INTISARI

DASAR DASAR KOMPUTER KUANTUM DAN PENERAPANNYA PADA DEKRIPSI ALGORITMA RSA

Oleh

Fathiyya Izzatun Az-zahra
17/418523/PPA/05307

Kajian teoritis mengenai dasar komputer kuantum dan penerapannya pada algoritma RSA telah dilakukan. Dasar komputer kuantum yang dipelajari adalah konsep qubit, operator, dan keterikatan (entanglement). Qubit dimanipulasi dengan menggunakan kumpulan operasi universal yaitu matriks uniter level dua dan matriks operasi tunggal. Disajikan prosedur konstruksi sirkuit berdasarkan operasi universal beserta beberapa contoh sirkuit penting dalam komputer kuantum.

Salah satu penerapan dari konsep komputer kuantum adalah pada algoritma faktorisasi Shor. Algoritma Shor memiliki kompleksitas sebesar d^3, sedangkan faktorisasi klasik dengan algoritma GNFS memiliki kompleksitas sebesar $\exp^{\alpha d^{\frac{1}{3}}}$. Algoritma Shor digunakan untuk mendekripsi algoritma RSA dan melalui persamaan dekripsi $(M^e)^r = 1 \mod N$. Tiap langkah algoritma Shor dijelaskan secara matematis. Aspek kuantum dari algoritma Shor juga dijelaskan secara lebih rinci. Pengukuran pada algortima Shor dilakukan sebelum operasi QFT, dan disajikan alasan diperbolehkannya langkah tersebut. Untuk pembahasan lebih lanjut, algoritma dekripsi RSA diterapkan pada kasus sederhana. Dimisalkan bahwa $E(M) = M \mod 8 = 3$ dan persamaan dekripsi untuk $E(M)$ adalah $3^r \mod 8$.Persamaan ini diselesaikan dengan menggunakan algoritma Shor dan diperoleh sirkuit dan wakilan matriks dekripsi RSA yang merupakan sirkuit dan wakilan matriks pencarian orde pada algoritma Shor.

Kata-kata kunci : komputer kuantum,qubit, algoritma RSA, algoritma Shor.

ABSTRACT

BASICS OF QUANTUM COMPUTER AND ITS APPLICATION ON DECRYPTION OF RSA ALGORITHM

By

Fathiyya Izzatun Az-zahra
17/418523/PPA/05307

Theoretical study of basics of quantum computer has been studied. The basics of quantum computer which are reviewed are the concept of qubit, quantum logical operations, and entanglement. Qubit can be manipulated by using universal operator, i.e collections of two level unitary operators and single gate operators. The procedures of constructing a circuit based on universal operators and several expamples of constructing important circuits are explained.

One of the application of quantum computer is Shor's algorithm for factorization process. Complexity of Shor's algorithm is d^3. In the other hand, the best factorization algorithm in classical computer, which is GNFS algorithm, has complexity $\exp^{(\alpha d^{\frac{1}{3}})}$. Shor's algorithm can be applied to decrypt RSA algorithm by using equation $(M^e)^r = 1 \mod N$. Every step of Shor's algorithm and its quantum aspects are reviewed and explained mathematically in detail. Furthermore, this concept will be applied for simple problem. Suppose that an encrypted message $E(M) = M^e \mod N = 3$, then the decryption equation for $E(M)$ is $3^r \mod 8$. This equation is solved by using Shor's algorithm and representation of quantum circuit and matrices for this problem is presented.

Keywords : quantum computer, qubit, RSA algorithm, Shor algorithm.