【基盤研究（S）】

大区分Ｃ

研究課題名　百年以上の超長期秘匿性を保証する情報通信ネットワーク基盤技術

北海道大学・大学院情報科学研究科・教授　富田（とみた）　章久（あきひさ）

研究課題番号：18H05237　研究者番号：60501434
キーワード：情報理論、ネットワーク、暗号

【研究の背景・目的】

近年、ゲノムデータや製薬情報など長期間秘匿性を担保する必要のある情報を電子的に伝送、保管、処理することが進められている。例えばゲノムデータはヒトの寿命を考えれば少なくとも百年は安全に保管されるべきである。ところが、現代の暗号は 20 年から 30 年ごとに世代交代が繰り返されている。現在の技術で暗号化された情報が百年以上たった後も安全であるとは考えにくい。

そこで、本研究では、将来いかに技術が進歩しても安全性が保たれる、情報理論的安全な情報保管ネットワークの基盤技術を開発する。安全な情報保管のために秘密分散を用いる。また、量子暗号鍵配送（QKD）技術によって秘密分散ネットワークを安全にする利用するために必要な秘匿通信を行う。最終的に、情報理論的に安全なデータの中継と保存、秘匿計算・復元を行うネットワークを実現可能とする。

【研究の方法】

本研究で実現を目指すネットワークの構成の概略を図 1 に示す。秘密分散サーバにおいてマルチユーザ化、サーバ同期、秘匿計算などネットワークに必要な機能を実現する。ユーザ-サーバ間・サーバ-サーバ間では近距離高速な QKD リンクを利用して鍵を共有してデータの秘匿伝送を行う。離れたエンドユーザ間でも長距離伝送可能な QKD リンクによって短いパスワードを共有して認証を行うことで情報理論的に安全なデータ中継が可能になる。

本研究は①ネットワーク構築技術、②長距離 QKD 技術、③近距離高速 QKD 技術、④安全性保証・効率的な鍵生成プロトコル理論の 4 つについて行う。前半では候補となる方式の実現性を理論と実験の両面から精査する。これにより情報理論的安全なネットワーク、長距離(100-300km)QKD リンク、高速（1TB データ転送）かつ光通信と共存する QKD リンクのそれぞれを実現する方式を決定する。後半では装置の製作およびそれらを取りまとめるシステム設計とソフトウェア開発、統合システムの動作実証を行う。

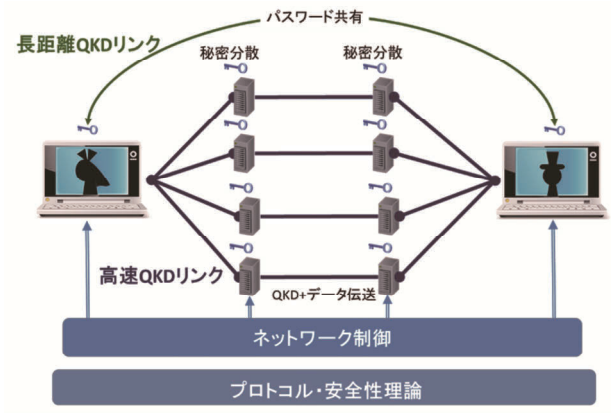

図１　情報理論的安全なネットワーク構成

【期待される成果と意義】

本研究は情報理論的な現代暗号技術と量子鍵配送技術との融合によって長期間秘匿性を保つことができる情報通信ネットワークを実現するものである。ここで実現される光量子ネットワーク基盤技術は高速光通信技術、標準技術、暗号技術等の IT 技術と量子情報技術が結び付いた世界に先駆けたものである。従来、情報理論的安全な暗号技術や QKD 技術は、将来的な可能性はあるものの実用には適さないとも考えられていた。それに対し本研究では両者の長所を組み合わせて真に実用可能なネットワーク基盤を確立し、超長期間の情報の安全性を担保する新たな枠組みを構築する。さらに要素技術として開発する光パルスの同期やレーザの位相・周波数制御は光通信の高度化にも寄与する。

【当該研究課題と関連の深い論文・著書】

・K. Nakata, A. Tomita, M. Fujiwara, K. Yoshino, A. Tajima, A. Okamoto, and K. Ogawa," Intensity fluctuation of a gain-switched semiconductor laser for quantum key distribution system," Optics Express, **25**,622-634 (2017)
・M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, O. Wakaha, and M. Sasaki, "Unbreakable distributed storage with quantum key distribution network and password authenticated secret sharing," Scientific Reports, **6**: 29988, 1-8 (2016).

【研究期間と研究経費】

平成 30 年度－34 年度
148,200 千円

【ホームページ等】

http://www.eng.hokudai.ac.jp/labo/hikari/index.htm