Implementasi Elliptic Curve Secp256k1 pada Transaksi dengan Bitcoin = Implementation of Secp256k1 on Bitcoin Transaction

Amira Zahra, author

Abstrak

Bitcoin adalah suatu sistem pembayaran elektronik. Proses transaksi dengan menggunakan bitcoin dilakukan tanpa otoritas sentral atau bank. Hal ini bertujuan untuk memotong biaya mediasi (mediation cost) dan juga membuat transaksi lebih praktis. Setiap pengguna bitcoin memiliki username sebagai kunci publik dan password sebagai kunci privatnya. Transaksi pada bitcoin memanfaatkan Elliptic Curve Digital Signature Algorithm (ECDSA). Adapun elliptic curve yang digunakan adalah secp256k1. Ada kriteria yang digunakan untuk menentukan tingkat keamanan kriptografi elliptic curve, salah satunya adalah kriteria safe curve yang diajukan oleh Bernstein dan Lange pada tahun 2013. Kriteria ini dibuat untuk menjamin keamanan kriptografi elliptic curve, tidak hanya menjamin keamanan Elliptic Curve Digital Logarithm Problem (ECDLP). Persyaratan suatu kurva merupakan safe curve meliputi persyaratan parameter dasar, persyaratan keamanan ECDLP (meliputi ketahanan dari serangan Rho dan transfer, diskriminan lapangan perkalian kompleks pada elliptic curve, dan rigidity), dan persyaratan keamanan kriptografi elliptic curve (meliputi penggunaan ladder Montgomery, ketahanan dari serangan twist, kelengkapan perkalian skalar, indistinguishability). Tujuan dari penelusuran literatur ini adalah untuk menjelaskan penggunaan secp256k1 pada transaksi bitcoin dan menganalisis kriteria safe curve yang tidak dipenuhi oleh secp256k1. Dari penelusuran literatur ini, dapat disimpulkan bahwa setiap pemilik bitcoin yang mentransfer bitcoin melakukan tanda tangan secara digital pada hash dari transaksi sebelumnya dan kunci publik pemilik berikutnya. Penandatanganan digital ini dilakukan dengan menggunakan kunci privat orang yang mentransfer bitcoin. Tanda tangan digital dapat diverifikasi menggunakan kunci publik pengguna yang mentransfer bitcoin. Pembentukan kunci publik dan kunci privat, pembentukan tanda tangan digital, dan verifikasi tanda tangan digital memanfaatkan elliptic curve digital signature algorithm (ECDSA), dengan elliptic curve yang digunakan adalah secp256k1. Secp256k1 tidak memenuhi persyaratan nilai minimum diskriminan lapangan perkalian kompleks pada E(F_p) karena memiliki nilai |D|=2^1.6<2^100. Secp256k1 tidak memenuhi persyaratan penggunaan ladder Montgomery, kelengkapan perkalian skalar, dan indistinguishability karena secp256k1 memiliki cofactor h=1. <hr /> Bitcoin is an electronic payment system. The transaction process by using Bitcoin is made without a central authority or bank. It has a purpose to cut mediation costs and also make transactions more practical. Every Bitcoin user has a username as a public key and password as its private key. Transactions on Bitcoin utilize the Elliptic Curve Digital Signature Algorithm (ECDSA). Specifically, the elliptic curve used is secp256k1. There are criteria used to determine the level of cryptographic security of an elliptic curve, one of which is the safe curve criteria proposed by Bernstein and Lange in 2013. These criteria are established not only to guarantee the security of Elliptic Curve Digital Logarithm Problems (ECDLP), but also to guarantee the safety of elliptic curve cryptography. The requirements for a curve are a safe curve including basic parameter requirements, ECDLP security requirements (including resistance to Rho and transfer attacks, complex multiplication field discriminant, and rigidity), and elliptic curve cryptography security requirements (including the use of

Montgomery ladders, resistance to twist, completeness of scalar multiplication, and indistinguishability). The purposes of this literature review are to explain how to use secp256k1 in Bitcoin transactions and to analyse not-satisfying of the safe curve criteria on secp256k1. It can be concluded that each owner transfers bitcoin to the next owner by signing a hash from previous transaction and the public key of the next owner. The process of private key and public key generation, digital signature, and verification utilize Elliptic Curve Digital Signature Algorithm (ECDSA). The elliptic curve used is secp256k1. The reason Secp256k1 does not meet the requirements of minimum complex field discriminant value of E(F_p) is it has |D|=2^1.6<2^100. Secp256k1 does not use Montgomery ladder and also does not meet the requirement of completeness of scalar multiplication and indistinguishability because it has cofactor 1.</p>