要 旨

量子暗号 B92 シミュレータ

松本 聡一郎

要旨

現代社会はインターネットの急速な普及により，とても便利になっている．コンピュータで自宅から銀行口座に振り込んだり，通信販売を利用する事も可能である．これはひとえに暗号が個人情報などの秘密情報を他人には読み取れない形にしているからである．一般的に暗号は第三者が解読するためには長い時間を必要とするよう作られているうえ，技術の進歩により暗号は更に複雑化している．しかし現代暗号は量子コンピュータが登場した事により，現代のコンピュータで解読に数億年単位の時間が掛かる暗号もわずか数日で解読されてしまう可能性があることが判明した．そのため新たな暗号として，量子暗号が注目されている．現段階では BB84 という量子暗号が研究機関での主な研究対象となっている．ここでは BB84 と E91 の発展型とされる B92 に注目し研究することとした．

第 2 章では量子暗号の安全性を証明する原理である“ 不確定性原理 ”と“ 重ね合わせ原理 ”を解説する．第 3 章では実際の量子暗号プロトコルである B92 を取り上げて説明する．第 4 章では第 3 章で取り上げた量子暗号プロトコルのシミュレータの詳しい動作を順を追って説明する．第 5 章では理論的共有成功率と，作成したシミュレータプログラムを用いて求めた実測共有成功率を比較し，観測者の行動如何で共有率に影響が出るかも観測する．また，ノイズによってデータが変化する場合も想定してシミュレータプログラムを修正し，実測データからどの程度ノイズに強いのかも判定する．最終的な結果から，新たに発見した B92 の性質も書く．

キーワード　量子暗号，電子，秘密鍵，不確定性，重ね合わせ，盗聴，観測，内積, ノイズ

Abstract

B92 Quantum cryptography simulator

Soichiro MATSUMOTO

English

Nowadays, the public key cryptosystem is widely used to provide security for internet shoppings and bankings. The public key cryptosystem is known to be efficiently deciphered by the Shor's quantum algorithm. A new cryptography has emerged in the shape of the quantum cryptography. In this article, we examine B92 protocol which is one of the quntum cryptography. In chapter 2, we explain the uncertainty principle and superposition principle. In chapter 3, we explain the B92 Quantum cryptography. In chapter 4, we explain the operation of the B92 quantum cryptography simulator. In chapter 5, we examin the statistical properties of B92 protocols.

key words Quantum cryptography, Electron, Secret key, Uncertainty principle, Superposition principle, Wiretapping, Observation, Inner product, Noise