情報通信研究機構
NICT先端研究 ㊸

究極の安全性保証 量子暗号装置を実現

電子や光子のミクロな世界を扱う量子力学という最新の物理学と、計算技術や通信技術を融合した量子情報技術は、従来技術の延長では不可能な抜本的な技術革新が可能になると期待され、情報通信研究機構（NICT）量子ICT先端開発センターでもその実現を目指した研究開発を進めている。

中心テーマの一つは、量子暗号である。現在の暗号方式は、将来的な計算技術の革新によって解読されてしまう危険性を常にはらんでおり、国家情報や医療情報など、機密性の高い情報の通信で重大な問題となる可能性が危惧されている。

量子暗号は、量子力学の不確定性原理に基づく光の揺らぎを活用した、これまでとは質的に異なる暗号通信で、実現すればいかなる計算能力を使っても原理的に解読不可能な究極の安全性を保証できる新しい技術である。我々はその実用化を目指し、東京圏に量子暗号の試験ネットワークを構築し長年実証実験に取り組み、世界最高性能の量子暗号装置を実現している。

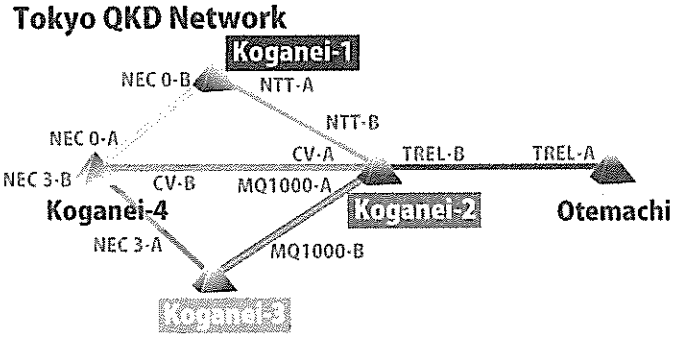
一方、量子情報は技術開発と基礎理論が同時進行で発展している研究分野である。現在のデジタル通信技術は、1948年にシャノンがその基本理論を確立し、その後、半世紀の技術革新を経て、今日の発展を迎えている。

だが量子暗号をはじめとする量子情報通信の場合、実は基礎理論の確立はまだ道半ばの状況だ。我々は実用化研究を進める傍ら、量子暗号・量子通信を背後から支配する基本法則を明らかにする理論の探求も進めてきた。

その結果、情報理論と量子物理の理論を適切に融合することで、現在実証されている量子暗号の原理的な性能限界や、ネットワークの複数ユーザーが協力してその限界を超える新しい可能性を示す理論の確立に成功している。こうした理論は、基礎科学として重要なだけでなく、量子暗号装置を新たに設計する際、どのような性能を目指すべきかというベンチマークを与え、技術開発においても重要な指針となる。

基礎・応用研究を同時に進めることで、量子現象の新しい応用が次々に実現されていくことを期待している。

（火曜日に掲載）



未来ICT研究所・量子ICT先端開発センター長　武岡 正裕

01年慶応義塾大学大学院博士課程修了。その後NICTで量子光学、量子情報理論、量子暗号の研究に従事。総務省勤務、米レイセオンBBNテクノロジーズ客員科学者を経て、16年より現職。