Penerapan fungsi bilinear pada skema tanda tangan agregat tanpa sertifikat = Implementation of bilinear function on certificateless aggregate signature scheme

Annisa Dini Handayani, author

Abstrak

Fungsi bilinear merupakan suatu fungsi yang berbentuk 𝑒: 𝑉 × 𝑉 → 𝐹, dengan 𝑉 adalah ruang vektor atas lapangan 𝐹 yang bersifat linear. Pada implementasinya, fungsi bilinear dapat diterapkan pada skema kriptografi. Kriptografi didefinisikan sebagai ilmu yang berkaitan dengan aspek keamanan informasi, seperti kerahasiaan, keutuhan data, otentikasi entitas dan otentikasi sumber data, dengan menggunakan teknik-teknik matematika. Salah satu skema kriptografi yang menggunakan fungsi bilinear adalah skema yang berkaitan dengan otentikasi sumber data, yaitu Tanda Tangan Agregat Tanpa Sertifikat (Certificateless Aggregate Signature).
Pada penelitian ini akan dibahas skema Tanda Tangan Agregat Tanpa Sertifikat (T2ATS) yang diajukan oleh Liu dkk pada tahun 2014 serta sifat/karakteristik dari fungsi bilinear yang harus dipenuhi guna menjamin keamanan dari skema kriptografi, khususnya skema T2ATS. Hasil dari penelitian ini menunjukkan bahwa fungsi bilinear yang digunakan pada skema T2ATS harus menggunakan domain dan kodomain yang memenuhi masalah logaritma diskrit (Discrete Logarithm Problem). Selain itu, penelitian ini juga akan menerapkan salah satu varian fungsi bilinear, yaitu fungsi weil pairing pada skema T2ATS.
.....
Bilinear map is a linear function that in form e: V × V → F, where V is a vector space over field F. Bilinear map can be used in cryptographic scheme. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. An example of bilinear map implementation used in cryptographic scheme is Certificateless Aggregate Signature (CLAS). CLAS is a cryptographic scheme related to data origin authentication.
This research will describe CLAS scheme proposed by Liu et.al (2014) and bilinear map properties hold to ensure security of this scheme. The result of this paper show that domain and codomain of bilinear map used in CLAS scheme should meet Discrete Logarithm Problem. This research also implement weil pairing as one of bilinear function commonly used in cryptography on CLAS scheme.