量子が支えるセキュアな社会技術基盤へ向けて

Quantum Cryptography - securing our future society

国立研究開発法人情報通信研究機構　○藤原 幹生

National institute of information and communications technology, ○Mikio Fujiwara

E-mail: fujiwara@nict.go.jp

ゲノムデータなど，世代を超えて秘匿しなければならない情報がインターネット上を行き来する時代であるにも関わらず，情報セキュリティの必要性に対しての認識が我が国の個人レベルでは希薄であることは否めない．計算機能力の向上や量子コンピュータの発展は現在我々が使用している暗号が数十年後には危殆化することを示唆しており，100 年を超す秘匿性を必要とする情報のやり取りに対し充分な耐性を有していない可能性を否定できない．現代暗号の研究分野でも耐量子計算機暗号の標準化に向けた活動がなされているが，轍鮒の急を有する情報セキュリティの安全性に対して我々は現在情報理論的に安全に暗号鍵を共有できる量子技術・量子鍵配送（QKD）技術の可能性を真剣に議論すべき時期である．NICT では国内の量子鍵配送研究機関とともに 2010 年より東京 QKD ネットワークを運用している．QKD 技術の高度化の他，ネットワーク化に向けたアーキテクチャ，QKD からの鍵を利用したアプリケーションの開発をすすめてきた．QKD 技術と現在の通信インフラとの融合は低コストでの普及に必須の技術である．また現在使用されているアプリケーションへの QKD ネットワークからの鍵を利用可能とするインターフェースの開発も量子技術を広く普及させるのに不可欠である．また QKD に必要な高速物理乱数発生器や鍵蒸留技術は QKD への適用のみならず，これからの IoT 社会での応用も期待できる．本講演では世界と我が国の QKD ネットワークの現状を紹介するとともに，2016 年度には一つのパスワードだけを用いても，認証・伝送・保存・復元を情報理論的に安全に実行できる分散ストレージを東京 QKD ネットワーク上に構築しデモンストレーションを行った[1]結果を報告し，量子技術のセキュアな社会インフラとしての成果イメージを報告する．

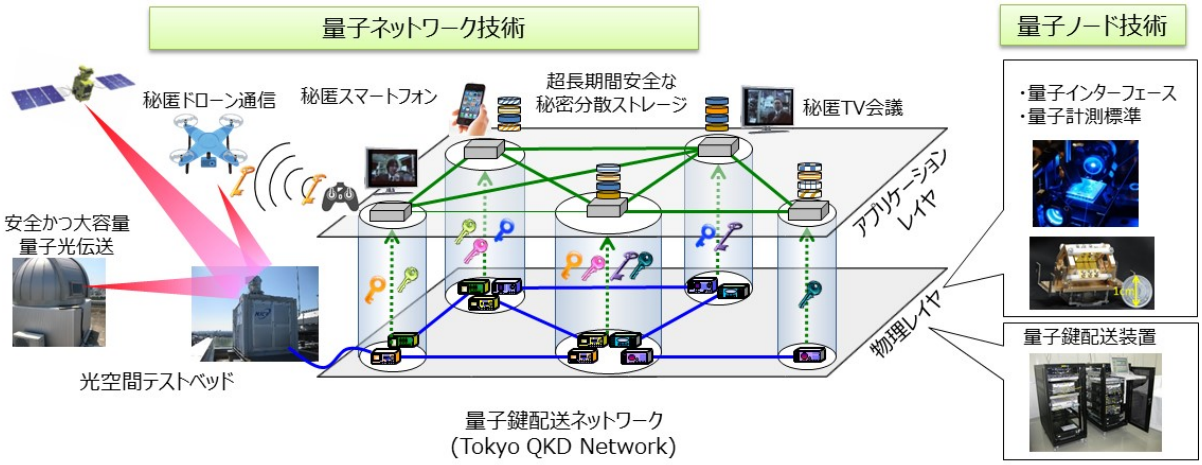

図 1　NICT が取り組む社会実装を目指した量子技術

(1) M. Fujiwara et al., Scientific Reports, 6:28988 (2016).