Algebraic Constructions of Modular Lattices

Hou Xiaolu
Supervisor: Prof. Frédérique Oggier

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University
Email: HO0001LU@e.ntu.edu.sg

Poster Presentation for SPCoding School

Modular Lattice

Definition

- Lattice: $\Lambda = \{\boldsymbol{x} = \lambda M_\Lambda \in \mathbb{R}^n : \lambda \in \mathbb{Z}^n\}$
- Dual Lattice: $\Lambda^* = \{\boldsymbol{x} \in \mathbb{R}^n : \boldsymbol{x} \cdot \lambda \in \mathbb{Z}\ \forall\lambda \in \Lambda\}$
- Integral Lattice: $\Lambda \subseteq \Lambda^*$
- $\ell-$modular Lattice(Quebbemann, 1995): $\Lambda \subseteq \Lambda^*,\ \tau(\Lambda^*) = \Lambda$
  $$\ell = \frac{\|\tau(\boldsymbol{u})\|^2}{\|\boldsymbol{u}\|^2}\ \forall \boldsymbol{u} \in \Lambda^*$$
- $\ell = 1$: Λ is called unimodular

Two Approaches

- Ideal Lattice
- Generalized Construction A

H.-G. Quebbemann, "Modular Lattice in Euclidean Spaces", *J. Number Theory* **54** (1995) 190-202.

Ideal lattice(Totally real number field)

- $b : I \times I \to \mathbb{R} \quad b(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$
- Arakelov-modular lattice of level ℓ (Bayer-Fluckiger 2005): $\exists \lambda \in K^*, \ (I, b) = (\lambda I^*, b)$
- $(I, b) \hookrightarrow \mathbb{R}^n$

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_2(\omega_1) & \dots & \sigma_n(\omega_1) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(\omega_n) & \sigma_2(\omega_n) & \dots & \sigma_n(\omega_n) \end{pmatrix},$$

where $\{\omega_1, \dots, \omega_n\}$ is a $\mathbb{Z}$-basis of I

Result for $K = \mathbb{Q}(\sqrt{d})$

$\exists (I, b)$ Arakelov-modular of level ℓ iff $\ell = d$.

E. Bayer-Fluckiger, I. Suarez, "Modular Lattices over Cyclotomic Fields", *J. Number Theory* **114**(2) (2005) 394-411.

Generalized Construction A

- $K = \mathbb{Q}(\sqrt{5})$, p a prime inert in K
- Define

$$\begin{array}{rcl} \rho : \mathcal{O}_K^N & \rightarrow & \mathbb{F}_{p^2}^N \\ (a_1, \ldots, a_N) & \mapsto & (a_1 \mod p\mathcal{O}_K, \ldots, a_N \mod p\mathcal{O}_K) \end{array}$$

- If $C \subseteq \mathbb{F}_{p^2}^N$ is a self-dual linear code, then $\rho^{-1}(C)$ with bilinear form

$$(x, y) \mapsto \frac{1}{p} \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i)$$

is a $5-$modular lattice.(H, Lin, Oggier, 2014)

X. Hou, F. Lin, F. Oggier, "Construction and Secrecy Gain of a Family of 5-modular Lattices", IEEE ITW 2014, Hobart, Australia.