ABSTRACT

RSA public-key algorithm has being widespread used in real-world application nowadays since it introductory in 1978. Its security strength that relies on the difficulty of factoring the modulus N draws attention of mathematician community around the world to come up a better algorithm to factor the modulus.

This paper explores the use of general Quadratic Sieve as the factoring algorithm to recover the prime factors of RSA modulus N. JavaSpace, a special service of Java JINI™ technology, provides the infrastructure of distributed and parallel implementation of Quadratic Sieve algorithm in a local area network. The parallelism was achieved based on the master-slave pattern where two main modules are integrated by JavaSpace service through loosely coupled communication. Factoring results show that Quadratic Sieve is an effective algorithm to factor large integer and suitable for parallel implementation.