Introduction aux réseaux euclidiens (lattices)

—

Un pas dans la cryptographie post-quantique

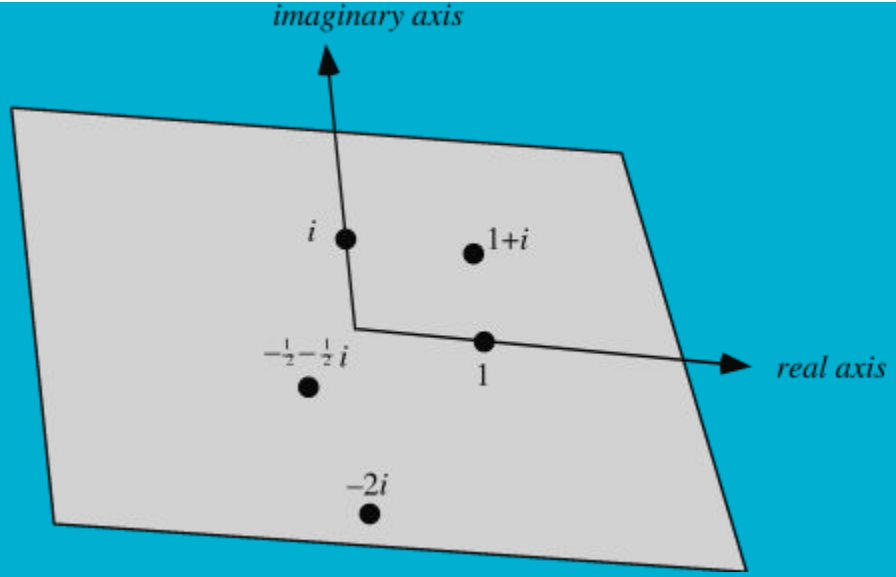
Le NIST

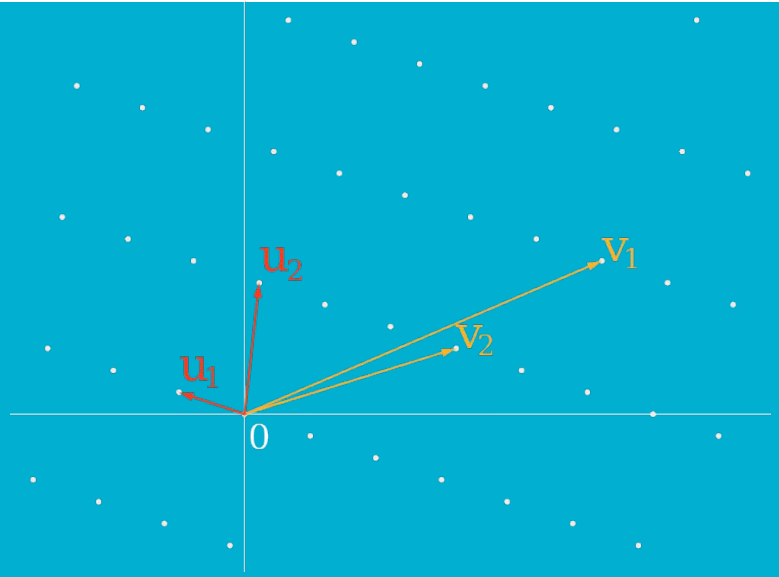
Third Round Finalists		Alternate Candidates	
Public-Key Encryption/KEMs	Type	Public-Key Encryption/KEMs	Type
Classic McEliece	Code-Based	BIKE	Code-Based
CRYSTALS-KYBER	Lattice-Based	HQC	Code-Based
NTRU	Lattice-Based	FrodoKEM	Lattice-Based
SABER	Lattice-Based	NTRU Prime	Lattice-Based
		SIKE	Supersingular Isogeny Based
Digital Signatures	Type	Digital Signature	Type
CRYSTALS-DILITHIUM	Lattice-Based	GeMSS	Multi-variate Based
FALCON	Lattice-Based	Picnic	Hash-Based
Rainbow	Multi-Variate Based	SPHINCS+	Hash-Based

	Round 3		Alternatives	
	Algorithm	Category	Algorithm	Category
KEM	Classic McEliece	Code	BIKE	Code
	Crypstals Kyber	LWE	FrodoKEM	LWE
	NTRU	NTRU	HQC	Code
	Saber	LWR	NTRU Prime	NTRU
			SIKE	Isogeny
Digital Signature	Crystals Dillithium	LWE	GeMMS	MQ
	Falcon	NTRU	Picnic	Secret
	Rainbow	MQ	Sphincs+	Hash

Un sous-espace vectoriel ?

$$EV = \{\forall (a_1, \ldots, a_n) \in \mathbb{R}^n, \sum_{i=1}^{n} a_i b_i\} \qquad L = \{\forall (a_1, \ldots, a_n) \in \mathbb{Z}^n, \sum_{i=1}^{n} a_i b_i\}$$





Le SVP et le CVP

- **S**hortest **V**ector **P**roblem: Trouver le plus petit vecteur dans un réseau euclidien L
- **C**losest **V**ector **P**roblem : Trouver le vecteur le plus proche d'un vecteur arbitraire u non présent dans L
- (Non utilisé directement dans la crypto PQ)
- Utilisé dans la cryptanalyse plus généralement (ROCA)

Le SIS et l'ISIS

$A \in \mathbb{Z}^{n*m}, u \in \mathbb{Z}^n$

$$\Lambda^{\perp}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{Az} = \mathbf{0} \mod q\},$$

$$\Lambda^{\perp}_{\mathbf{u}}(\mathbf{A}) = \{\mathbf{z} \in \mathbb{Z}^m : \mathbf{Az} = \mathbf{u} \mod q\}.$$

$SIS_{q,n,m,\beta}$: *Soit* $A \in \mathbb{Z}_q^{n*m}$, *trouver* $x \in \lambda^{\perp}(A)$ *tel que* $\|x\| < \beta$

$ISIS_{q,n,m,\beta}$: *Soit* $A \in \mathbb{Z}_q^{n*m}$, $u \in \mathbb{Z}^n$, *trouver* $x \in \lambda_u^{\perp}(A)$ *tel que* $\|x\| < \beta$

Gauss et LLL

- Possible de trouver une solution au SVP / CVP si dimension < 4
- Algorithme de Gauss en dimension 2
- LLL (Lenstra–Lenstra–Lovász) pour des dimensions supérieures