

INTISARI

Paralelisasi Perkalian Toom-Cook pada Pembangkitan Kunci RSA menggunakan CUDA

Oleh

Syaddam
16/403716/PPA/05233

Algoritme kriptografi kunci asimetri dianggap lebih aman dibandingkan algoritme kriptografi kunci simetri, hal ini dikarenakan kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Salah satu kriptografi kunci asimetri yang banyak digunakan adalah RSA (Rivest Shamir Adleman). Keamanan RSA terletak pada panjang kunci yang digunakan untuk proses pembangkitan kuncinya. Masalah muncul ketika panjang kunci yang digunakan membuat proses perhitungannya memakan waktu dan komputasi yang mahal. Toom-Cook merupakan metode perkalian yang dapat menangani perkalian dalam jumlah besar, metode ini dapat menangani operasi perkalian di dalam proses pembangkitan kunci RSA. Dengan menggunakan paralelisasi pada perkalian Toom-Cook serta pemanfaatan GPU di dalam proses perhitungan pembangkitan kunci RSA dapat mengurangi waktu komputasi.

Tujuan dari penelitian ini adalah untuk meningkatkan kecepatan perhitungan perkalian di dalam proses pembangkitan kunci RSA dengan menggunakan metode Toom-Cook yang akan diparalelkan menggunakan bantuan GPU.

Dari hasil penelitian yang telah dilakukan, perkalian Toom-Cook secara paralel dapat menyelesaikan tugas perkalian delapan belas kali lebih cepat dibandingkan proses sekuensial. Dengan mengimplementasikan perkalian ini secara paralel di dalam proses pembangkitan kunci RSA pengurangan waktu terjadi hingga 15.74%.

Kata Kunci: CUDA, GPU, Kriptografi, Paralel, RSA, Toom-Cook.