INTISARI

PROTOKOL PERTUKARAN KUNCI DIFFIE-HELLMAN BERBASIS RING-LWE

Oleh

INDRIANI SAFITRI

20/459341/PA/20002

Sistem kriptografi LWE (*Learning With Error*) merupakan salah satu pendekatan kriptografi berbasis latis dengan penambahan galat pada sistem persamaan linear. Pada tugas akhir ini, akan dikaji mengenai pengembangan dari sistem kriptografi LWE yakni sistem kriptografi RLWE (Ring *Learning With Error*). RLWE merupakan perluasan dari LWE ke struktur aljabar yang lebih kompleks, yaitu ring polinomial. RLWE memberikan solusi yang lebih efisien dibandingkan dengan LWE. Selanjutnya, RLWE akan diterapkan dalam protokol pertukaran kunci yang didasarkan pada kesulitan masalah logaritma diskrit yang dikenal sebagai pertukaran kunci Diffie-Hellman. Pada tugas akhir ini juga dibahas mengenai pengembangan RLWE pada protokol pertukaran Diffie-Hellman yang melibatkan 3 entitas.

ABSTRACT

DIFFIE-HELLMAN KEY EXCHANGE PROTOCOL BASED ON RING-LWE

By

INDRIANI SAFITRI

20/459341/PA/20002

LWE (*Learning With Error*) cryptosystem is one of the lattice-based cryptography with an addition of errors in the linear equation system. In this final project, we introduce one of the LWE cryptosystem variance, the RLWE (*Ring Learning With Error*) cryptosystem. RLWE is an extension of LWE to a more complex algebraic structure. RLWE provides a more efficient solution than LWE. Furthermore, it also discusses how RLWE can be applied in in a key exchange protocol based on the difficulty of the discrete logarithm problem, known as the Diffie-Hellman key exchange. In this final project, we discusses the development of RLWE in the Diffie-Hellman exchange protocol in 3 entities.