NTRU+

Jonghyun Kim * Jong Hwan Park†

July 8, 2022

Abstract

In this section, ..

Keywords: Post Quantum Signature, Pseudorandom Generator

1 Introduction

Definition 1.1 (RLWE problem)**.** Let n, q, p be positive integers such that $q > p$. Let $\mathcal{R}_q$ and $\mathcal{R}_p$ be polynomial rings constructed by $\Phi_{3n}(x)$, and $\mathcal{D}_s$ be a distribution over $\mathcal{R}_q$. A decisional RLWR *problem*$\mathsf{RLWR}_{n,1,q,p}(\Phi_{3n})$ is to distinguish uniformly random $(a,u) \in \mathcal{R}_q \times \mathcal{R}_p$ and

$(a, b = \frac{p}{q}a \cdot s) \in \mathcal{R}_q$

$\times \mathcal{R}_p$ where s is sampled from $\mathcal{D}_s$. Then, the advantage of an adversary $\mathcal{A}$ in solving the decisional RLWR problem $\mathsf{RLWR}_{n,1,q,p}(\mathcal{D}_s)$ is defined as follows:

$$\mathrm{Adv}^{\mathcal{RLWR}}_{n,1,q,p}(\mathcal{A}) = \Pr[\mathcal{A}(a,b) = 1] - \Pr[\mathcal{A}(a,u) = 1].$$

2 Base Encryption Scheme

KeyGen:

- $f' \leftarrow \mathcal{R}$
- $f = 3f' + 1$
- if f is not invertible in R_q, restart
- $g \leftarrow \mathcal{R}$
- $h = 3g/f$
- **return**$(sk = f, pk = h)$

Encrypt:

- $c = hr + m$

Decrypt:

- $m = (cf \mod^{\pm} q) \mod^{\pm} 3$

*Korea University, Seoul, Korea. Email:yoswuk@korea.ac.kr.

†Institution2. Email: abc@abc.abc.