussian Distribution on $\mathbb{Z}$: $D_{\mathbb{Z},c,\sigma}$

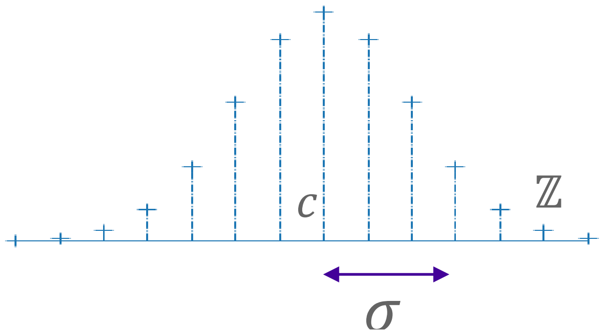


GAUSSIAN DISTRIBUTIONS

- Gaussian Distribution $\mathcal{N}_{\mathbb{R},c,\sigma}$



- Discrete Gaussian Distribution on $\mathbb{Z}$: $D_{\mathbb{Z},c,\sigma}$

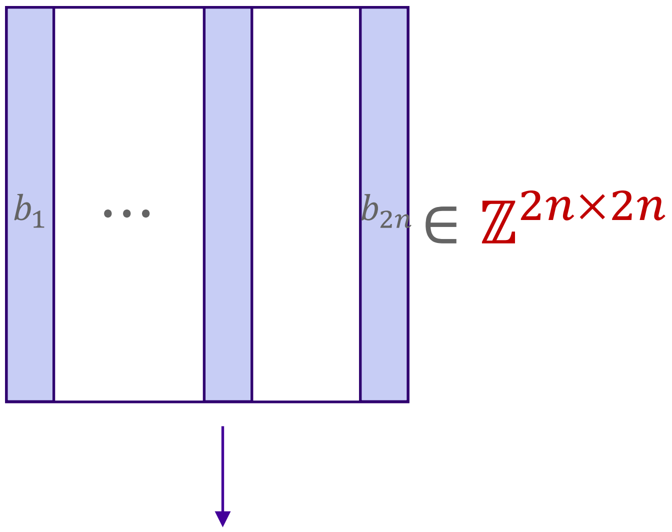


- Discrete Gaussian Distribution on Ring $\mathcal{R}$: $D_{\mathcal{R},c,\sigma}$

EFFICIENT DISCRETE GAUSSIAN SAMPLING

EFFICIENT DISCRETE GAUSSIAN SAMPLING

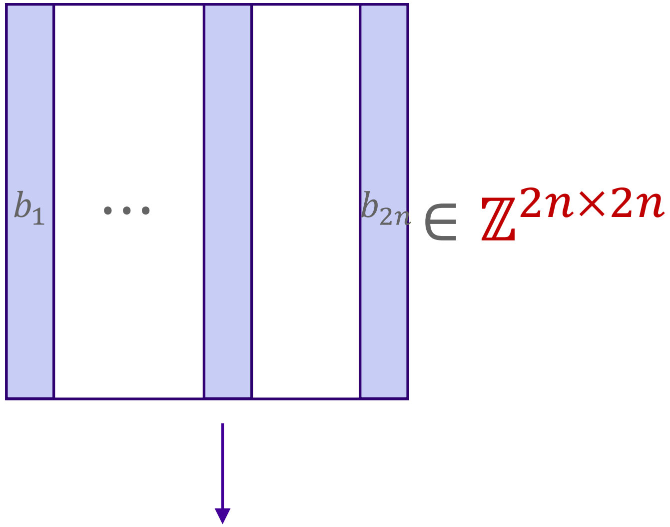
KGPV sampler
[Kle00,GPV08]



Falcon's
Trapdoor **sk**

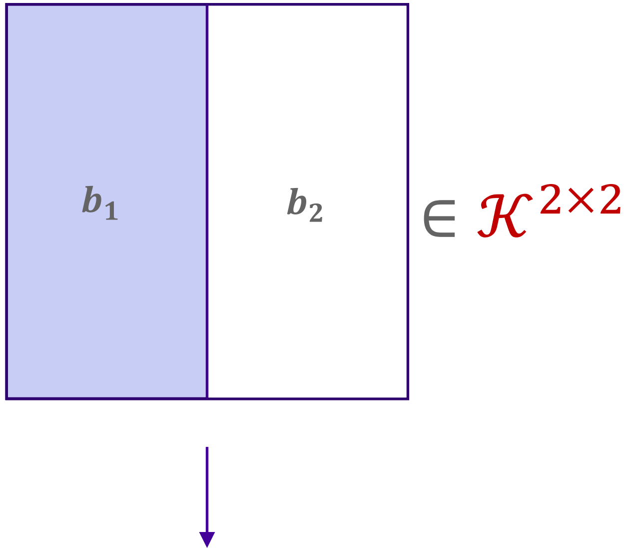
EFFICIENT DISCRETE GAUSSIAN SAMPLING

KGPV sampler
[Kle00,GPV08]



Falcon's
Trapdoor **sk**

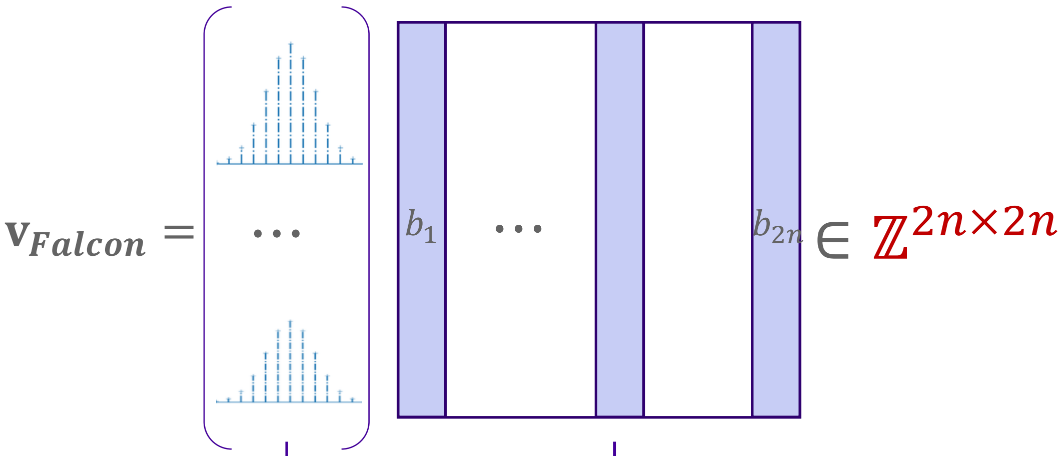
Hybrid sampler
[Pre15]



Mitaka's
Trapdoor **sk**

EFFICIENT DISCRETE GAUSSIAN SAMPLING

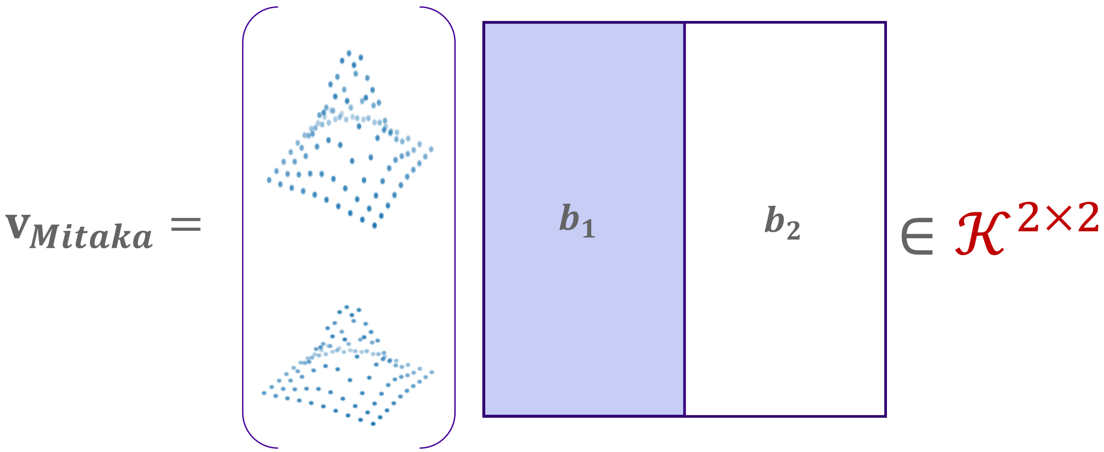
KGPV sampler
[Kle00,GPV08]



$2n$ Discrete Gaussian Samplers on $\mathbb{Z}$

Falcon's Trapdoor **sk**

Hybrid sampler
[Pre15]

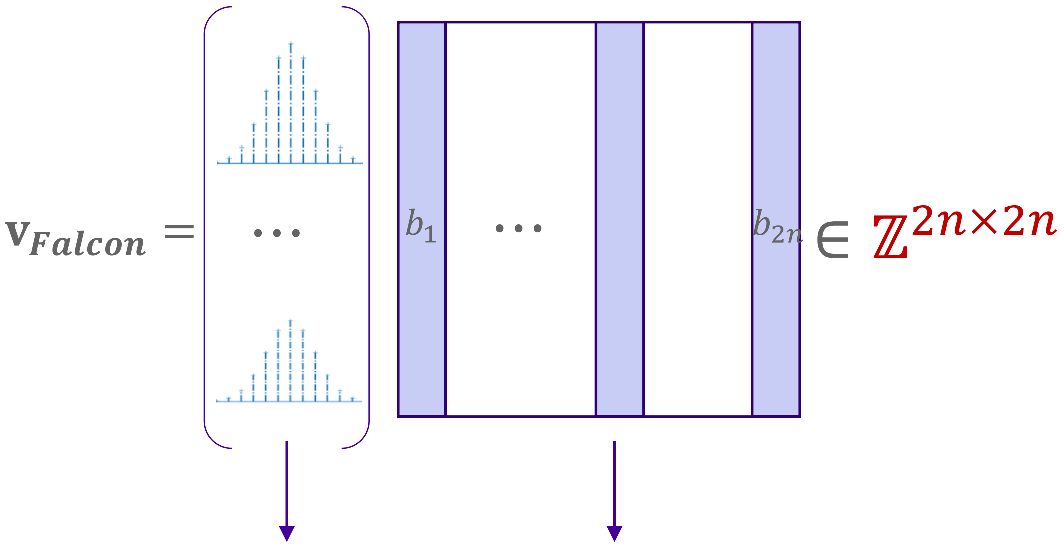


2 Discrete Gaussian Samplers on $\mathcal{K}$ [Pei10]

Mitaka's Trapdoor **sk**

EFFICIENT DISCRETE GAUSSIAN SAMPLING

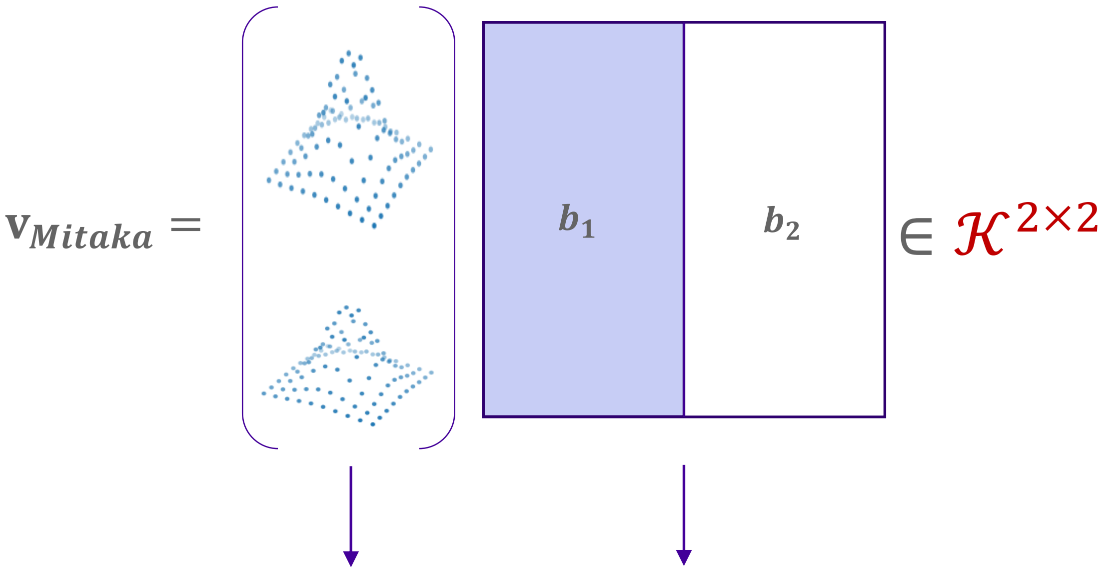
KGPV sampler
Quadratic



$2n$ Discrete Gaussian Samplers on $\mathbb{Z}$

Falcon's Trapdoor **sk**

Hybrid sampler
Quasi-linear



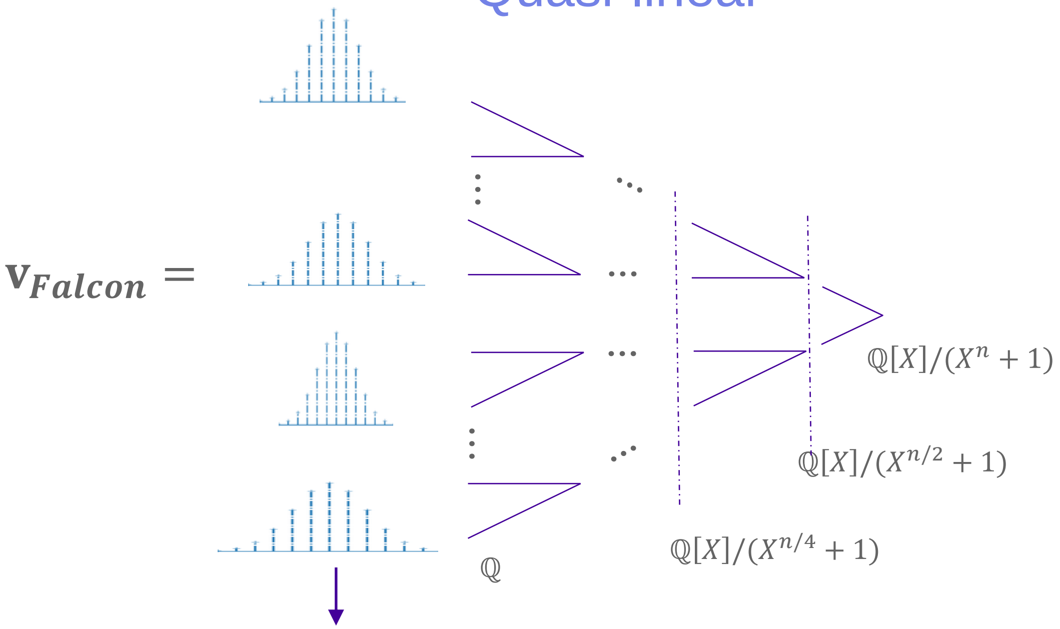
2 Discrete Gaussian Samplers on $\mathcal{K}$ [Pei10]

Mitaka's Trapdoor **sk**

EFFICIENT DISCRETE GAUSSIAN SAMPLING

FFO sampler [DP16]

Quasi-linear

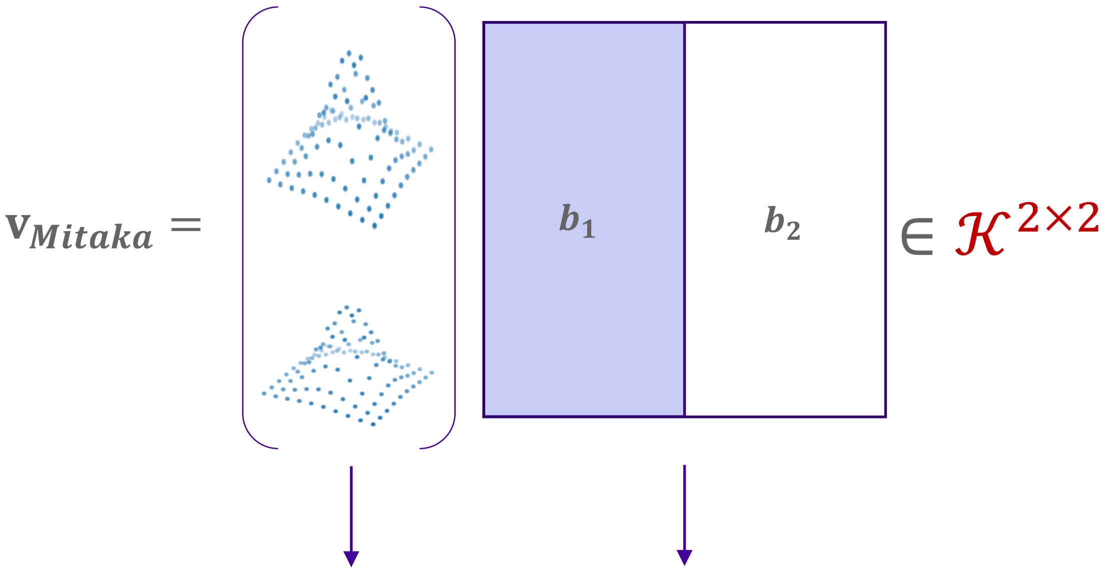


$2n$ Discrete Gaussian Samplers on $\mathbb{Z}$

Falcon's tree: complicated Trapdoor **sk**

Hybrid sampler

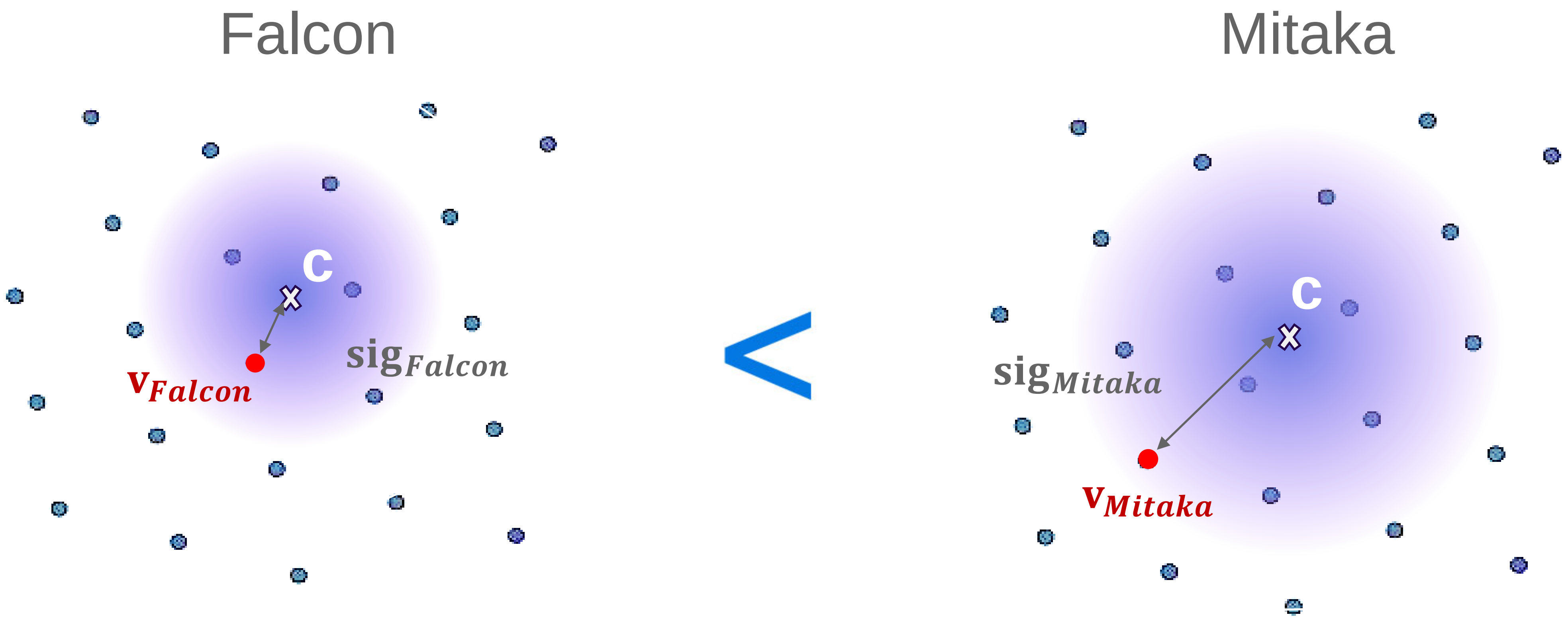
Quasi-linear



2 Discrete Gaussian Samplers on $\mathcal{K}$ [Pei10]

Mitaka's Trapdoor **sk**

SAMPLER/SIGNATURE'S SIZE

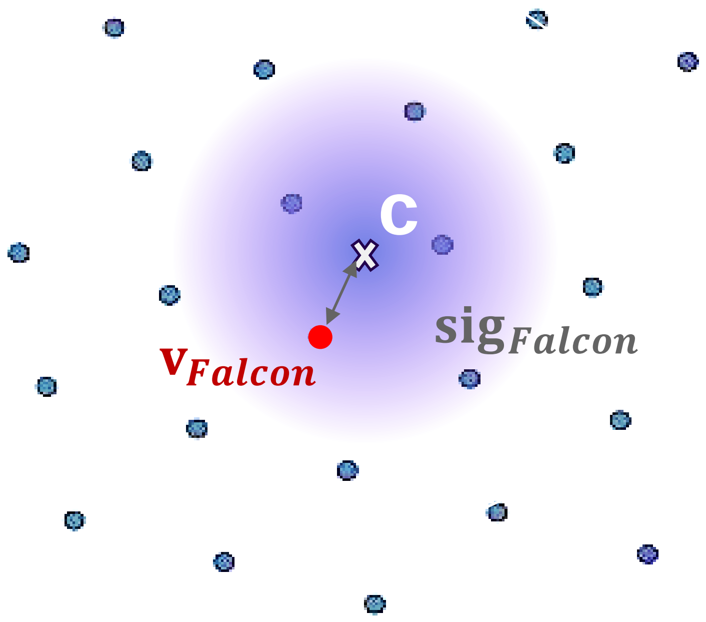


$\|\mathbf{sig}_F\| \propto \|\mathbf{sk}\|_{FFO} \approx 1.17\sqrt{q}$

$2.04\sqrt{q} \approx \|\mathbf{sk}\|_{hybrid} \propto \|\mathbf{sig}_M\|$

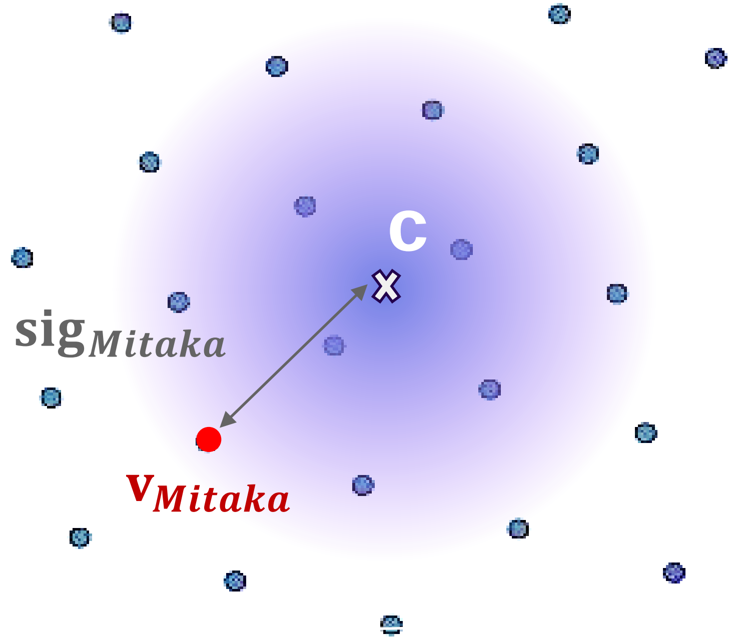
SAMPLER/SIGNATURE'S SIZE

Falcon



$<$

Mitaka



$\|\mathbf{sig}_F\| \propto \|\mathbf{sk}\|_{FFO} \approx 1.17\sqrt{q}$

$2.04\sqrt{q} \approx \|\mathbf{sk}\|_{hybrid} \propto \|\mathbf{sig}_M\|$

Quality α

QUALITY α AND TRAPDOOR GENERATION

The security of the scheme depends on the quality α of the **trapdoor**

$$\alpha = \frac{\|\mathbf{sk}\|}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $\|\cdot\|$ defined by the **sampler** .

Goal: reduce α.

QUALITY α AND TRAPDOOR GENERATION

The security of the scheme depends on the quality α of the **trapdoor**

$$\alpha = \frac{\|\mathbf{sk}\|}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $\|\cdot\|$ defined by the **sampler** .

Goal: reduce α.

› Observation: α only depends on f, g.

QUALITY α AND TRAPDOOR GENERATION

The security of the scheme depends on the quality α of the **trapdoor**

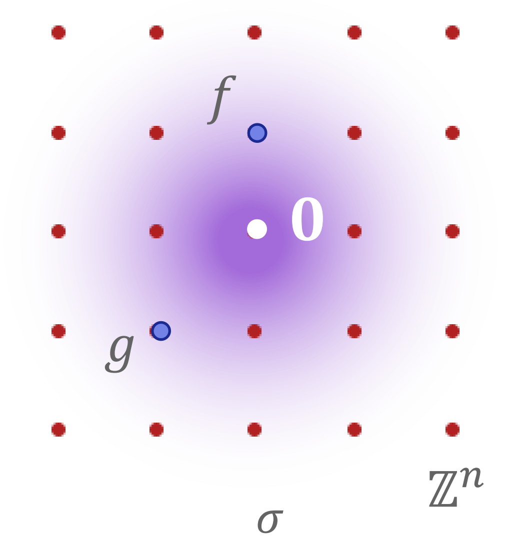
$$\alpha = \frac{\|\mathbf{sk}\|}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $\|\cdot\|$ defined by the **sampler** .

Goal: reduce α.

- Observation: α only depends on f, g.
- Falcon's method: Sample f, g from a small $D_{\mathbb{Z}^n,0,\sigma}$

  With a reasonable number of repetitions
  we can find f, g with $\|\mathbf{sk}\| \leq \alpha(\sigma)\sqrt{q}$.



QUALITY α AND TRAPDOOR GENERATION

The security of the scheme depends on the quality α of the **trapdoor**

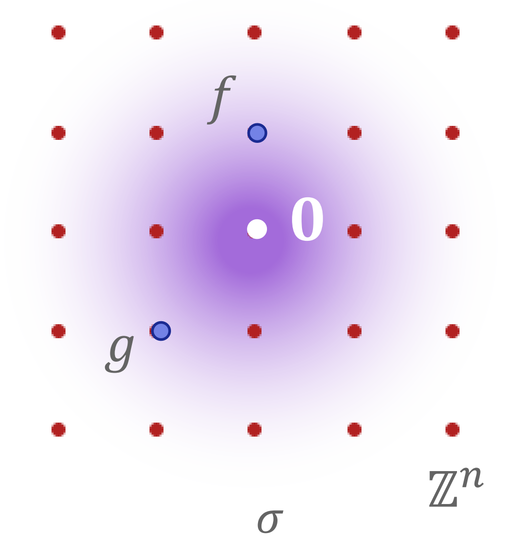
$$\alpha = \frac{\|\mathbf{sk}\|}{\sqrt{q}} = \frac{1}{\sqrt{q}} \left\| \begin{pmatrix} f & F \\ g & G \end{pmatrix} \right\|$$

with $\|\cdot\|$ defined by the **sampler** .

Goal: reduce α.

- Observation: α only depends on f, g.
- Falcon's method: Sample f, g from a small $D_{\mathbb{Z}^n,0,\sigma}$
  With a reasonable number of repetitions
  we can find f, g with $\|\mathbf{sk}\| \leq \alpha(\sigma)\sqrt{q}$.
- Our method:

ANTRAG: Annular Trapdoor Generation
$\alpha_{hybrid} = 1.14$



ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION

$$\mathbb{Z}^n \approx \mathcal{K} \ni \sum_n f_i x^i = f \xrightarrow{\text{DFT}} \big(f(\zeta_1), \cdots, f(\zeta_n)\big) \in \mathbb{C}^n$$

ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION

$$\mathbb{Z}^n \approx \mathcal{K} \ni \sum_n f_i x^i = f \xrightarrow{\text{DFT}} \big(f(\zeta_1), \cdots, f(\zeta_n)\big) \in \mathbb{C}^n$$

- For fixed $\alpha_{hybrid} = \alpha$, we want to find f, g such that for $\forall i \leq n$

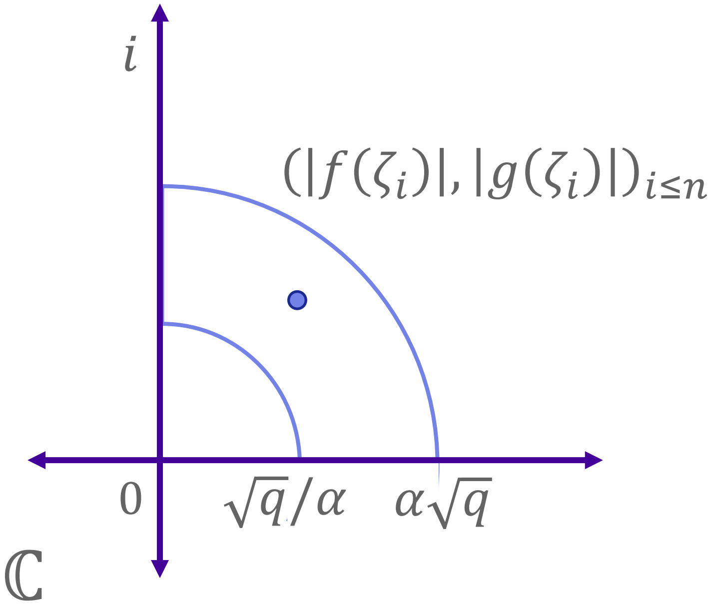
$$\frac{q}{\alpha^2} \leq |f(\zeta_i)|^2 + |g(\zeta_i)|^2 \leq \alpha^2 q$$

ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION

$$\mathbb{Z}^n \approx \mathcal{K} \ni \sum_n f_i x^i = f \xrightarrow{\text{DFT}} \left(f(\zeta_1), \cdots, f(\zeta_n)\right) \in \mathbb{C}^n$$

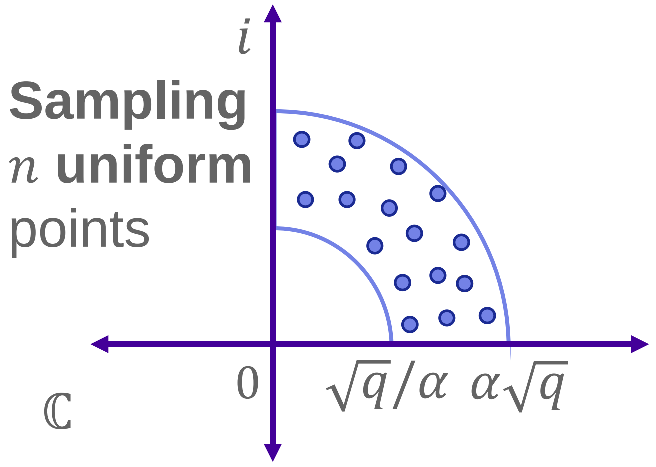
- For fixed $\alpha_{hybrid} = \alpha$, we want to find f, g such that for $\forall i \leq n$

$$\frac{q}{\alpha^2} \leq |f(\zeta_i)|^2 + |g(\zeta_i)|^2 \leq \alpha^2 q$$

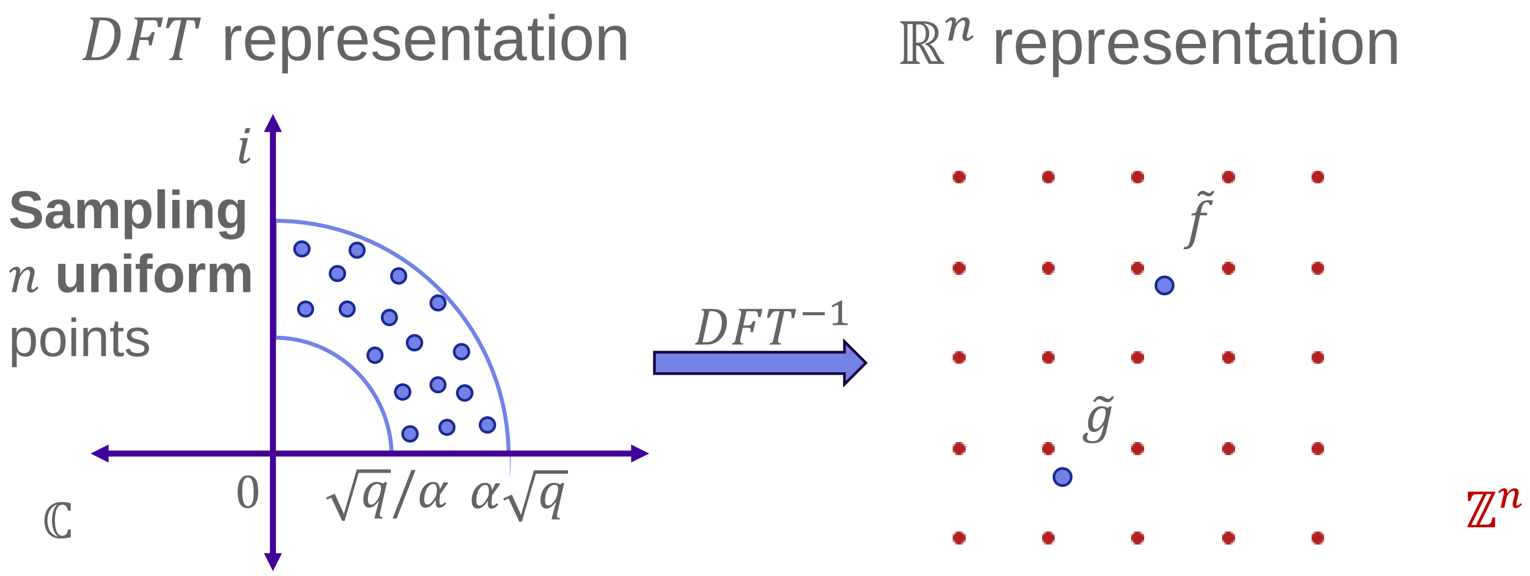


ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

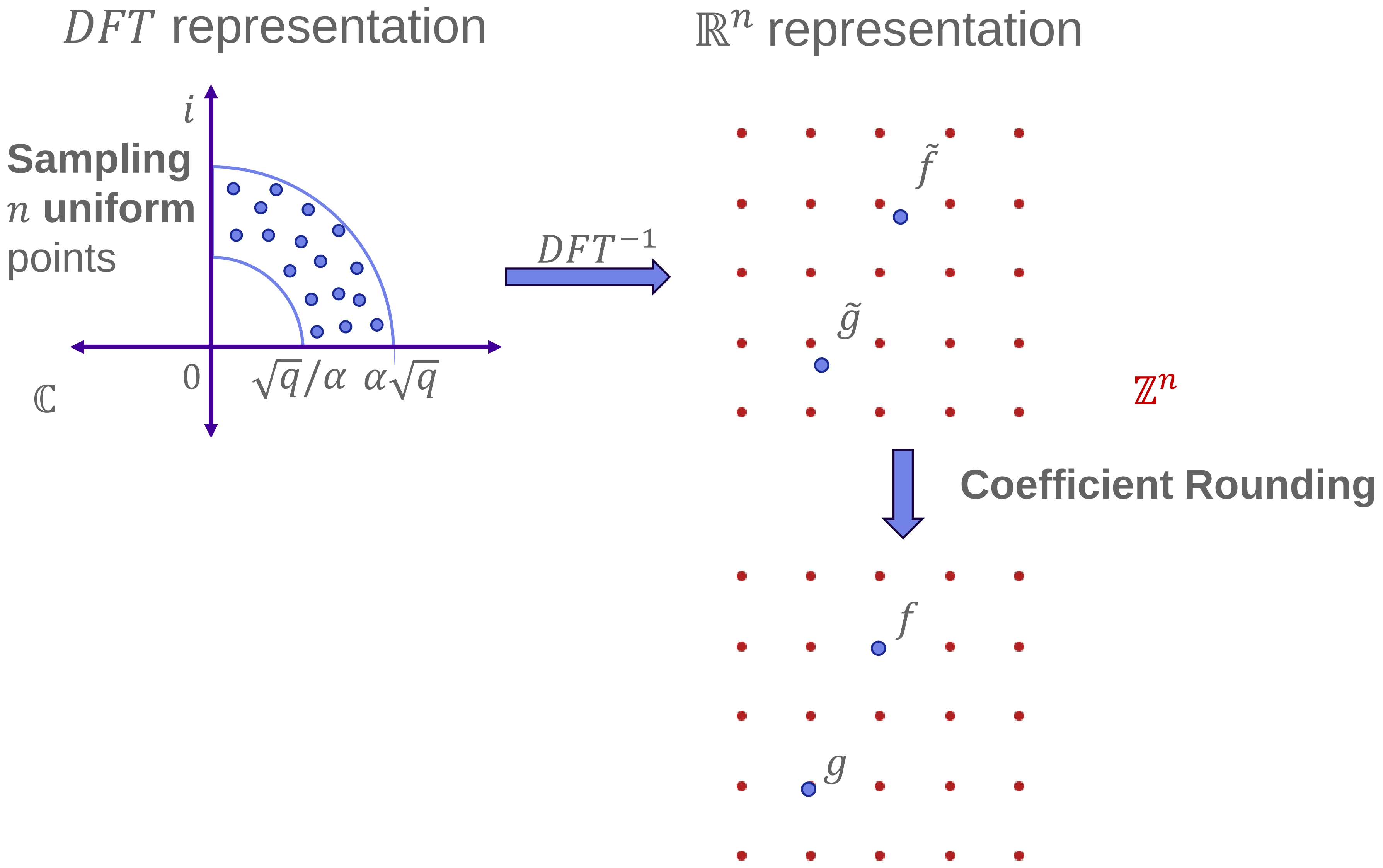
DFT representation



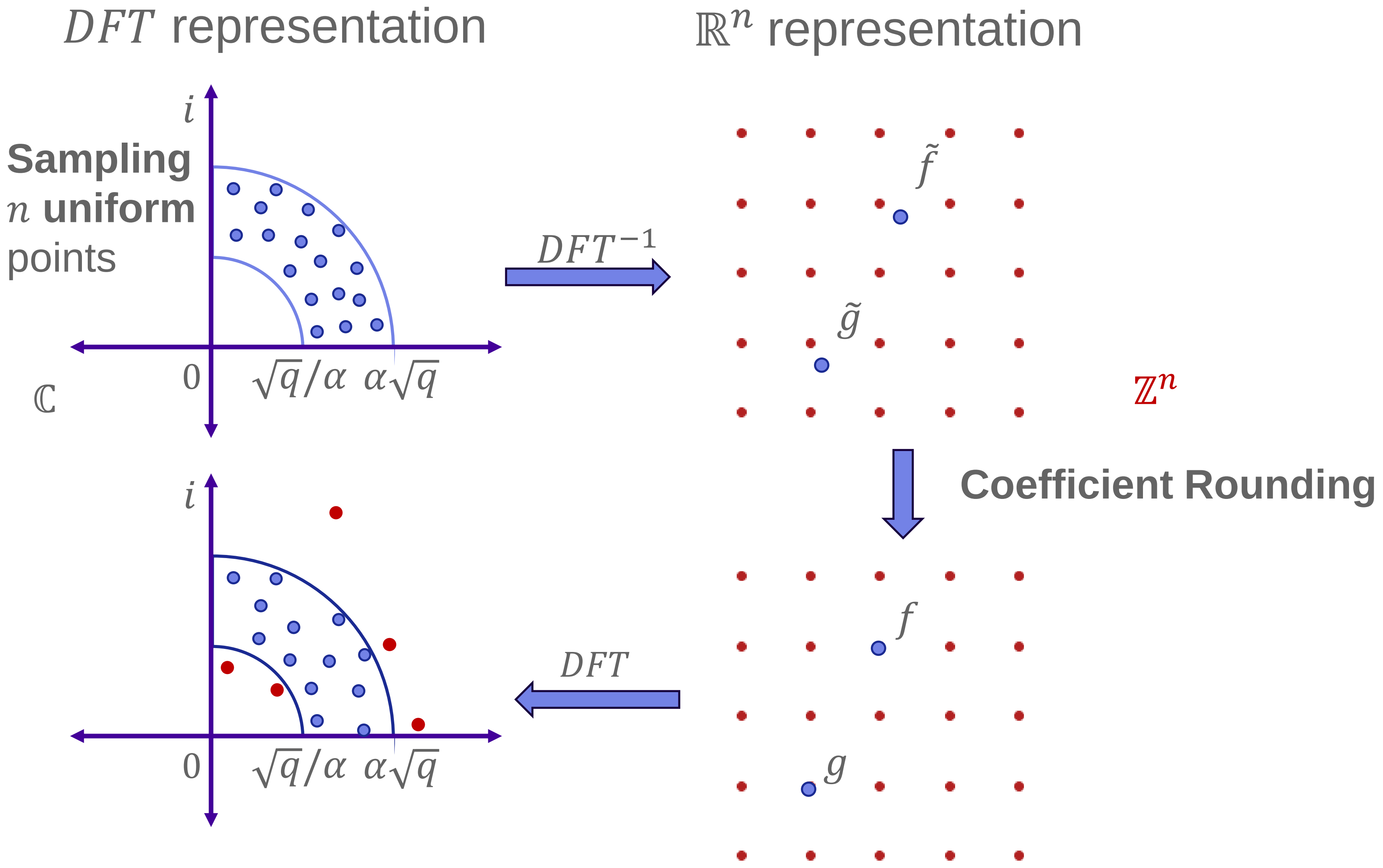
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)



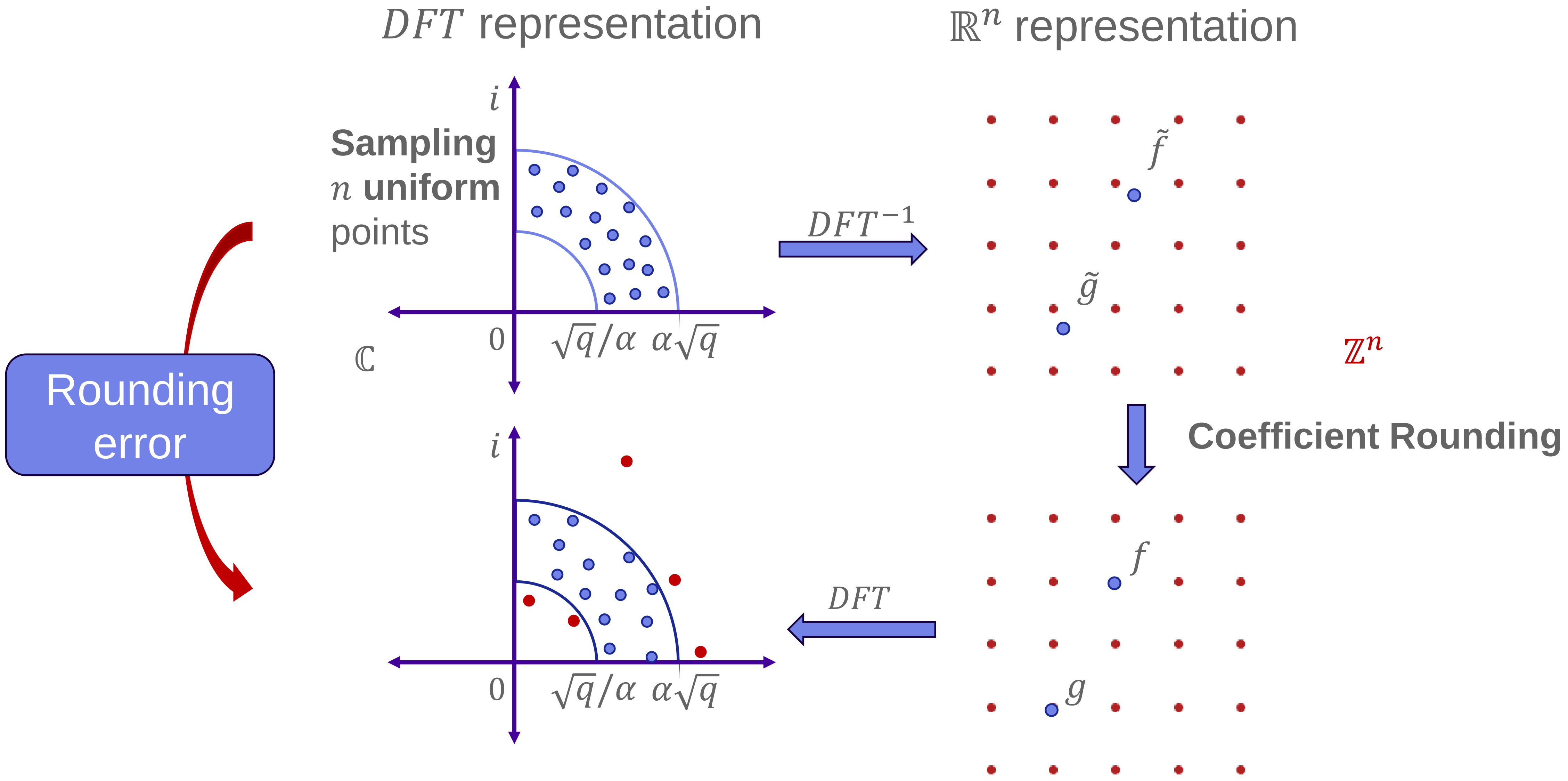
ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)



ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)

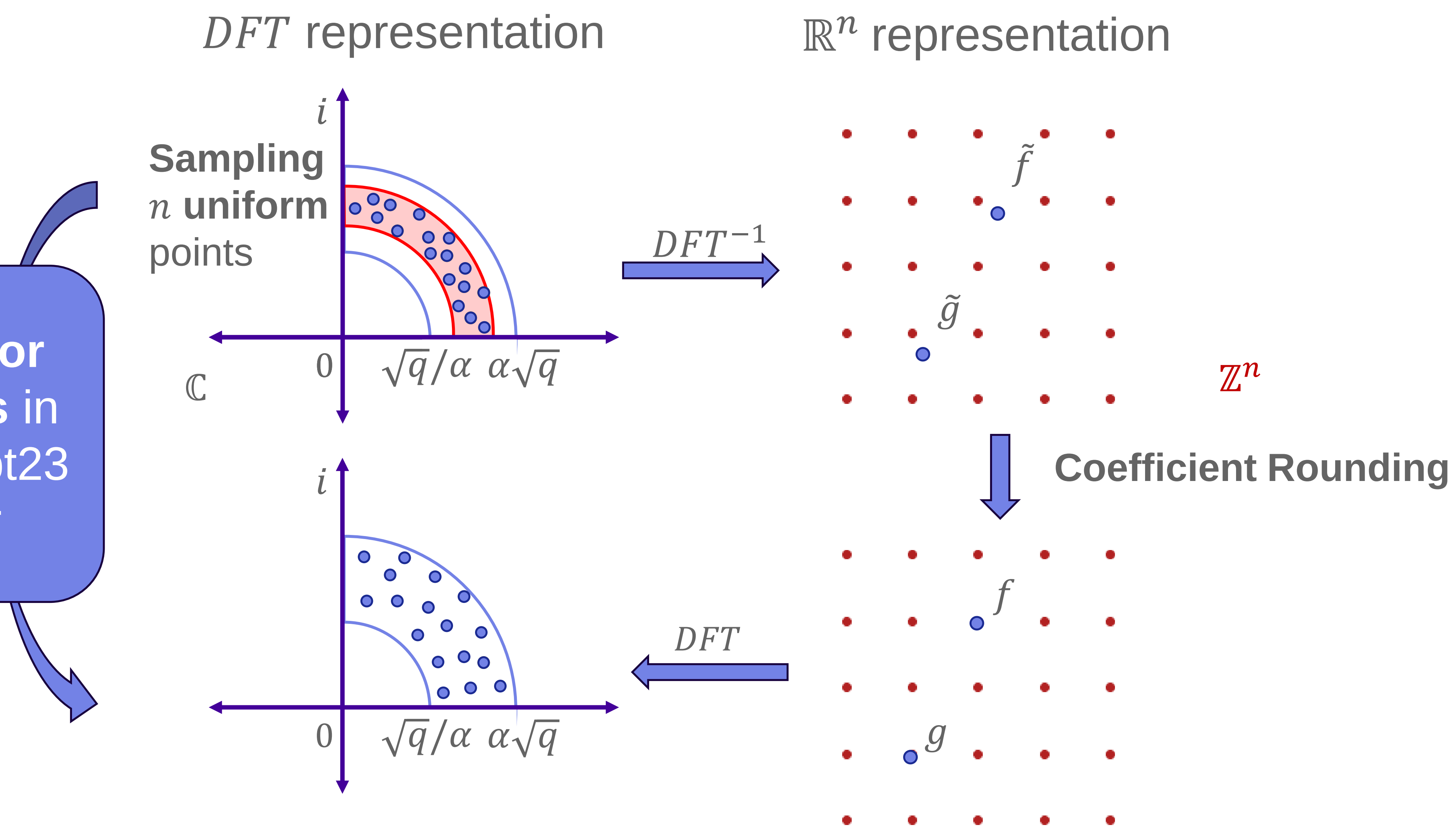


ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (1)



ANTRAG: ANNULAR NTRU TRAPDOOR GENERATION (2)

See **error analysis** in AsiaCrypt23 paper



SECURITY OF ANTRAG’S TRAPDOOR

› Formal security

- Same as Falcon

  → Security of keys : based on NTRU assumption

  → Security of signatures : based on GPV framework

SECURITY OF ANTRAG'S TRAPDOOR

〉Formal security

- Same as Falcon

  → Security of keys : based on NTRU assumption

  → Security of signatures : based on GPV framework

〉Concrete security

- Signature forgery:

  → Improved trapdoor for hybrid sampler => signature has the same security level as Falcon's

- Key recovery:

  → Usual attacks: same as Falcon

  → Attack from the structure of Antrag: voided due to rounding error

SECURITY OF ANTRAG'S TRAPDOOR

〉Formal security

- Same as Falcon

  → Security of keys : based on NTRU assumption

  → Security of signatures : based on GPV framework

〉Concrete security

- Signature forgery:

  → Improved trapdoor for hybrid sampler => signature has the same security level as Falcon's

- Key recovery:

  → Usual attacks: same as Falcon

  → Attack from the structure of Antrag: voided due to rounding error

ANTRAG's trapdoor has the same security level as FALCON's

PERFORMANCE: FALCON VS ANTRAG

	512			1024		
	Falcon	**Antrag-1r**	**Antrag-1s**	**Falcon**	**Antrag-5r**	**Antrag-5s**
Classical sec (bits)	123	123	**122**	284	284	**257**
Key size (bytes)	896	896	**768**	1792	1792	**1664**
Sign size (bytes)	666	666	**590**	1280	1280	**1208**
Keygen (ms)	6.4	**5.7**	**6.1**	19.1	19.1	**15.4**
Signing (μs)	202	**115**	**120**	399	**240**	**238**
Verification (μs)	27	**24**	**42**	58	**49**	**88**

› **Antrag-Xr parameters are fully compatible with Falcon**

- Same format for keys and signatures
- The verification algorithm of each accepts signatures from the other.

› **Antrag-Xs parameters are optimized for the signature’s size/security**

- Shorter keys and signatures while maintaining the same security level.

CONCLUSIONS

Antrag : Novel technique to generate high quality trapdoors for the hybrid Gaussian sampler

→ gives much simpler signature scheme with **improved performance** + no security loss

→ supports **all** NIST security levels (I to V)

→ achieves full verification compatibility with Falcon **or** shorter keys and signatures.

ia.cr/2023/1335

github.com/mti/antrag_opt

THANK YOU!