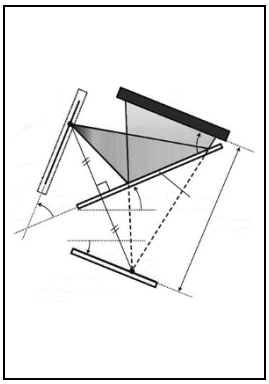

Society 5.0 時代の産業基盤に不可欠な暗号技術(Y-00 量子ストリーム暗号)の開発

玉川大学　量子情報科学研究所
廣田　修，相馬正宜

１．はじめに

本稿では，最初に Society5.0 時代のセキュリティ技術の要となる耐量子コンピュータ暗号開発の基本的な概念と，その目的に答える技術として現在，研究・開発されている数理暗号と量子暗号の位置づけを紹介する。次に，その技術開発において中核的な技術として期待されている「量子情報理論に基づいて通信路上の信号を盗聴させないことを安全性保証原理とする量子暗号」の詳細を説明し，それらを実用化するための研究活動などを紹介する。

２．Society 5.0 における暗号技術の考え方

2-1　秘匿用暗号の分類と基地局間通信セキュリティ保護技術

暗号学の権威として活躍されている辻井重男：東工大名誉教授は，セキュリティ業界の状況を以下のように説明している。「素因数分解や離散対数問題などの数学的解読困難性に依拠している RSA 暗号や楕円曲線暗号等の公開鍵暗号が，10 年以内に解読される程，量子コンピュータの実用化が速くはないが，今から制定する暗号方式に対しては，20 年～30 年の耐用を考える必要があるため，NIST では耐量子コンピュータ暗号の候補選定が進められている。また，秘匿用暗号の用途は，データ自体の秘匿伝送と，そのための鍵配送・保管に分類され，学術的手法の視点からは数理暗号と量子暗号に分けられる。数理暗号には，公開鍵暗号と共通鍵暗号があり，公開鍵暗号はデータ暗号化伝送の為の初期鍵を安全に配送・保管できる利点があるが，処理速度が遅いので，データ暗号化は共通鍵暗号が担っている。他方，量子暗号は量子現象を利用して安全性能を高める暗号技術である。公開鍵暗号が担っている鍵配送を量子通信で実行する技術は BB-84 量子鍵配送と呼ばれ，データ自体の暗号伝送を量子通信で実現する技術は Y-00 量子ストリーム暗号と呼ばれる(図 1 参照)」。さて，2 つの量子技術は共に，“量子情報理論に基づいて通信系を設計することで盗聴者が通信路上の信号を盗むことを困難にする”という概念に立脚している。このような信号自体を守る機能は数理暗号では実現できない。

これらの量子暗号技術のシステム運用法としては，鍵の配送を BB-84 量子鍵配送で送り，データの暗号化は従来の数理暗号を採用する方式と，認証と鍵配送は従来型の公開鍵暗号で送り，データの暗号化を Y-00 量子ストリーム暗号で実施する方式が考えられている。これらの量子暗号技術は図2のように次世代 5G や 6G のシステムにおける特別重要な基地局間の通信の究極的な安全性を確保する技術という位置づけである。以下に，その技術的内容と実社会での応用可能性，開発動向などを解説する。

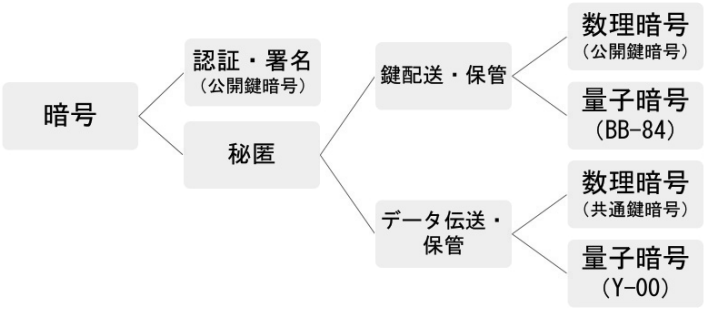

図 1　暗号技術の分類