INTISARI

Learning With Error (LWE) Sebagai Kriptografi Berbasis Latis

Oleh

Aisyah Nooravieta Setiawan

21/476076/PPA/06147

Dalam menghadapi era komputer kuantum, tentunya perkembangan ilmu kriptografi sangat dibutuhkan untuk menciptakan sistem keamanan yang *secure* baik terhadap serangan komputer klasik ataupun komputer kuantum. Salah satu pendekatan yang dapat digunakan membangun sistem kriptografi tersebut adalah dengan latis. Oleh sebab itu, pada tulisan ini akan dijelaskan mengenai sistem kriptografi berbasis latis yaitu Learning With Error (LWE), serta LWE Ring (RLWE) yang merupakan pengembangan dari LWE yang diganti strukturnya dengan menggunakan ring polinomial $\mathbb{Z}[x]/\langle x^n + 1\rangle$.

Kata kunci: Kriptografi Berbasis Latis, Short Integer Solution, Learning With Error, Learning With Error Ring.

ABSTRACT

Learning With Error (LWE) As Lattice-Based Cryptography

By

Aisyah Nooravieta Setiawan

21/476076/PPA/06147

In encountering the era of quantum computers, the development of cryptography is definitely needed for constructing a secure system of cryptography from any raid neither classical computers nor quantum computers, The cryptography system is called Quantum Secure Cryptography. One of the methods that can be approached for constructing Quantum Secure Cryptography is Lattice. Therefore, this thesis will explore more about the lattice-based cryptography Learning With Error (LWE). Furthermore, the development of LWE which algebraic structure is replaced with polynomial ring$\mathbb{Z}[x]/\langle x^n + 1\rangle$.

Keywords: Lattice-Based Cryptography, Short Integer Solution, Learning With Error, Ring Learning With Error.