INTISARI

WEIL PAIRING PADA KRIPTOGRAFI KURVA ELIPTIK

Oleh

NAJIB MUBAROK

13/354957/PPA/04326

Diberikan kurva eliptik $E : y^2 = x^3 + ax + b$ atas lapangan K dengan $char(K) \notin \{2, 3\}$. Dibentuk subgrup $E[n]$ yang beranggotakan elemen-elemen n-torsi dari grup kurva eliptik $E(K)$. Dalam tesis ini, dibahas proses konstruksi dan karakterisasi dari *weil pairing* yang merupakan fungsi dari elemen-elemen di $E[n] \times E[n]$ menuju grup multiplikatif μ_n yang beranggotakan akar-akar ke-n dari uniti di K. Lebih lanjut, *Weil pairing* mempunyai sifat bilinear, identitas, dan *non-degeneracy* yang membuat *weil pairing* aplikatif dalam kriptoanalisis dan kriptografi. Dalam kriptoanalisis, *weil pairing* mempunyai peran dalam melakukan reduksi pada logaritma diskrit kurva eliptik yang dikenal dengan *MOV attack*.

ABSTRACT

WEIL PAIRING ON ELLIPTIC CURVE CRYPTOGRAPHY

By

NAJIB MUBAROK

13/354957/PPA/04326

Given elliptic curve $E : y^2 = x^3 + ax + b$ over field K with $char(K) \notin \{2, 3\}$. The subgroup $E[n]$ is formed by taking all n-torsion elements of elliptic curve group $E(K)$. In this thesis, we will discuss the construction and the properties of Weil pairing that is a map from $E[n] \times En$ to a multiplicative group formed by n-th roots of unity in K. Furthermore, Weil pairing has three important properties, that are bilinearity, identity, and non-degeneracy that make Weil pairing applicable in both cryptanalysis and cryptography. In Cryptanalysis, Weil pairing is used to reduce the security of elliptic curves discrete logarithm problem known as MOV attack.