要 旨

量子暗号 BB84 シミュレータ

中本　衡

要旨

現代の社会において，情報の交換にはインターネットが利用される場合がほとんどである．そして，インターネットを利用した情報交換では暗号が使用され，情報をより安全に交換することが可能となっている．技術の進歩とともに暗号化技術もより複雑なものが用いられるようになり，一般的に暗号を解読するためには膨大な時間をかけるしかないように設計されている．しかし，現在開発研究されている量子計算機が実用化されれば，話は別である． Shor のアルゴリズムと呼ばれる量子アルゴリズムを用いることで，既存のコンピュータを用いて解読に数億年から数兆年かかる暗号ですら，わずか数日で解読される可能性が予測されたからである．この問題に対して新しく考えられた暗号が量子暗号である．第 2 章では，量子暗号が考案されるに至った経緯として現代暗号について簡単に解説を行った．第 3 章では，量子暗号を理解する上で必要である「量子状態」,「不確定性原理」,「重ね合わせの原理」について詳しく解説を行った．第 4 章，量子暗号の中で最も基本となる「BB84 プロトコル」について詳しく書いた．第 5 章では，実際に行った数値実験の内容の解説を書いた．最終章では，現在の量子暗号における問題点と今後の展望について書いている．

キーワード　公開鍵暗号，秘密鍵暗号，量子力学，量子状態，量子ビット，量子暗号，BB84，重ね合わせの原理，不確定性原理，盗聴，ノイズ

Abstract

Quantum cryptography BB84 Simulator

Kou Nakamoto

The internet has become the primary means of information exchanges in modern society. In order to guarantee the security of the internet, cryptographic technology is crucial. With the emergence of quantum computation, security of even most modern cryptography is in danger. That is where quantum cryptography comes in for rescue. In this work, we construct a simulator of quantum cryptography on classical computers, and examine its working in detail to understand how quantum cryptography works. In chapter 2, we review the modern classical cryptography as the background. In chapter 3, we present the basics of quantum theory that form the basis for the quantum cryptography. In chapter 4, we present detailed explanations of the BB84 protocol which is the most basic of quantum cryptography. In chapter 5, we lay out the numerical and statistical analysis of BB84 using our simulator. In the last chapter, we examine the problems and the prospects of quantum cryptography.

key words Public key cryptosystem, Secret key cryptosystem, Quantum mechanics, Quantum state, Quantum bits, Quantum cryptography, BB84, Superposition principle, Uncertainty principle, Wiretapping, noise