Reduction of the ring-LWE distribution from $\mathcal{O}_K^\vee$ to the ring-LWE distribution from $\mathcal{O}_K$

Léo Ducas Alain Durmus Vadim Lyubashevsky

November 25, 2011

1 Preliminaries

1.1 Number theory requirement

We need, in a first time, to define objects, that we will manipulate and state some of their properties. We define a field extension L/K to be two field L and K such that $K \subset L$. Then, if L/K is a field extension, L has a structure of K vector space, and we call the degree of an extension L/K the dimension of L as a K vector space. Then, if the degree

2 Reduction from $\mathcal{O}_K^\vee$-LWE to $\mathcal{O}_K$-LWE

2.1 Definitions

2.1.1 Ring-LWE problems

Definition 2.1 ($\mathcal{O}_K^\vee$-LWE distribution)**.** *For $s \in R_q^\vee$ and an error distribution ψ over $K_\mathbb{R}$ a sample from the $R_q^\vee$-LWE distribution $A_{s,\psi}^\vee$ over $R_q^\vee \times \mathbb{T}^\vee$ is generated by choosing $a \leftarrow R_q^\vee$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = \frac{as}{q} + e \mod R^\vee)$*

Definition 2.2 ($\mathcal{O}_K$-LWE distribution)**.** *For $s \in R_q$ and an error distribution ψ over $K_\mathbb{R}$ a sample from the R_q-LWE distribution $A_{s,\psi}^\vee$ over $R_q \times \mathbb{T}$ is generated by choosing $a \leftarrow R_q$ uniformly at random, $e \leftarrow \psi$, and outputting $(a, b = \frac{as}{q} + e \mod R)$*

2.1.2 Error distributions

2.2 The $\mathcal{O}_K^\vee$ to $\mathcal{O}_K$ reduction

2.2.1 Passage from $\mathcal{O}_K^\vee$ to $\mathcal{O}_K$

For our reduction from $\mathcal{O}_K^\vee$-LWE to $\mathcal{O}_K$-LWE, we need to know how to go from $\mathcal{O}_K^\vee$ to $\mathcal{O}_K$. More precisely, we know that $\mathcal{O}_K$

Proposition 2.1
Let $K = \mathbb{Q}(\zeta_n)$ be the n^{th} cyclotomic field. So,

$$n\mathcal{O}_K^\vee \subset \mathcal{O}_K$$

Proof. We already know that

$$\mathcal{O}_K^\vee = \frac{1}{\Phi_n'(\zeta_n)}\mathcal{O}_K$$

Thus, if we prove that $\frac{n}{\Phi'_n(\zeta_n)} \in \mathcal{O}_K$, we will prove the assertion above. For this, we consider the factorization of $X^n - 1$ by $\Phi_n(X)$: $X^n - 1 = \Phi_n(X)g(X)$, with $\Phi_n(X)$ and $g(X) \in \mathbb{Z}[X]$. And we derivate this expression.

$$nX^{n-1} = \Phi'_n(X)g(X) + \Phi_n(X)g'(X)$$

We evaluate the expression for $X = \zeta_n$. So as $\Phi_n(\zeta_n) = 0$),

$$n\zeta_n^{n-1} = \Phi'_n(\zeta_n)g(\zeta_n)$$

Which we multiply by ζ_n. And substituting ζ_n^n by 1, we finally have:

$$\begin{aligned} n &= \zeta_n\Phi'_n(\zeta_n)g(\zeta_n) \\ \frac{n}{\Phi'_n(\zeta_n)} &= \zeta_n g(\zeta_n) \end{aligned}$$

As $g(X) \in \mathbb{Z}[X]$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$, $\zeta_n g(\zeta_n) \in \mathcal{O}_K$. So, we have proved that $\frac{n}{\Phi'_n(\zeta_n)} \in \mathcal{O}_K$ and therefore $n\mathcal{O}_K^\vee \subset \mathcal{O}_K$. □