INTISARI

IMPLEMENTASI MEKANIKA KUANTUM DALAM KRIPTOGRAFI KUANTUM

Oleh

Abdurrahman Wachid Shaffar
15/378001/PA/16476

Sebuah informasi penting tidak ingin dengan mudahnya diakses oleh sembarang orang, karena itulah keamanan informasi menjadi hal yang penting untuk dikaji. Kriptografi merupakan mekanisme pengamanan informasi dengan skema yang paling banyak digunakan adalah kriptografi kunci publik dengan menggunakan faktorisasi prima bilangan sebagai kunci rahasia. Di sisi lain, berkembangnya model komputasi baru yang disebut komputasi kuantum dengan memanfaatkan konsep mekanika kuantum membuat proses komputasi menjadi lebih efektif, dan melalui algoritma Shor (1994) maka membongkar kunci rahasia dari kriptografi kunci publik bukanlah suatu masalah. Diperlukan sebuah mekanisme keamanan baru yang bisa mengantisipasi terjadinya kebocoran informasi. Arthur Ekert (1991) mencetuskan sebuah mekanisme keamanan yang bisa mendeteksi adanya penyadapan (*eavesdropping*) pada saluran komunikasi yang digunakan. Mekanisme yang diberi nama protokol E91 memanfaatkan fenomena belitan kuantum (*quantum entanglement*) yang tunduk pada pertidaksamaan Bell untuk mendeteksi penyadap.

Pada penelitian ini telah diuraikan secara analitik proses yang terjadi pada komputer kuantum ketika menjalankan sirkuit kuantum protokol E91. Uraian matematis ini didasarkan pada konsep distribusi kunci kuantum, dicontohkan oleh Ani dan Budi yang ingin bertukar informasi rahasia melalui saluran kuantum, informasi tersebut diwakilkan dalam bentuk superposisi keadaan *qubit* tunggal $|\psi\rangle$. Sirkuit kuantum yang digunakan dibangun oleh Satsangi dan Patvardhan (2015) yang diberi nama sirkuit teleportasi kuantum. Uraian matematis menunjukkan adanya proses enkripsi dan dekripsi pada keadaan *qubit* selama proses operasi dalam sirkuit kuantum. Hasil analitik yang diuraikan dibandingkan dengan hasil komputasi kuantum dengan Qiskit dan didapatkan kesamaan pada keadaan akhir *qubit*, metode yang sama diujikan juga pada sembarang keadaan *qubit* dan diadapatkan hasil yang konsisten.

Kata-kata kunci : distribusi kunci kuantum, qiskit, sirkuit kuantum.

ABSTRACT

QUANTUM MECHANICS IMPLEMENTATION IN QUANTUM CRYPTOGRAPHY

By

Abdurrahman Wachid Shaffar
15/378001/PA/16476

An important information does not want to be easily accessed by anyone, that's why information security becomes an important thing to study. Cryptography is an information security mechanism with the most widely used scheme is public key cryptography by using prime factorization as a secret key. On the other hand, the development of a new computational model called quantum computing by utilizing the concept of quantum mechanics makes the computational process more effective, and through the Shor (1994) algorithm, revealing the secret key from public key cryptography is not a problem. A new security mechanism is needed that can anticipate information leaks. Arthur Ekert (1991) discovered a security mechanism that could detect eavesdropping on the communication channel used. The mechanism named E91 protocol utilizes the phenomenon of quantum entanglement which is subject to Bell's inequality to detect eavesdroppers.

This research has analyzed analytically the processes that occur in quantum computers when running the E91 protocol quantum circuit. This mathematical description is based on the concept of quantum key distribution, by utilizing photons in entangled state as a medium for delivering information in the form of keys. Exemplified by Ani and Budi who want to exchange confidential information through quantum channels, this information is represented in the form of superposition of a single qubit state. The quantum circuit used was built by Satsangi and Patvardhan (2015) was called quantum teleportation circuit. Mathematical description shows the existence of the encryption and decryption process of the qubit state during the operation process in the quantum circuit. The analytical results described are compared with the results of quantum computation with Qiskit and similarities are found in the final qubit state. The same method is also tested in any qubit state and consistent results are obtained.

Keywords : quantum key distribution, qiskit, quantum circuits.