要 旨

量子暗号 E91 シミュレータ

坂本 泰之

要旨

現代社会はインターネットの普及によってますます情報の流通は拡大しており, セキュリティの確保は必要不可欠なものとなっている. そしてそのセキュリティの確保に使われているものが暗号である. 情報化社会である現在, 暗号技術による情報の秘匿性や非改ざんは大変重要な意味を持つ. 現在の通信方式の安全性は NP 問題に依存したものであり, この問題が解決されると安全性が保証できなくなってしまう. 量子暗号による通信は従来の通信方式とは異なる方法で通信を行い, 安全に通信を行うことができる.

本稿ではいくつかある量子暗号プロトコルの内, E91 プロトコルを取り上げ, コンピュータ上にシミュレータを実現, その動作結果を確認する. そして盗聴者の存在検知や通信効率に関する統計的性質を調べる.

キーワード　量子暗号,E91 プロトコル, エンタングル状態, キュビット

Abstract

E91 Quantum Simulator

Yasuyuki Sakamoto

Summary

Because of the phenomenal increase of information exchange through internet in modern society, the security of communication is essential, which is provided solely by the cryptography. With the current open-key cryptography, the security is guaranteed by the intractability of NP problem, and the potential solution of NP problems in polynomial time by quantum computation threatens this essential security. With quantum cryptography, the security of communication is guaranteed by physical principle of quantum uncertainty, thus is unbreakable. In this work, among several proposed quantum cryptography, we examine E91 protocol which utilizes quantum entanglement. We construct a simulator of E91 protocol on computer, in order to understand the detailed workings of quantum cryptography. We also study the statistical properties of E91 communication under the noise to examine the robustness of E91 protocol in realistic environment.

key words Quantum cryptography, E91 protocol, Entangled state, qubit