Keunggulan Performansi Rank Quasi Cyclic Signature Dibandingkan Dengan Cryptonote Signature

Hafizh Fadhilah Radi Briantama[1], Prof. Ir. Ari Moesriami Barmawi, M.Sc., Ph.D.[2]

[1,2,3]Fakultas Informatika, Universitas Telkom, Bandung
[4]Divisi Digital Service PT Telekomunikasi Indonesia
[1]hafizhradi@students.telkomuniversity.ac.id, [2]mbarmawi@melsa.net.id,

Abstrak

Digital Signature merupakan bagian penting dari proses pengiriman suatu dokumen digital. Digital signature berfungsi untuk melindungi dokumen digital pada saat proses pengiriman dari pihak ketiga. Salah satu digital signature adalah *Cryptonote Signature*. *Cryptonote Signature* masih sering digunakan dalam beberapa *Crypto Currency*. *Cryptonote Signature* memiliki kelemahan berupa kunci yang cukup panjang sehingga diperlukan waktu komputasi yang cukup lama. Perlu diperbandingkan *Digital Signature* yang lain untuk mengatasi kekurangan tersebut yaitu *Rank Quasi Cyclic Signature* atau RQCS. RQCS dipilih karena memiliki panjang kunci yang pendek sehingga waktu yang perlukan untuk melakukan komputasi lebih singkat. Selain itu pada RQCS memiliki proses iterasi lebih sedikit dibandingkan dengan Cryptonote Signature karena menggunakan perkalian matriks, sementara pada Cryptonote Signature terdapat proses iterasi cukup banyak karena pada Cryptonote Signature menggunakan perkalian titik yang terdapat pada ecc. Percobaan dilakukan dengan membandingkan waktu komputasi dari setiap proses yang terdapat pada masing – masing *digital signature*. Proses tersebut berupa proses *Key Generation* yaitu proses pembuatan Kunci, proses *Signature Generation* yaitu proses pembuatan *Signature*, dan proses *Verification* yaitu proses verifikasi pesan yang diterima adalah valid. Pada hasil percobaan yang dilakukan didapat perbedaan pengaruh panjang kunci pada kedua *Digital Signature*, pada *Cryptonote Signature* tidak terlihat perubahan waktu yang signifikan terhadap perubahan panjang kunci yang digunakan, sedangkan pada RQCS terdapat perubahan waktu yang cukup signifikan terhadap panjang kunci. Hasil percobaan menunujukan RQCS memiliki waktu penyelesaian komputasi jauh lebih cepat dibandingkan dengann *Cryptonote Signature*.

Kata kunci : digital signature, cryptonote signature, RQCS

Abstract

Digital Signature is an important part of the process of sending a digital document. Digital signature functions to protect digital documents during the sending process from a third party. One of the digital signatures is Cryptonote Signature. Cryptonote Signature is still often used in several Crypto Currencies. Cryptonote Signature has a weakness in the form of a key that is quite long so that it requires a long computing time. It is necessary to compare other Digital Signatures to overcome these shortcomings, namely Rank Quasi Cyclic Signature or RQCS. RQCS was chosen because it has a short key length so that the time needed to perform the computation is shorter. In addition, RQCS has fewer iteration processes compared to Cryptonote Signature because it uses matrix multiplication, while Cryptonote Signature has quite a lot of iteration processes because Cryptonote Signature uses dot multiplication found in ecc. The experiment was carried out by comparing the computing time of each process contained in each digital signature. The process is in the form of a Key Generation process, namely the process of creating a Key, a Signature Generation process, namely the process of creating a Signature, and a Verification process, namely the process of verifying the message received is valid. The results of the experiments conducted showed differences in the influence of key length on both Digital Signatures, in Cryptonote Signature there was no significant change in time to the change in the key length used, while in RQCS there was a significant change in time to the key length. The results of the experiments showed that RQCS had a much faster computational completion time compared to Cryptonote Signature.

Keywords: digital signature, cryptonote signature, RQCS