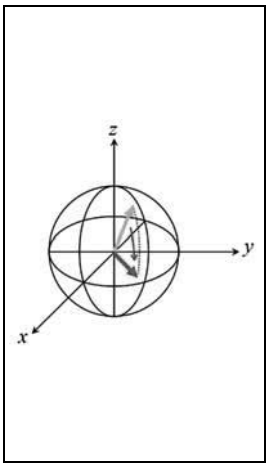

長距離量子暗号

大阪大学
井元信之

１．はじめに

通信の内容が第三者に漏れないようにするために，太古より暗号が使われている。暗号はいずれ破られ，さらに強力な暗号が考案され，それもまた破られるというイタチごっこで進歩してきた。ここにきて従来と毛色の異なる量子暗号が生まれ，それは「絶対破られない暗号」と喧伝されることがある。むろん現実はそう単純ではない。しかし現実を理想に近づけるべく努力するにつれ，従来の暗号とは異次元の可能性も見えて来る。そればかりでなく従来の情報処理との絡み合いも深くかつ多様化して来ており，分野として分離させておくことは必ずしも得策ではなくなって来ている。

量子暗号は通信の一種なので，その実現には光技術が欠かせない。しかし通常の光通信では問題にならないことが問題になるなど，技術的ハードルが上がり，特に長距離になるといろいろな問題が顕在化して来る。長距離とはどれほどかというと，要求する通信速度にもよるが，オーダーとして 100 km を越すと課題が多様かつ困難になり，より根本レベルでの解決が望まれる。ここに，大学より企業の方が強くなってきた感のある量子暗号にあって，大学での基礎研究も必要とされる理由がある。

本稿では，量子暗号とは何か，課題は何か，新しい可能性は何かを解説し，世界の情勢がどうなっているかを概観し，中でも長距離化の問題点とその解決に向けて取ってきたアプローチ，そして今後の考えられるアプローチについて解説する。そこで中心となるのは光技術である。

２．量子暗号とは

2-1　量子以前の暗号

量子暗号を知るためには，暗号の一般論を知る必要がある。暗号とは，送信者（暗号分野の慣習に従ってアリスと呼ぶ）がオリジナルメッセージを適当に変換して暗号文にし，それを受け取った受信者（ボブと呼ぶ）が逆変換して元のメッセージに戻すものである。量子暗号以前の現在流布している暗号（現代暗号と呼ぶが，本稿では量子物理と古典物理の対句を踏襲して古典暗号と呼ぶ）では，通信路自体の安全性はないという前提に立つ。すなわち，アリスとボブ以外の第三者も暗号文を手にすることができ，それもアリスとボブに気づかれないように傍受することができるという前提に立つ。言い換えれば暗号文は公開されているに等しいので，そこには盗聴者という概念がない。したがってこの暗号の安全性（＝秘匿性）は，第三者が暗号文を解読し元のメッセージを復元することができてしまう確率を如何に小さくできるかに依存する。古典暗号には以下に述べる（1）秘密鍵暗号と（2）公開鍵暗号がある。量子暗号は実は秘密鍵暗号を構成する前段階の「鍵配送」と後段階の「暗号文の通信」のうち鍵配送を安全に行うものである。（2）の公開鍵暗号はコンピューターの進歩（特に量子コンピューターの出現）により破れてしまうことが予想されているが，量子暗号を用いた秘密鍵暗号は破れることはない。

（1）秘密鍵暗号

《概念》他人に知られていない乱数表（＝秘密鍵）をアリスとボブが共通の鍵として事前に保有していて，アリスはメッセージを数字に直したもの（たとえば文章を JIS コードの羅列にしたときにでき