UNIVERSITAS
GADJAH MADA
Analisis Kerja Belitan Kuantum Pada Kriptografi Kuantum
ADRIAN AFFAN MUTTAQIN, Drs. Pekik Nurwantoro, M.S., Ph.D.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

INTISARI

ANALISIS KERJA BELITAN KUANTUM PADA KRIPTOGRAFI KUANTUM

Oleh

Adrian Affan Muttaqin
15/383160/PA/16820

Kriptografi merupakan mekanisme pengaman informasi dengan berbagai skema. Salah satu cara untuk membuat kriptografi menjadi lebih baik dengan memanfaatkan kriptografi kuantum dengan belitan kuantum. Oleh karena itu, fokus pada penelitian ini dengan menganalisa cara kerja belitan kuantum yang memanfaatkan protokol BB84 dan protokol E91 sebagai mekanisme untuk mengetahui adanya penyadapan(*eavesdropping*) pada saluran yang digunakan. Penelitian ini dilakukan dengan pengamatan pada protokol BB84 dan E91 dengan Budi dan Ani sebagai dua orang yang saling bertukar informasi.

Hasil dari penelitian ini, protokol BB84 dan protokol E91 menunjukkan belitan kuantum membawa informasi dengan menukarkan pengamatan antara satu bagian dengan bagian lain sehingga dihasilkan 0 maupun 1 yang akan dienkripsi menjadi informasi dalam bahasa komputer kuantum. Protokol E91 menunjukkan bahwa, belitan kuantum tidak dapat digandakan dikarenakan superposisi yang menyebabkan spin ↑↓ secara bersamaan sehingga. dibutuhkan pengamatan untuk menentukannya. Protokol E91 menunjukkan perubahan filter akan merubah hasil pengamatan, sehingga bisa dipastikan pengkloningan tidak dapat dilakukan pada distribusi kunci kuantum.

Kata-kata Kunci : kriptografi kuantum, protokol BB84, protokol E91, belitan kuantum

UNIVERSITAS
GADJAH MADA
Analisis Kerja Belitan Kuantum Pada Kriptografi Kuantum
ADRIAN AFFAN MUTTAQIN, Drs. Pekik Nurwantoro, M.S., Ph.D.
Universitas Gadjah Mada, 2023 | Diunduh dari http://etd.repository.ugm.ac.id/

ABSTRACT

ANALISIS KERJA BELITAN KUANTUM PADA KRIPTOGRAFI KUANTUM

by

Adrian Affan Muttaqin
15/383160/PA/16820

Cryptography is an information security mechanism with various schemes. One way to make cryptography better is by utilizing quantum cryptography with quantum entanglement. Therefore, the focus of this research is to analyze how quantum entanglement works using the BB84 protocol and the E91 protocol as a mechanism to detect eavesdropping on the channel used. This research was conducted by observing the BB84 and E91 protocols with Budi and Ani as two people exchanging information.

The results of this study, the BB84 protocol and the E91 protocol show that quantum entanglement carries information by exchanging observations between one part and another so that 0's and 1's are produced which will be encrypted into information in the language of a quantum computer. Protocol E91 shows that, quantum entanglement cannot be multiplied due to superposition causing spins ↑↓ simultaneously so that. observation is needed to determine it. The E91 protocol shows that filter changes will change the observation results, so that cloning cannot be done on the quantum key distribution.

Key Words : quantum cryptography, protocol BB84, protocol E91, quantum entanglement