INTISARI

PARALELISASI PEMANGKATAN MODULAR POLINOMIAL

Oleh

MUHAMMAD RIDWAN APRIANSYAH BUDIKAFA
13/348667/PA/15466

Pemangkatan modular merupakan operasi yang penting dalam protokol keamanan jaringan. Pemangkatan modular polinomial adalah pemangkatan modular dengan basis dan *modulus* berupa polinomial. Salah satu kegunaannya adalah pada algoritma AKS, salah satu algoritma pengecekan bilangan prima tercepat saat ini.

Pada tugas akhir ini dikembangkan algoritma pemangkatan modular paralel yang diusulkan oleh Lara et al. (2012) untuk melakukan pemangkatan modular polinomial secara paralel, dan dibandingkan dengan 2 algoritma paralel lain yang diusulkan. Pada hakikatnya ketiga algoritma tersebut hanya berbeda pada metode *load balancing*-nya. Diperoleh hasil bahwa untuk bilangan eksponen sepanjang 2048 bit, implementasi algoritma paralel yang diusulkan oleh Lara et al. (2012) memiliki waktu eksekusi yang 28.01% lebih kecil dibandingkan implementasi algoritma sekuensial. Algoritma tersebut juga lebih efisien dibandingkan 2 algoritma lain yang diusulkan.

Kata Kunci: pemangkatan modular, pemangkatan modular polinomial, komputasi paralel, *load balancing*

ABSTRACT

PARALLELIZATION OF MODULAR POLYNOMIAL EXPONENTIATION

By

MUHAMMAD RIDWAN APRIANSYAH BUDIKAFA
13/348667/PA/15466

Modular exponentiation is very important in the network security protocol. Modular polynomial exponentiation is a type of modular exponentiation where the base and modulus are polynomials. One of its usages is on the AKS Algorithm, one of the fastest prime checking algorithm today.

In this research, parallel modular exponentiation algorithm which proposed by Lara et al. (2012) was developed to solve modular polynomial exponentiation in parallel, and compared with two other proposed parallel algorithms. Essentially those algorithms differ only in the load balancing method. The result was, for exponents with a length of 2048 bits, the implementation of parallel algorithm proposed by Lara et al. (2012) has 28.01% smaller execution time compared to the sequential algorithm. The algorithm was also more efficient than the two other proposed algorithms.

Keyword: modular exponentiation, modular polynomial exponentiation, parallel computing, load balancing