Smooth (or Not So Smooth) Lattice Sampling

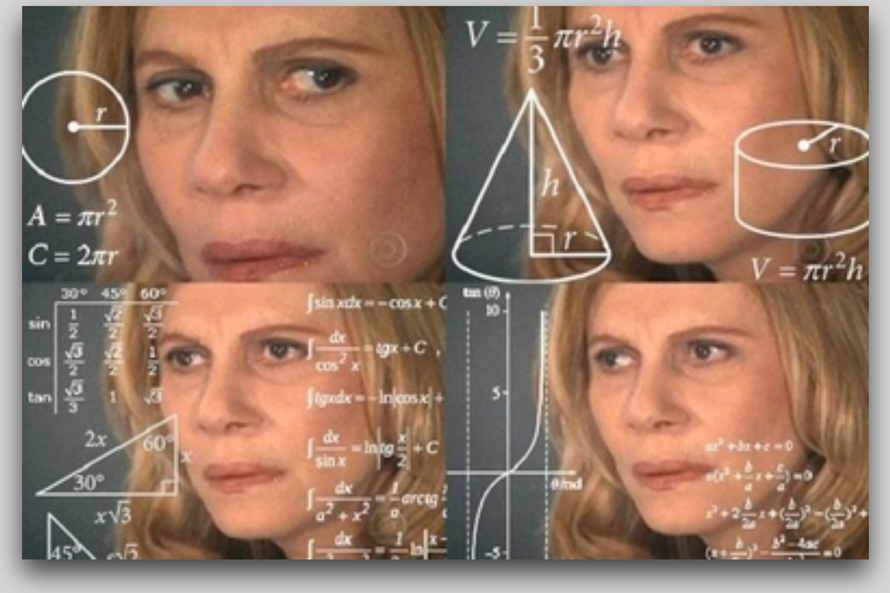
Maiara F. Bollauf

joint work with Maja Lie & Cong Ling

FOUNDATIONS SEMINAR - UNIVERSITY OF TARTU

Outline

- Mathematics of cryptography
- Why and how to sample from lattices?
- State of the art



Cryptography

Behind every secure cryptosystem lies a mathematical problem that must be hard to solve

Cryptography

RSA

Hard problem: Decomposition of a number into prime factors

Given $N = pq$, where p and q are large primes,

find p and q given just N

Cryptography

Elliptic-Curve Cryptography

Hard problem: The discrete logarithm problem

Given G a finite group, $a \in G$, and $b \in \langle a \rangle$

find a positive integer x such that $a^x = b$

Cryptography

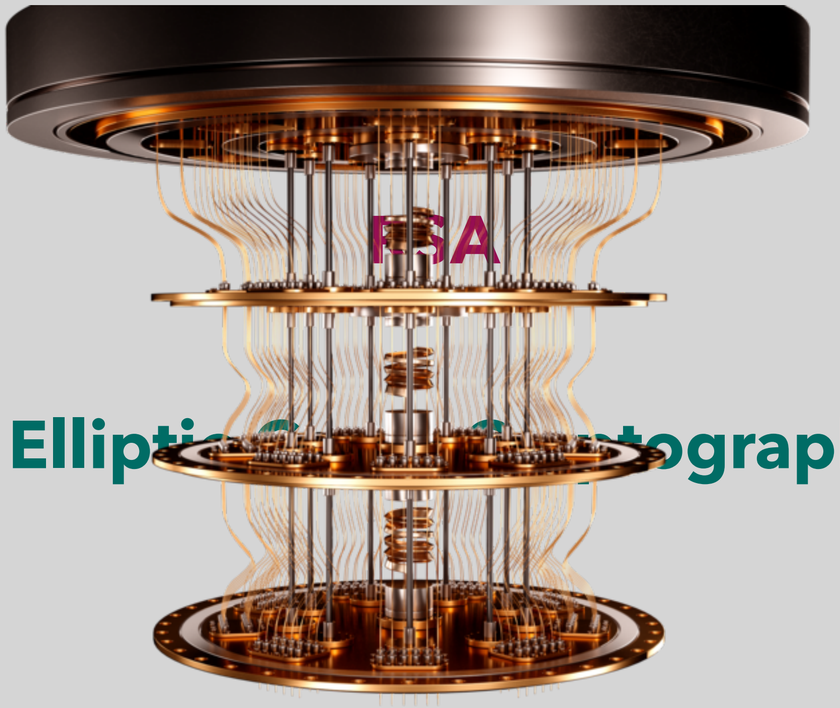
Peter Shor

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

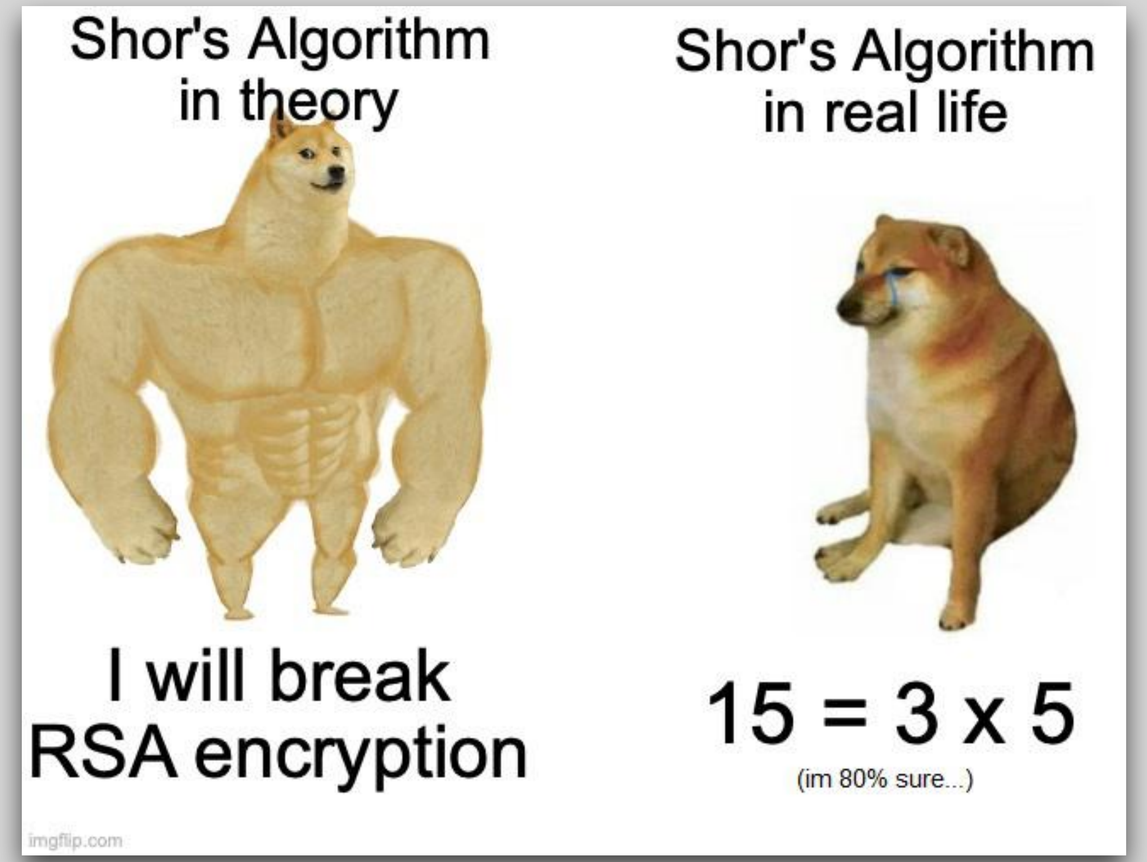
1994

Cryptography



Elliptic Curve Cryptography

Cryptography



Source: Reddit - https://images.app.goo.gl/FTyyeF1reNgppc2f9

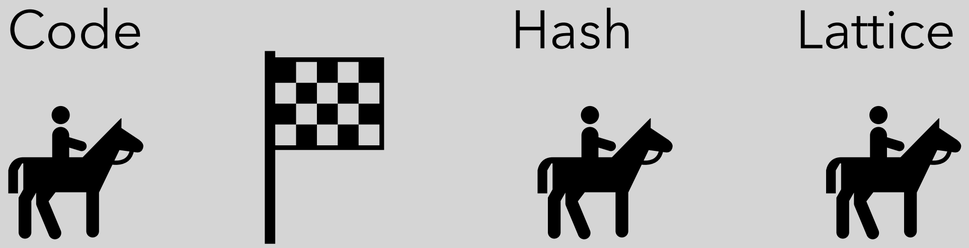
Post-Quantum Cryptography

NIST (*National Institute of Standards and Technology*) proposed a standardization process for post-quantum cryptography in 2016

Post-Quantum Cryptography

The selected algorithms were announced in 2022

and published in 2024

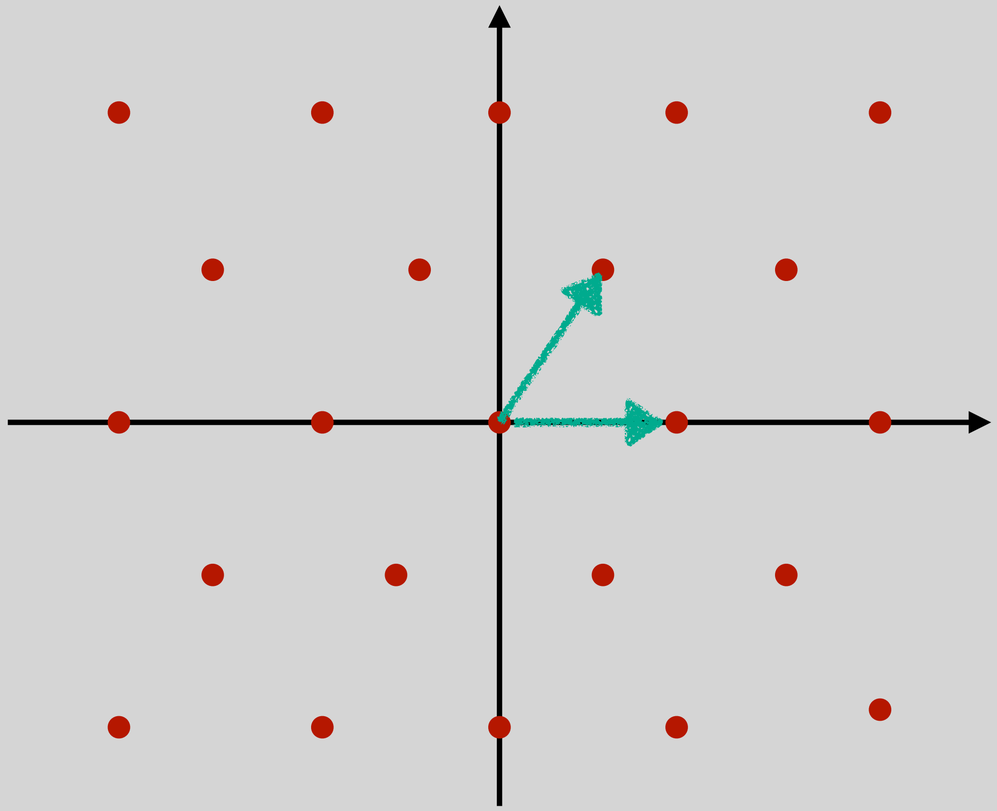


Post-Quantum Cryptography

Type	PKE/KEM	Signature
Lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
Hash-based		SPHINCS+

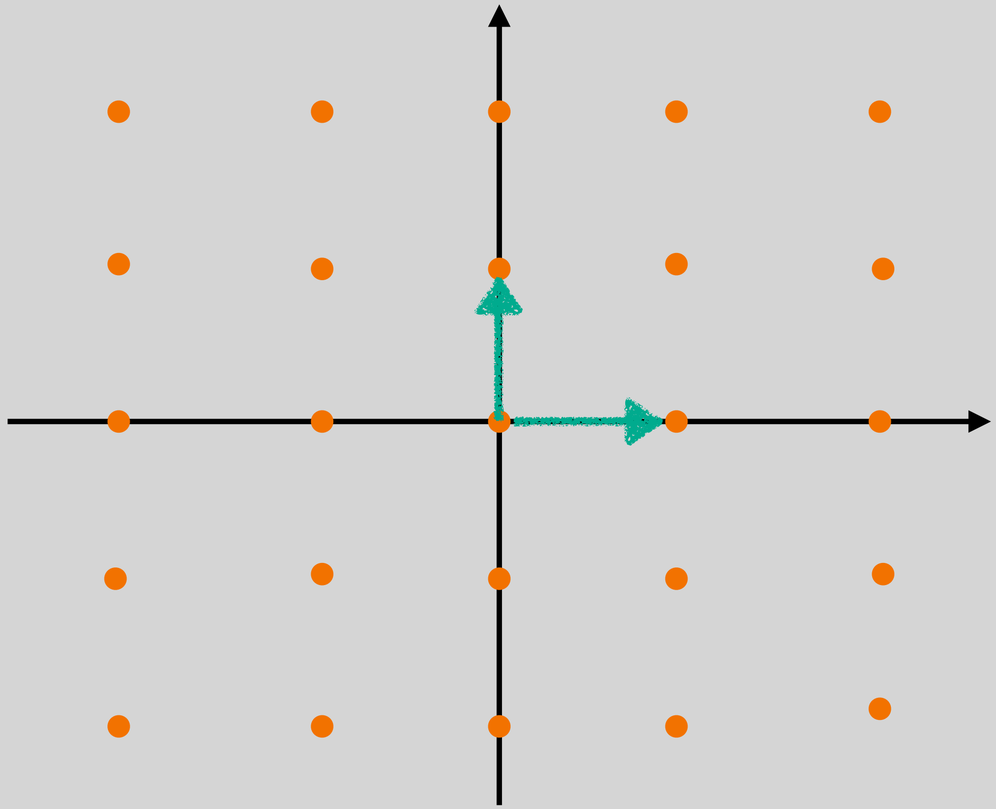
Lattice

Discrete additive subgroup of $\mathbb{R}^n$.

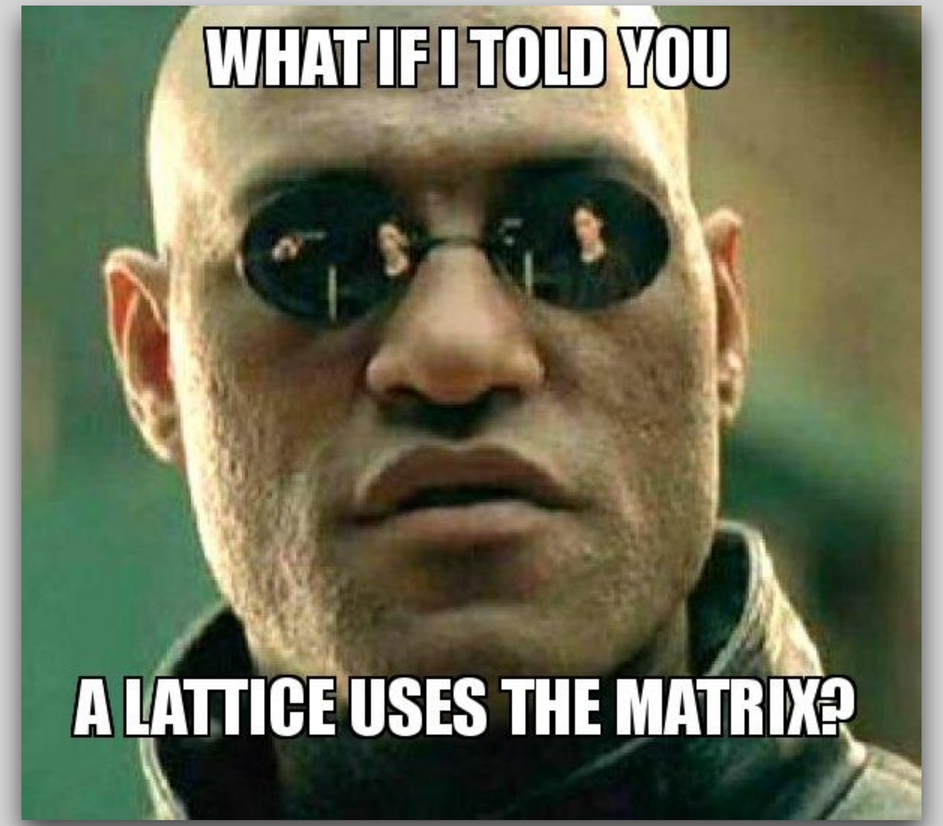


Lattice

For crypto applications, subgroups of $\mathbb{Z}^n$ are complicated enough.



Lattice

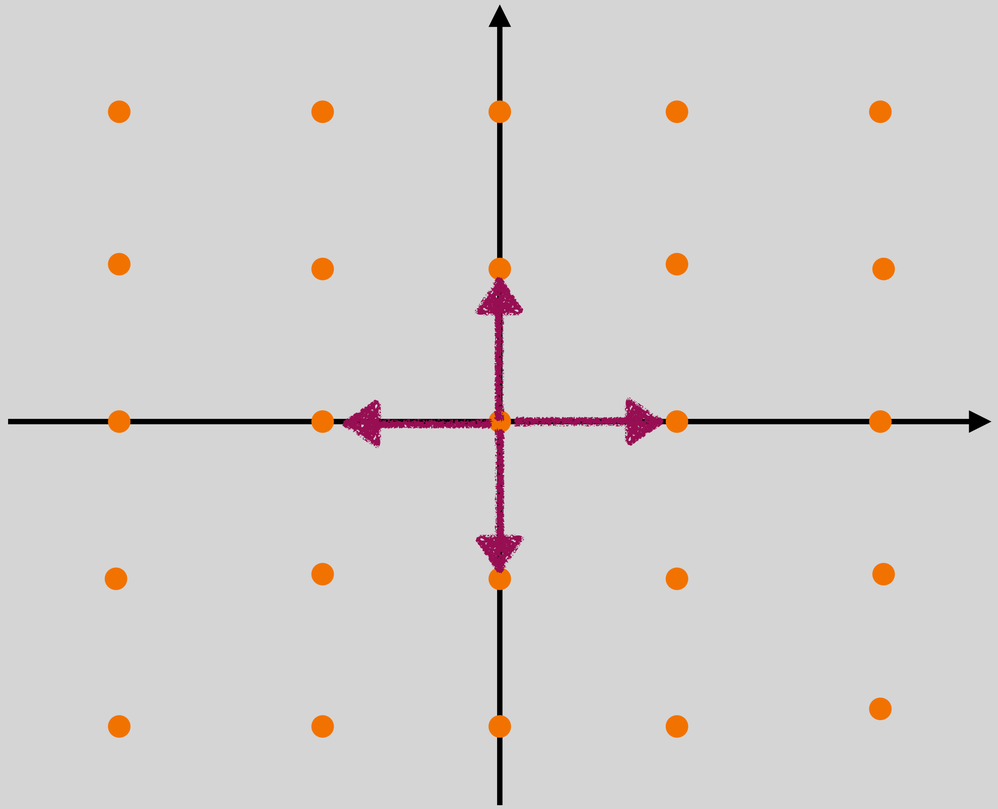


Source: https://images.app.goo.gl/ExdgiqxX1stUkgXDA

Hard Problems on Lattices

SVP (Shortest Vector Problem)

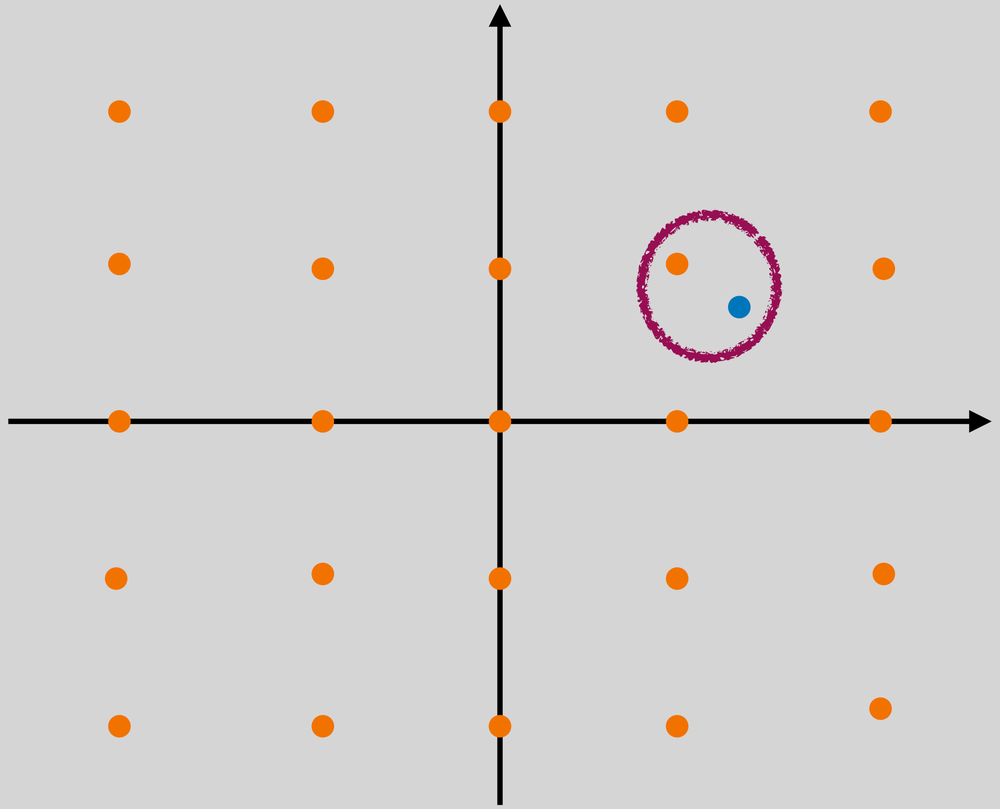
Given a lattice Λ, find a lattice vector with the smallest Euclidean norm.



Hard Problems on Lattices

CVP (Closest Vector Problem):

Given a lattice Λ and a real vector $\mathbf{v}$, find the lattice vector closest to $\mathbf{v}$.



Hard Problems on Lattices

And many others…

- **LWE** (**L**earning **w**ith **E**rrors)
- **LIP** (**L**attice **I**somorphism **P**roblem)
- **SIS** (**S**hort **I**nteger **S**olution)
- **SIVP** (**S**hortest **I**ndependent **V**ectors **P**roblem)
- **SBP** (**S**hortest **B**asis **P**roblem)
- …

Sampling

// The act, process or technique of selecting a suitable sample for the purpose of determining parameters or characteristics of the whole”

Sampling for Lattices

Given a lattice Λ, a vector $\mathbf{c} \in \mathbb{R}^n$ and $s > 0$,

a sampler is a randomized decoder that outputs a lattice vector

relatively close to $\mathbf{c}$

Sampling for Lattices

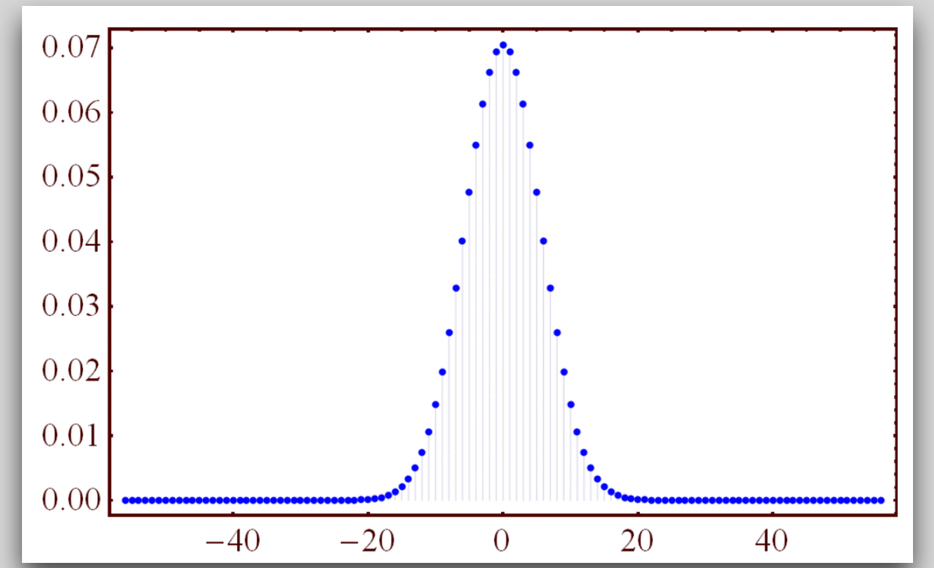
The **discrete Gaussian distribution** on a lattice Λ with parameter s

and center $\mathbf{c} \in \mathbb{R}^n$ is the distribution that assigns to each

point $\mathbf{x} \in \Lambda$ mass proportional to $e^{-\pi\|\mathbf{x}-\mathbf{c}\|^2/s^2}$

$D_{\Lambda,\mathbf{c},s}$

Sampling for Lattices



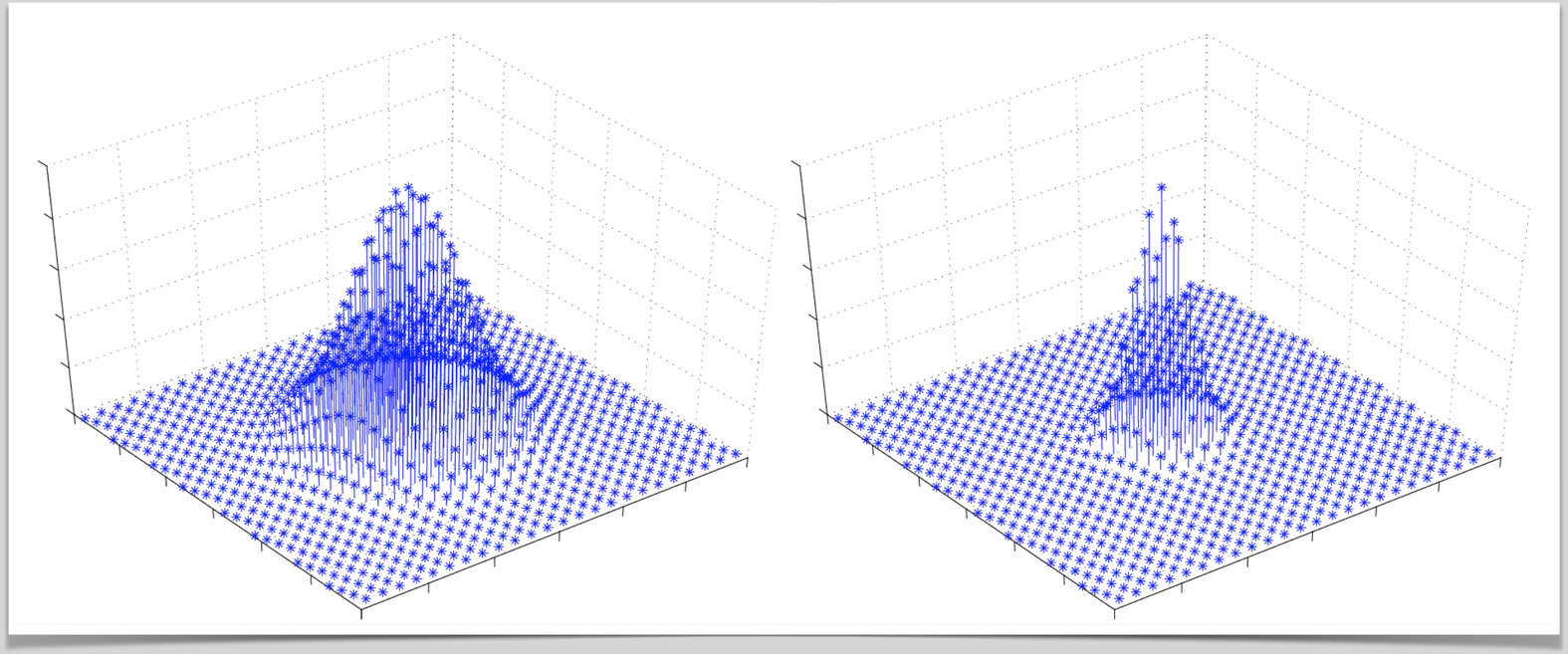
O. Regev, *The Learning with Errors Problem* , 2010

$$D_{\mathbb{Z}_{113},s=5.65}$$

Sampling for Lattices

$D_{\Lambda,2}$, $D_{\Lambda,1}$

for a 2D lattice Λ



O. Regev, *The Learning with Errors Problem* , 2010

Samples from $D_{\Lambda,s}$ are lattice vectors of norm $\sqrt{n}s$, considering that s is not too small

Sampling for Lattices

Continuous Gaussian

Discrete Gaussian

$$\mathbf{x} \sim \text{Gauss}(s) \rightarrow \frac{\mathbf{x}}{2} \sim \text{Gauss}\,(s/2)$$

$$\mathbf{y} \sim D_{\Lambda,s} \nrightarrow \frac{\mathbf{y}}{2} \sim D_{\Lambda,s/2}$$

$$\mathbf{x}_1, \mathbf{x}_2 \sim \text{Gauss}(s) \rightarrow \frac{\mathbf{x}_1 + \mathbf{x}_2}{2} \sim \text{Gauss}\left(\sqrt{s}/2\right)$$

$$\mathbf{y}_1, \mathbf{y}_2 \sim D_{\Lambda,s} \nrightarrow \frac{\mathbf{y}_1 + \mathbf{y}_2}{2} \sim D_{\Lambda,\sqrt{s}/2}$$

Smoothing Parameter

For any n-dimensional lattice Λ and a positive real $\varepsilon > 0$,

the **smoothing parameter** $\eta_\varepsilon(\Lambda)$ is the smallest $s > 0$ such that

$$\sum_{\mathbf{x} \in \Lambda^* \setminus \{\mathbf{0}\}} e^{-\pi s^2 \|\mathbf{x}\|^2} \leq \varepsilon$$

$\Lambda^* = \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z},\ \forall \mathbf{x} \in \Lambda\}$ is the dual lattice

Smoothing Parameter

For any n-dimensional lattice Λ and a positive real $\varepsilon > 0$,

the **smoothing parameter** $\eta_\varepsilon(\Lambda)$ is the smallest $s > 0$ such that

$$\sum_{\mathbf{x} \in \Lambda^* \setminus \{\mathbf{0}\}} e^{-\pi s^2 \|\mathbf{x}\|^2} \leq \varepsilon$$

Not trivial to calculate/estimate

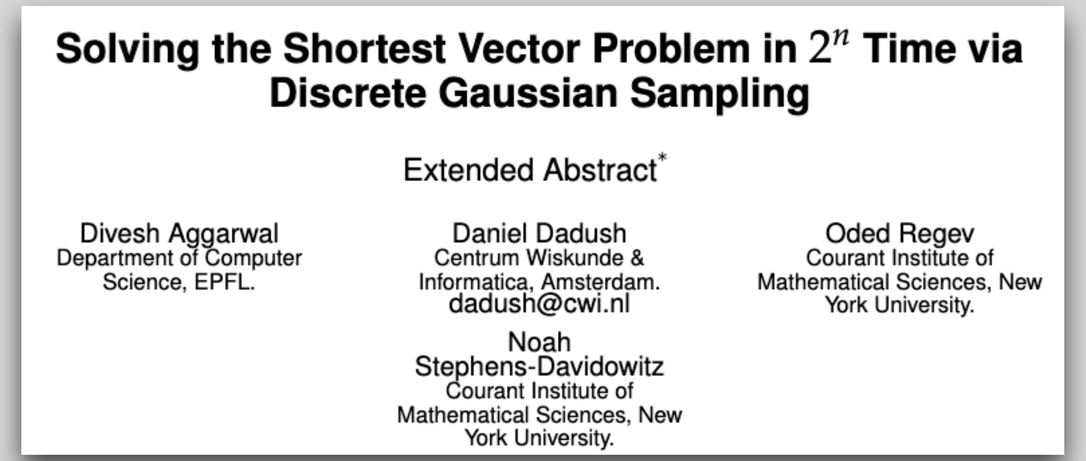
My favorite lattice measure: the theta series

Smoothing Parameter

- It is the minimal amount of noise such that the result is distributed almost uniformly at random
- For large enough s, the discrete Gaussian distribution resembles the continuous Gaussian distribution

Why to Sample?

Small sampling width s



Solving the Shortest Vector Problem in 2^n Time via Discrete Gaussian Sampling

Extended Abstract*

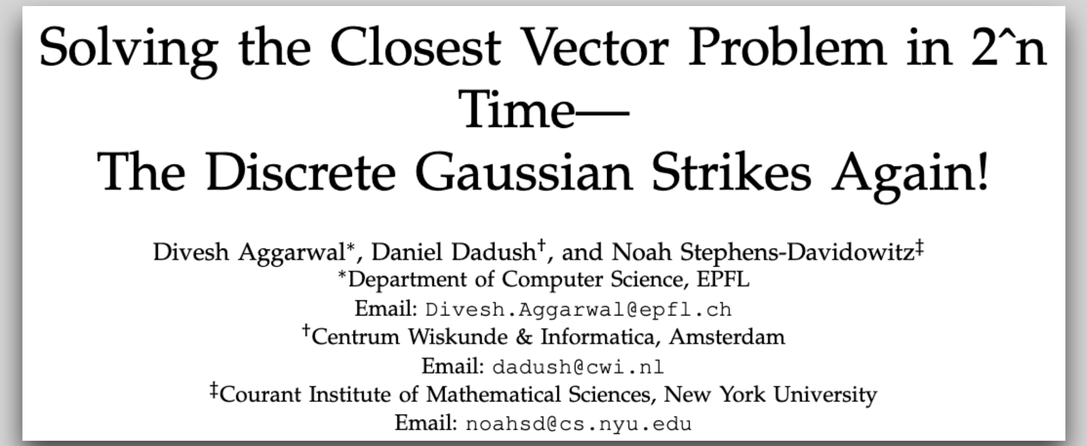
Divesh Aggarwal
Department of Computer Science, EPFL.

Daniel Dadush
Centrum Wiskunde & Informatica, Amsterdam.
dadush@cwi.nl

Noah Stephens-Davidowitz
Courant Institute of Mathematical Sciences, New York University.

Oded Regev
Courant Institute of Mathematical Sciences, New York University.

STOC'15



Solving the Closest Vector Problem in 2^n Time—
The Discrete Gaussian Strikes Again!

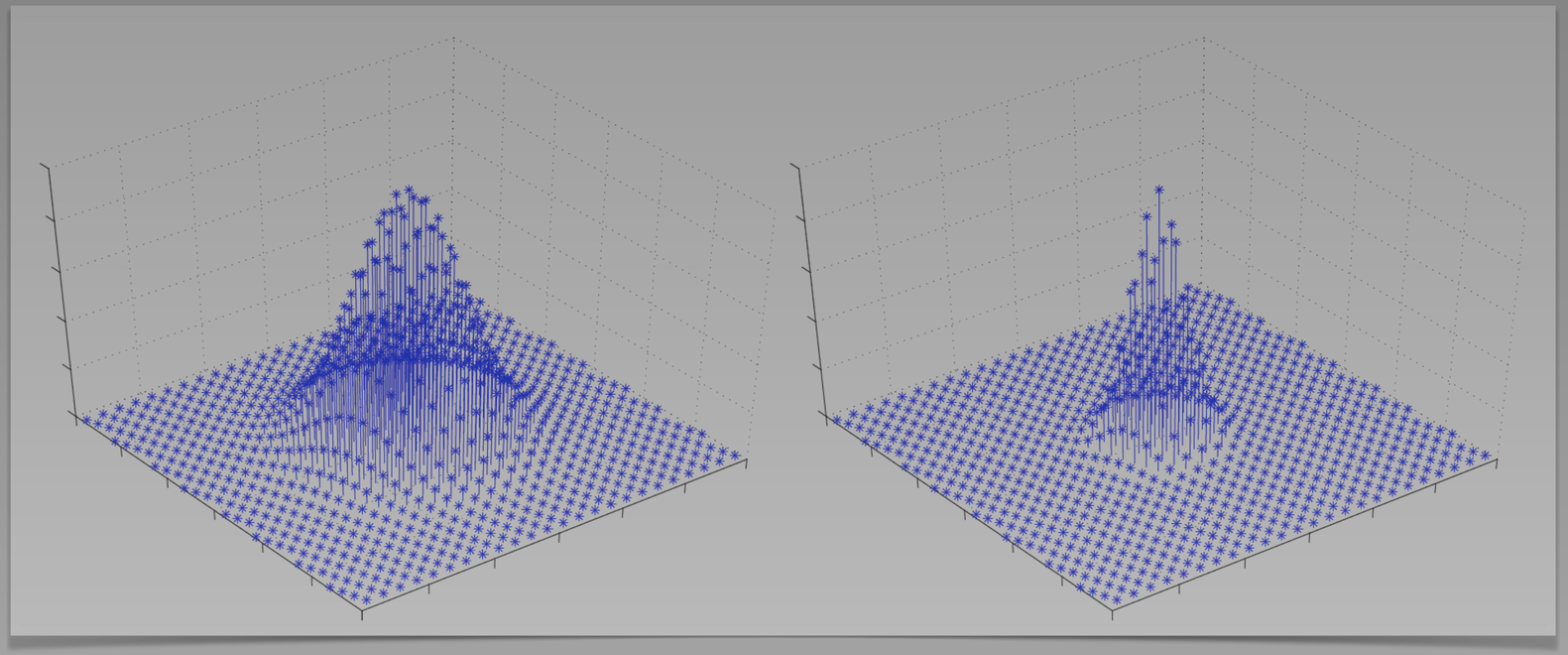
Divesh Aggarwal*, Daniel Dadush†, and Noah Stephens-Davidowitz‡
*Department of Computer Science, EPFL
Email: Divesh.Aggarwal@epfl.ch
†Centrum Wiskunde & Informatica, Amsterdam
Email: dadush@cwi.nl
‡Courant Institute of Mathematical Sciences, New York University
Email: noahsd@cs.nyu.edu

FOCS'15

Sampling for Lattices

$D_{\Lambda,2}$, $D_{\Lambda,1}$

for a 2D lattice Λ

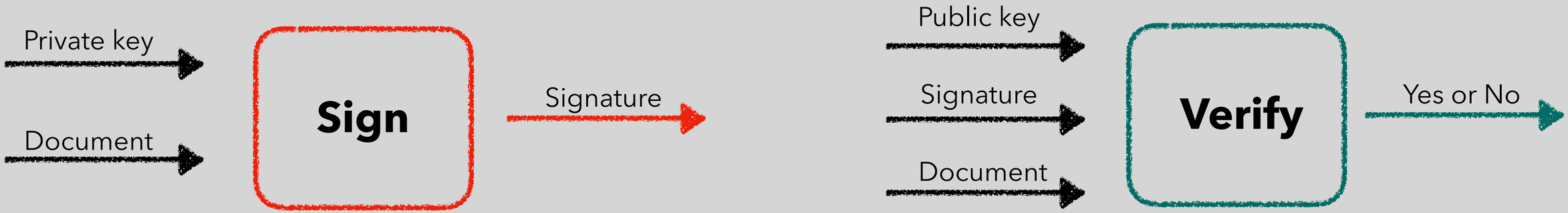


O. Regev, *The Learning with Errors Problem* , 2010

Samples from $D_{\Lambda,s}$ are lattice vectors of norm $\sqrt{n}s$, considering that s is not too small

Why to Sample?

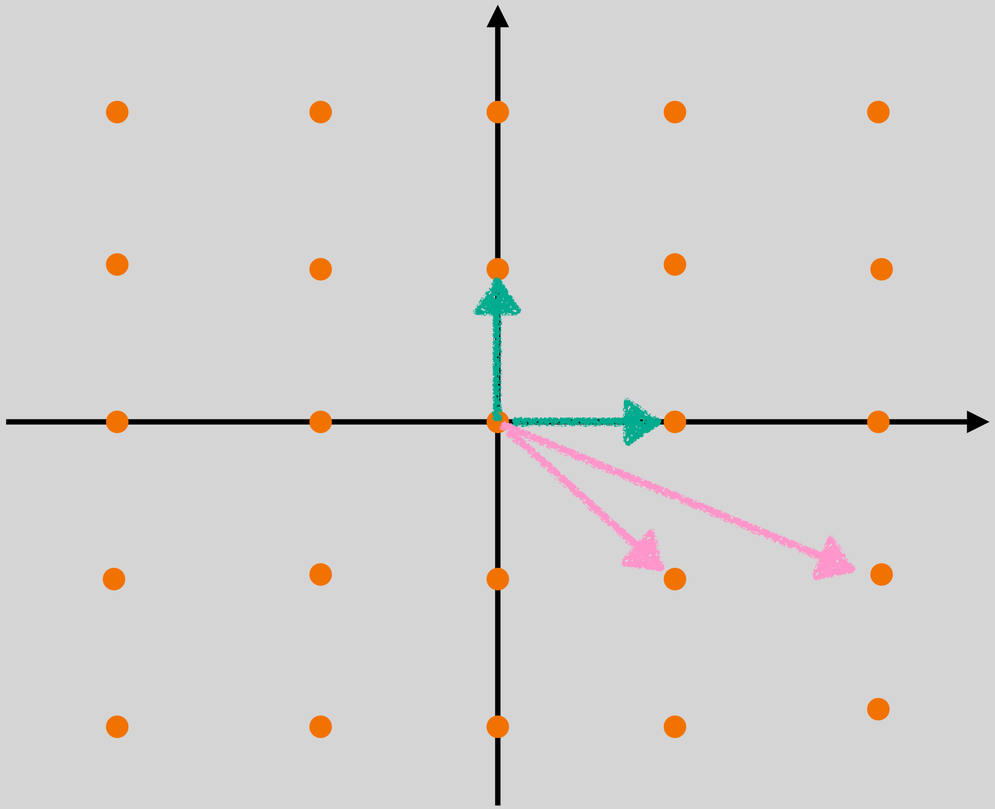
Applications in digital signature schemes



Verify(PubKey, Sig, Doc) = YES ⟷ Sig=Sign(PrivKey,Doc)

Why to Sample?

Some broken signature schemes were using only the geometry of the lattice basis for signing



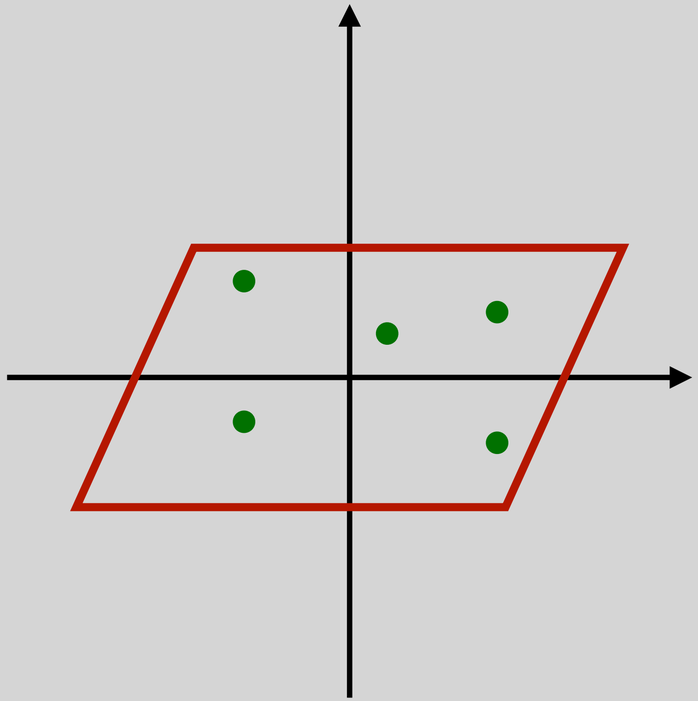
Geometry of the basis

$\neq$

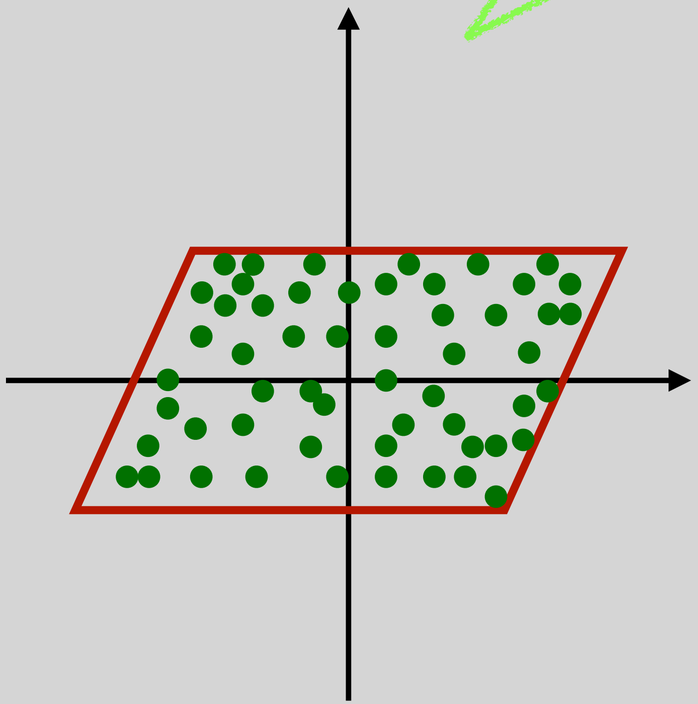
Geometry of the lattice

Why to Sample?

One can get enough information to guess the secret basis!



Few signatures



Lots of signatures

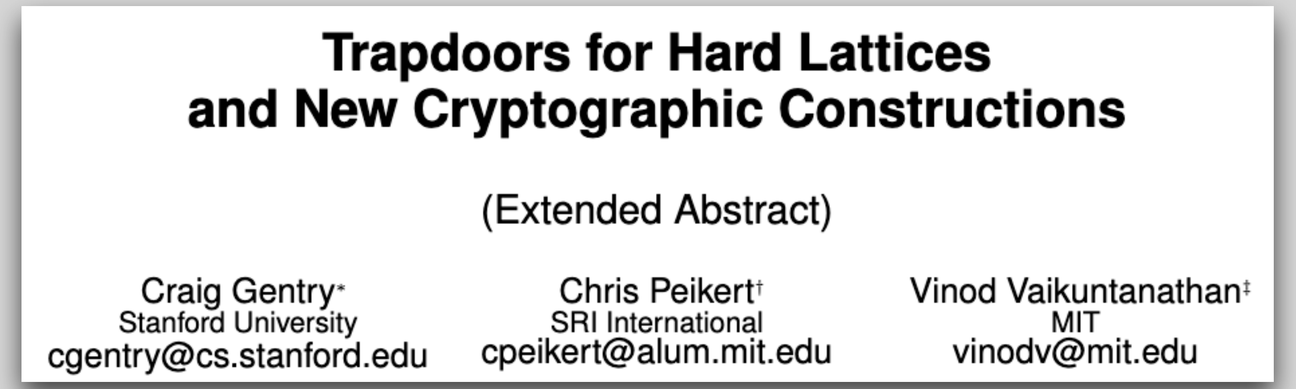
Why to Sample?

Ideal signature schemes are based on

functions that do not reveal the good basis geometry

Why to Sample?

Applications in digital signature schemes: [GPV08]



Trapdoors for Hard Lattices and New Cryptographic Constructions

(Extended Abstract)

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

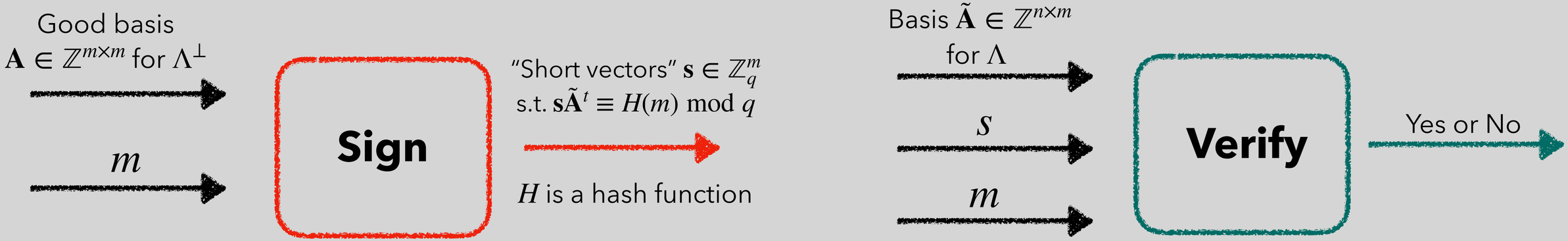
Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu

STOC'08

- "Hash-then-sign" signature scheme
- Requires sampling from a discrete Gaussian where s is the length of the longest Gram-Schmidt vector of the basis

Why to Sample?

Applications in digital signature schemes: [GPV08]



Compute $\mathbf{t} \in \mathbb{Z}_q^m$ s.t. $\mathbf{t}\tilde{\mathbf{A}}^t \equiv H(m) \bmod q$

Find a vector $\mathbf{v} \in \Lambda(\mathbf{A})$ "close" to $\mathbf{t}$

The signature is $\mathbf{s} = \mathbf{t} - \mathbf{v}$

Gaussian sampling

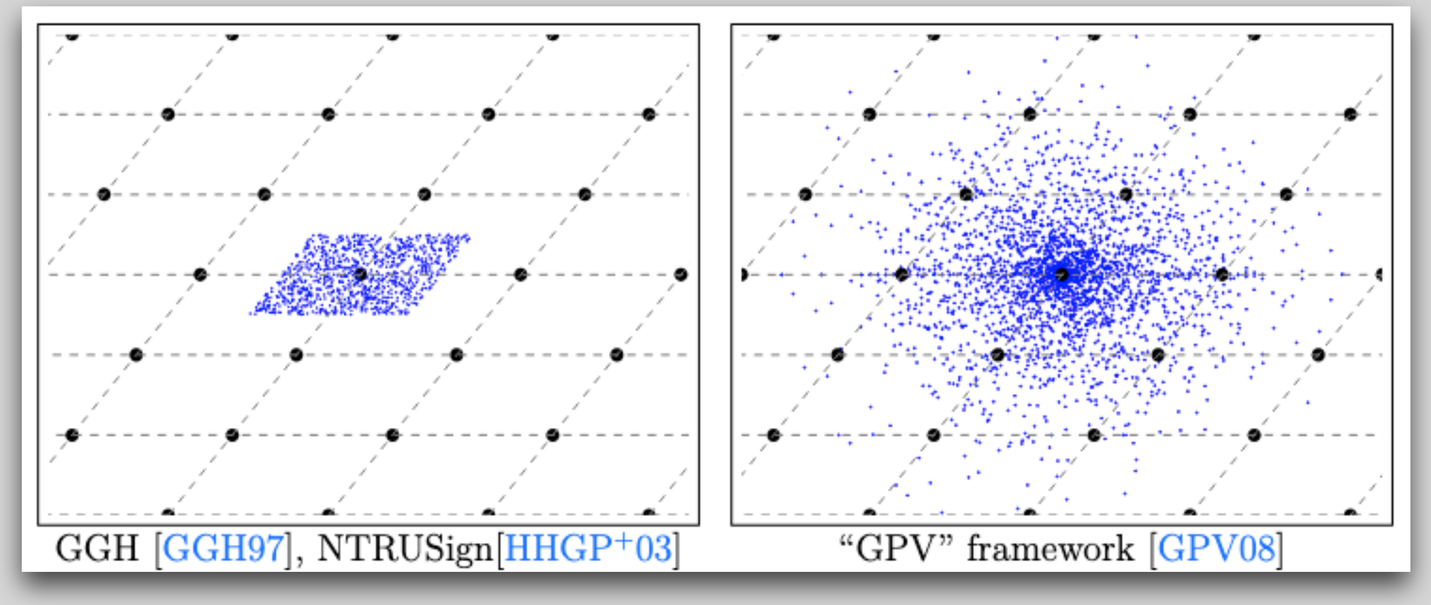
Use $\tilde{\mathbf{A}}$ to check that $\mathbf{s}\tilde{\mathbf{A}}^t \equiv H(m) \bmod q$

Check that $\|\mathbf{s}\|$ is small

$\mathbf{A}\tilde{\mathbf{A}}^t \equiv \mathbf{0} \bmod q$

Why to Sample?

Applications in digital signature schemes: [GPV08]



Thomas Prest, *Gaussian Sampling in Lattice-Based Cryptography*, PhD Thesis, 2015

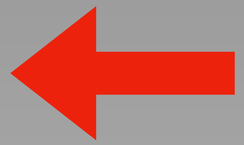
Why to Sample?

Applications in digital signature schemes: [GPV08]

- The smaller $\|\mathbf{s}\|$, the harder to forge signatures
- The better the secret basis, the smaller the samples
- Their sample is efficient for $s \gg \lambda_1(\Lambda)$, above the smoothing parameter

Post-Quantum Cryptography

Type	PKE/KEM	Signature
Lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
Hash-based		SPHINCS+



Why to Sample?

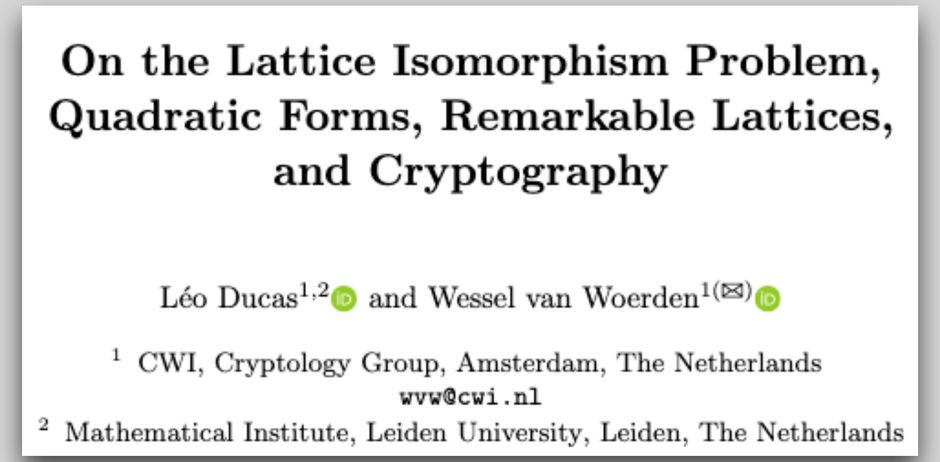
Applications in digital signature schemes: FALCON

uses the [GPV08] framework on NTRU lattices

Why to Sample?

"Our signature scheme can be instantiated with any lattice for which we can sample efficiently at small Gaussian widths"

Applications in digital signature schemes: [DW22]



On the Lattice Isomorphism Problem, Quadratic Forms, Remarkable Lattices, and Cryptography

Léo Ducas[1,2] and Wessel van Woerden[1(✉)]

[1] CWI, Cryptology Group, Amsterdam, The Netherlands
wvw@cwi.nl
[2] Mathematical Institute, Leiden University, Leiden, The Netherlands

EUROCRYPT'22

- Signature scheme based on Gaussian sampling
- Does not depend on Gram-Schmidt or Cholesky matrices

Why to Sample?

Applications in digital signature schemes: [DW22]

Compute $\mathbf{t} \leftarrow H(m)$

Sample $\mathbf{s}' \leftarrow D_{\mathbb{Z}^n, \rho/\sqrt{n}, U\mathbf{t}}$

Compute $\mathbf{s} \leftarrow U^{-1}\mathbf{s}'$, $\mathbf{s} \in \mathbb{Z}^n$

Gaussian sampling with width $\rho/\sqrt{n}$

Compute $\mathbf{t} \leftarrow H(m)$

$$b = \begin{cases} 1, \text{ if } \mathbf{s} \in \mathbb{Z}^n \text{ and } \|\mathbf{t} - \mathbf{s}\| \leq \rho \\ 0, \text{ otherwise} \end{cases}$$

A Core Memory

s

Reveals the lattice structure

Could solve hard lattice problems

s

Smoothing parameter

Ideal sampling width

S

Easier to forge signatures

Lattice-based signature schemes rely on being able to sample efficiently

What Is Known About Sampling?

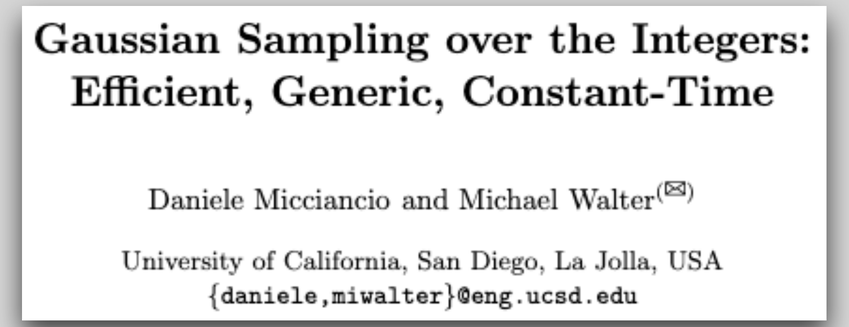
Finding the closest lattice vector when it's unusually close

Philip Klein*
Brown University

SODA'00

Works well for $s \geq \eta_\varepsilon(\mathbb{Z}) \max_i \|\mathbf{b}_i^*\|$,
where $\mathbf{B}^*$ is an orthogonal basis for the lattice

What Is Known About Sampling?



Gaussian Sampling over the Integers: Efficient, Generic, Constant-Time

Daniele Micciancio and Michael Walter(✉)

University of California, San Diego, La Jolla, USA
{daniele,miwalter}@eng.ucsd.edu

CRYPTO'17

- Works well for the $\mathbb{Z}^n$ lattice using one-dimensional samplers
- It is commonly used as subroutine for other lattices

What Is Known About Sampling?

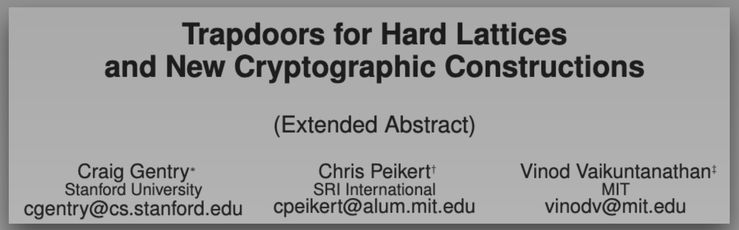
ON GAUSSIAN SAMPLING, SMOOTHING PARAMETER
...
APPLICATION TO LATTICE SIGNATURES

THOMAS ESPITAU*, ALEXANDRE WALLET*, AND YANG YU†

ASIACRYPT'23

- Works well for known families of lattices, such as root lattices
- The sampling width can be set to the smoothing parameter, but it relies on approximations
- Best results are for 2D lattice A_2

What Is Known About Sampling?



Trapdoors for Hard Lattices and New Cryptographic Constructions

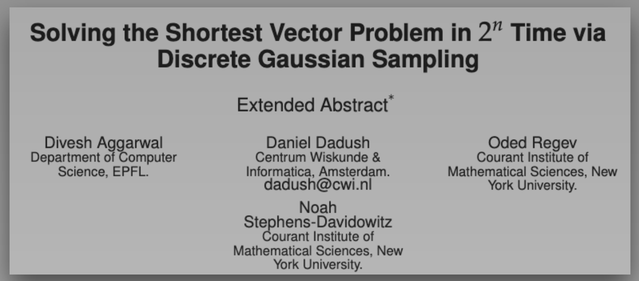
(Extended Abstract)

Craig Gentry*
Stanford University
cgentry@cs.stanford.edu

Chris Peikert†
SRI International
cpeikert@alum.mit.edu

Vinod Vaikuntanathan‡
MIT
vinodv@mit.edu

STOC'08



Solving the Shortest Vector Problem in 2^n Time via Discrete Gaussian Sampling

Extended Abstract*

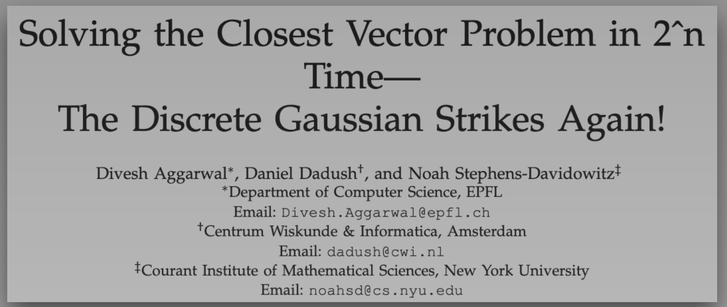
Divesh Aggarwal
Department of Computer Science, EPFL.

Daniel Dadush
Centrum Wiskunde & Informatica, Amsterdam.
dadush@cwi.nl

Noah Stephens-Davidowitz
Courant Institute of Mathematical Sciences, New York University.

Oded Regev
Courant Institute of Mathematical Sciences, New York University.

STOC'15



Solving the Closest Vector Problem in 2^n Time—
The Discrete Gaussian Strikes Again!

Divesh Aggarwal*, Daniel Dadush†, and Noah Stephens-Davidowitz‡
*Department of Computer Science, EPFL
Email: Divesh.Aggarwal@epfl.ch
†Centrum Wiskunde & Informatica, Amsterdam
Email: dadush@cwi.nl
‡Courant Institute of Mathematical Sciences, New York University
Email: noahsd@cs.nyu.edu

FOCS'15

What Is Known About Sampling?

- Efficient but limited samplers (with s depending on the basis or much larger than the smoothing parameter)
- Very inneficient but arbitrarily good samplers $\sim 2^{n+o(n)}$

Our Brand New Discovery….

On Gaussian Sampling for q-ary Lattices and Linear Codes with Lee Weight

Maiara F. Bollauf[1], Maja Lie[2], and Cong Ling[2]

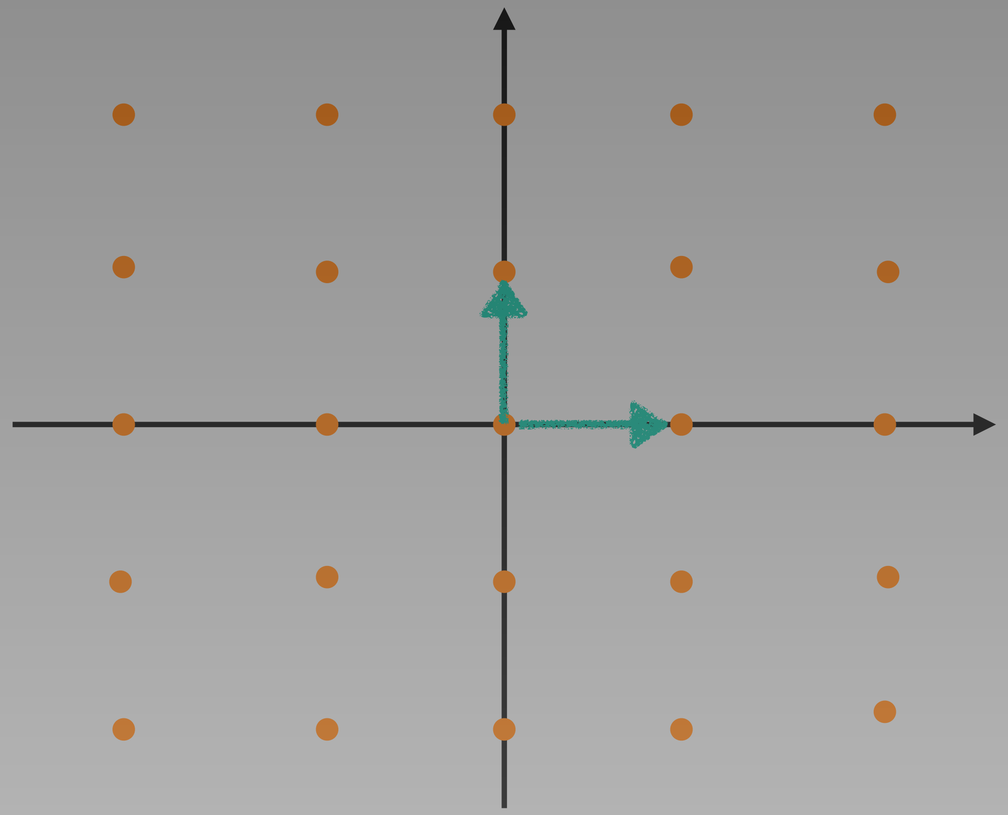
CRYPTO'25

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

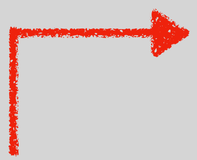
Imperial College London

Lattice

For crypto applications, subgroups of $\mathbb{Z}^n$ are complicated enough.



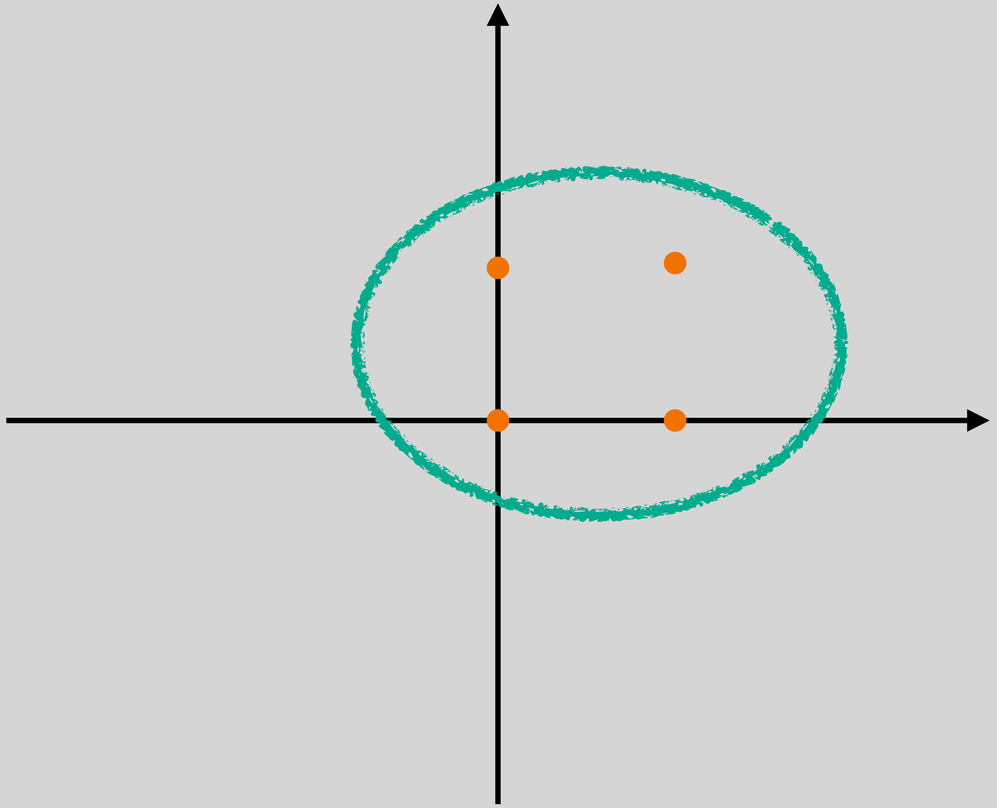
Sampling for Lattices via Linear Codes



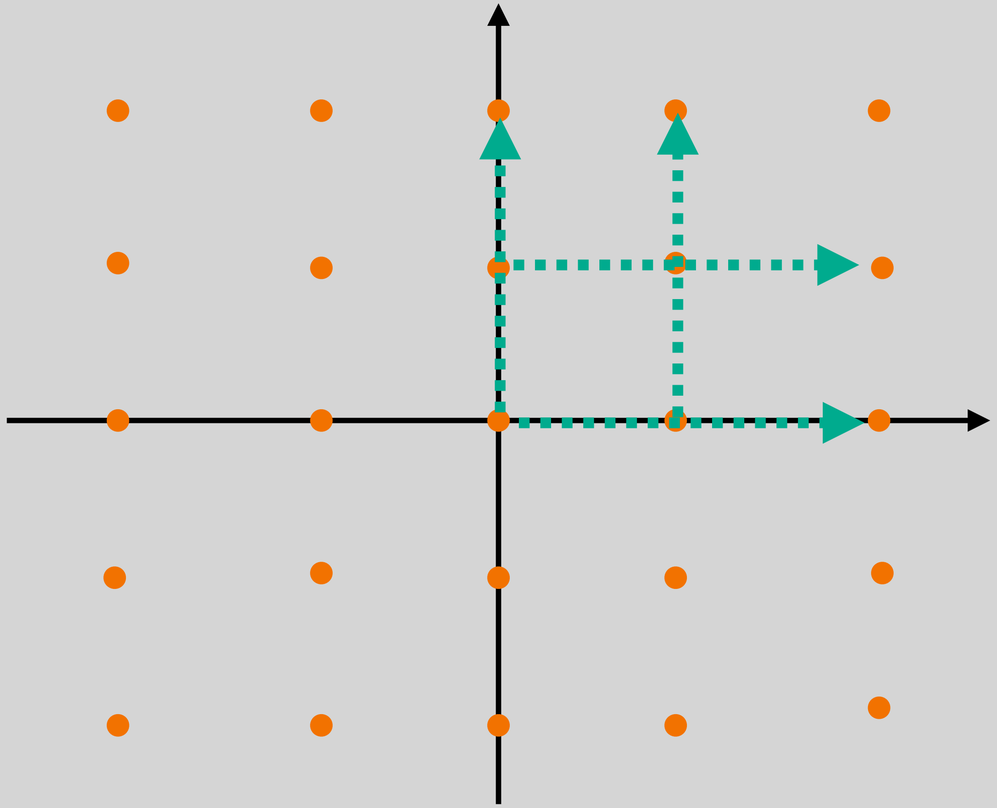
q-ary lattices

- Lattices such that $q\mathbb{Z}^n \subseteq \Lambda \subseteq \mathbb{Z}^n$
- They can be expressed as $\mathscr{C} + q\mathbb{Z}^n$, $\mathscr{C}$ is a linear code over $\mathbb{Z}_q$

Sampling for Lattices via Linear Codes

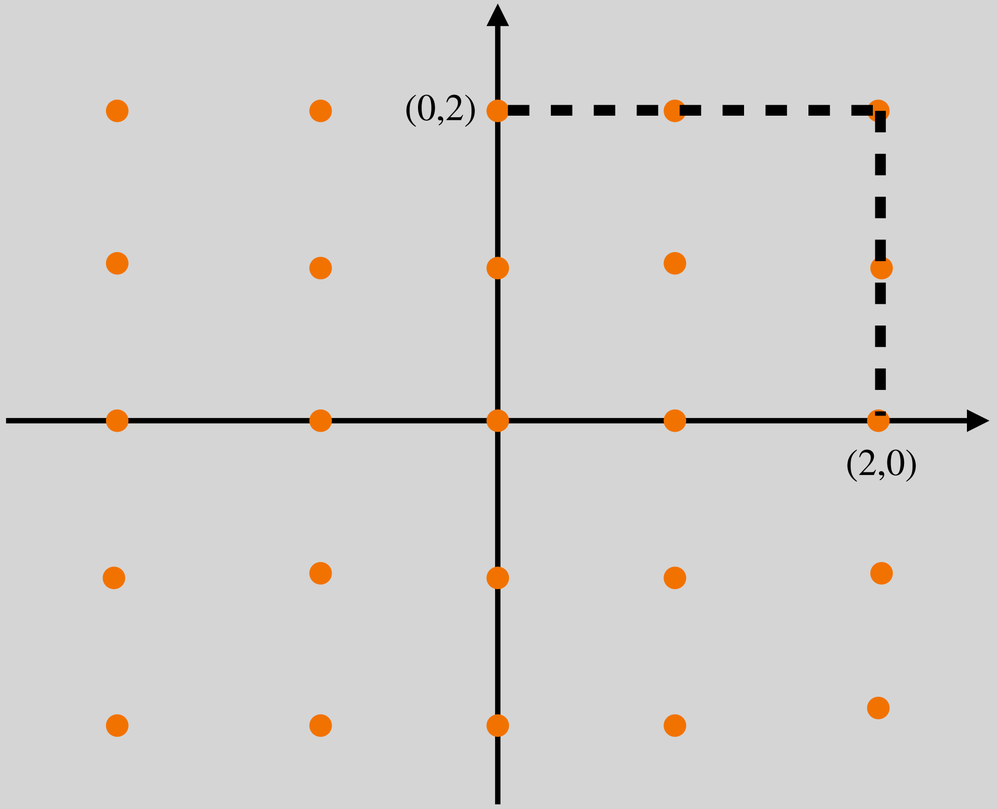


$\mathscr{C} = \{(0,0), (1,0), (0,1), (1,1)\}$



$\mathscr{C} + 2\mathbb{Z}^2$

Sampling for Lattices via Linear Codes



$\mathscr{C} + 2\mathbb{Z}^2$

Sampling for Lattices via Linear Codes

Gaussian sampling on q-ary lattices

Sampling codewords with respect to the Lee weight

$$\omega_{Lee}(x) = \min\{x, q - x\}$$

Sampling for Lattices via Linear Codes

We propose a new sampler for arbitrary width s

Techniques: Lee weight + cosets +

code symmetries + sampling over $\mathbb{Z}$

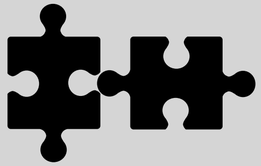
Sampling for Lattices via Linear Codes

We improve the state-of-the-art sampling for some families of lattices

	Complexity	**Sampling Width s**			
Lattice	Speed-up (UB)	[13]	This work	**LWP Table Size**	**#Cosets**
A_2	$18\times$	$\approx \eta_\epsilon(\mathrm{A}_2)$	$= \eta_\epsilon(\mathrm{A}_2)$	-	2
E_8	$22\times$	$\approx \eta_\epsilon(\mathrm{E}_8)$	$= \eta_\epsilon(\mathrm{E}_8)$	14 bits	2^4
D_n	$2\times$	$\approx \eta_\epsilon(\mathrm{D}_n)$	$= \eta_\epsilon(\mathrm{D}_n)$	-	2
Λ_{24}	$2\times$	$\approx \eta_\epsilon(\mathrm{E}_8)$	$= \eta_\epsilon(\Lambda_{24})$	34 bits	2^{12}
BW_{16}	$11\times$	$> \eta_\epsilon(\mathrm{BW}_8)$	$= \eta_\epsilon(\mathrm{BW}_{16})$	17 bits	2^{11}

Sampling for Lattices via Linear Codes

Sampling tehcnique



Exact calculation of the smoothing parameter

Sampling for Lattices via Linear Codes

Not efficient in general, since it requires enumerating

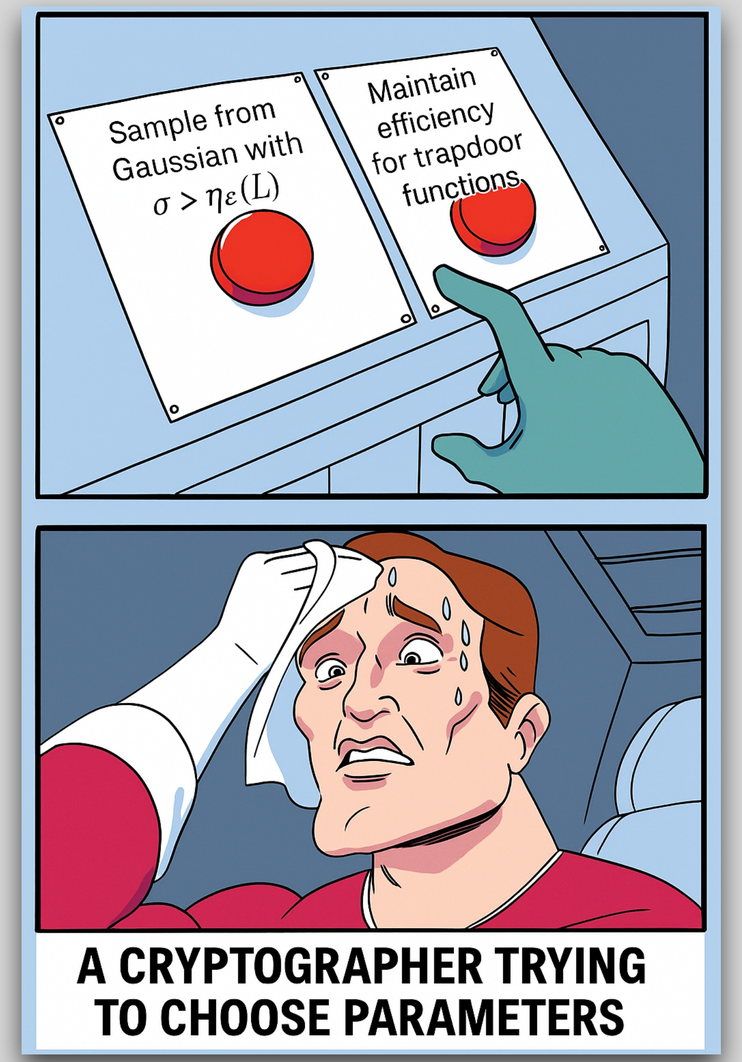
the codewords and their weights

More Details?

University of Tartu News

Tuesday 03/06/2025 Institute of Computer Science

Maja Lie will visit Tartu from 29/06/2025 to 11/07/2025 and will present an extended ~~and slightly more technical~~ version of our joint work



Source: ChatGPT

Thank you!

More details at: https://eprint.iacr.org/2025/087