要 旨

古典暗号と量子暗号の比較研究

戸田　知憲

要旨

現代社会において，インターネットなどで情報交換する際には必ずといっていいほど暗号が使われている．技術の進歩により暗号化も複雑なものが用いられており，一般に解読には長い時間をかける必要があるように設計されている．しかし，現在研究開発が行われている量子コンピュータが実用段階に入れば話は別である．Shor のアルゴリズムによって，現在のコンピュータでは解読に数億年〜数兆年かかる暗号ですら，数日で解読されてしまうことが予測されたからである．そのため，新たな暗号方式が求められている．第 2 章は古典暗号，特に現代暗号の DES や RSA 暗号について詳しく書いた．第 3 章では量子暗号を学ぶ上で必要だと思われる量子論についてわかりやすく書いている．第 4 章，第 5 章では実際の量子暗号について書いた．第 6 章では今後の量子暗号に応用可能な量子力学の現象について書いてある．最終章では現代の暗号と量子暗号を比較したうえで今後の展開について書いてある．

キーワード　暗号，古典暗号，現代暗号，共通鍵暗号，秘密鍵暗号，公開鍵暗号，Data Encryption Stanard，DES，RSA 暗号，量子論，不確定性原理，重ね合わせの原理，量子ビット，量子エンタングルメント，量子テレポーテーション，エンタングルメント・スワッピング量子暗号，量子鍵配送，BB84，E91

Abstract

Comparison research on Classics code and Quantum cryptography

tomonori toda

English

In today's society with ubiquitous internet, the importance of information security cannot be overstated. The security of encryption of internet traffic is guaranteed by schemes that are based on computational complexity. However, the rapid advances in quantum information technology is starting to threaten this security, because the quantum computation is known to provide massive parallelism that renders current encryption techniques obsolete. Fortunately, the same quantum technology comes for the rescue by providing us new schemes of encryption based not on the computational complexity, but on the security in code sharing. In this work, we provide a comparative review of both classical cryptography which is now under active use, and quantum cryptography which holds the hope of absolute information security. The construction of this review is as follows. In chapter 2, we review DES and RSA cryptographies as representatives of modern cryptography. In chapter 3, we introduce minimal quantum mechanics as is needed in the following chapters. Chapters 4 and 5 contain the detail description of BB84 and E91, two representative schemes in quantum cryptography. In chapters 6 and 7, we attempt a brief illustration of the technique of quantum teleportation which is at the core of recent new directions in quantum cryptography.

key words Code, Classics code, Present age code, Smmetric-key encryption, Secret key cryptosystem, Public key cryptosystem, Data Encryption Stanard, DES, RSA code Quantum theory, Indeterminacy principle, Superposition principle, Quantum bits, Quantum entanglement, Quantum teleportation, Entanglement swapping, Quantum code, Quantum key distribution, BB84, E91