量子暗号　Ｅ 91

発表者　山根　基文
指導教官　賀数清孝

概要

ここ十数年の間にＰＣとインターネットは信じられないほど爆発的に普及した。ＰＣは日々進化し、インターネットは情報で溢れかえっている。そして今や情報化社会といわれるまでになってきており、ＰＣとインターネットは社会的インフラの地位を得つつある。しかしその裏で、私達の情報、プライバシーなどが常に危険にさらされる事になっている。

そうした情報を守るために、安全な暗号の重要性が高まっている。そもそも暗号はカエサル暗号までさかのぼるとされている。かの有名なカエサルが使用していたとされる暗号とは、平文をアルファベット順にある数だけずらすというものであった。ローマ帝国の時代からすでに暗号の重要性は高かったようである。

現在広く使われている暗号として、ＲＳＡ暗号がある。それは因数分解の難解さに着目した暗号である。暗号文を受け取りたい人は、ある素数同士を掛け合わせた巨大な数を公表して、それを使って暗号化してもらう。暗号文を受け取った後に、その人はその数の素数を基に復号化する。素数がわからないと復号化できないので、盗聴者は巨大な数を素因数分解しようとするが至難の業である。素数同士を掛け合わせるのは簡単なのに、である。だが、量子力学を使用した量子コンピューターが実用化されれば、その難解さは低下し、解読される可能性が高いことがすでに示されている。それはもはや暗号ではない。

では、量子コンピューターが実用化された後にも、暗号を暗号たらしめるにはどうすればよいか？そのために量子コンピューターと同様に、暗号でも量子力学を使用することが考えられている。有名な量子暗号としては、ＢＢ８４プロトコルが挙げられる。これは、量子力学において、ある量子状態のｑｕｂｉｔは決して複製することはできないという定理から安全性が保障されている。

タイトルのＥ 91 プロトコルでは、送信者と受信者がおり、そこでもつれ合ったＥＰＲ対の特性と、ベルの不等式を利用して、盗聴者の発見と鍵の配布が行われる。このことについて述べていく予定である。