科学研究費助成事業（基盤研究（Ｓ））公表用資料
〔令和２(2020)年度 中間評価用〕

平成　30 年度採択分
令和２年３月３１日現在

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

Information communication technology ensuring the long term security over a century

課題番号：18H05237

富田　章久（TOMITA, AKIHISA）

北海道大学・大学院情報科学研究院・教授

研究の概要（４行以内）
秘密分散に代表される情報理論的安全な暗号技術と QKD による鍵共有を融合させ、秘匿情報を伝送・保管・処理する秘匿情報通信ネットワークを構想した。本研究では「現実に意味のある融合システムの構築」および「融合システムの実現に対して十分な性能を持つ QKD 装置の開発」の２点に取り組み、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を確立する。

研　究　分　野：電気電子工学

キ　ー　ワ　ー　ド：情報通信ネットワーク基盤 / 情報理論的安全 / 量子暗号鍵配送 / 秘密分散 / 量子鍵配送 / 量子通信 / 量子ネットワーク / 安全性保証

１．研究開始当初の背景

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の電子的な伝送、保管、処理が進められている。ここでいう長期間とはヒトの寿命、百年以上を意味する。

しかし、現代暗号は長期間のうちに危殆化し、世代交代が必要となる。傍受されたデータが長期間解読されないことを保証できる暗号技術を用いた秘匿情報通信ネットワークの実現が望まれる。

２．研究の目的

本研究では情報理論的に安全な暗号技術と量子技術のお互いの長所を生かしつつ欠点を補う融合システムを構築する。具体的には秘密分散と量子暗号鍵配送（QKD）の融合により、超長期安全性を保証する情報通信ネットワーク基盤を実現する。そのために、ネットワーク構築技術の開発と QKD 技術の高度化を行い、それらを統合したネットワークを研究開発する。

３．研究の方法

提案している秘匿情報通信ネットワークは秘密分散サーバを QKD リンクで構成される。

QKD と連携が可能な秘密分散を開発する。秘密分散 - QKD 融合ネットワーク制御も研究し、両者を合わせてネットワークを構築する。

QKD リンクは離れたユーザ間の秘密共有を可能にするための長距離リンクと、ユーザ-サーバ間、サーバクラスター内の通信を行う近距離高速リンクが必要になる。北それぞれの用途に適した QKD リンクを研究開発する。

秘匿情報通信ネットワークにおいては現実の不完全な装置における安全性の保証が重要であり、そのための理論研究を行う。実装されたシステムについて実験を担当するグループと連携して安全性保証を行う。

具体的な研究項目は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秘密分散－QKD ネットワーク理論の４つとし、それぞれ NICT、北海道大学、学習院大学、富山大学が主に担当する。共通する技術について知見を共有しつつ研究開発を進め、最終年度に統合システムの実証を行う。

４．これまでの成果

①ネットワーク構築技術：データ中継時において、正しい相手にパスワード情報を伝送する認証機能を持つシステムを開発している。また、QKD で供給される乱数を用いて情報理論的安全なデータの完全性保証を第三者により実施できるシステムを実現した。

②長距離 QKD 技術：送信される光パルスの光子数を事後的に制御して実効的に単一光子に近づける QKD プロトコルを提案し、シミュレーションで効果を確認した。

光子検出器の暗計数の影響を低減できる測定装置無依存型（MDI）QKD については装置の不完全性によって生じる光パルスの識別可能性の影響と許容範囲を数値的に示した。また、MDI-QKD 実現の鍵となるパルス同期を中間点での測定と補償で完結する実用的な手法を考案した。

実際の装置での安全性保証に適用できるトモグラフィによる量子状態評価法を開発した。この方法を BB84 プロトコルの量子状態に用い、高速 QKD システムでの位相による量子状態生成には Dual Parallel Modulator が有効であることも示した。

③近距離高速 QKD 技術:連続変数 QKD(CV-QKD)を選択した。CV-QKD では受信機での局部発振光の独立が重要である。光注入同期を用いる手法と電気的なフィードバックを用いる手法について研究している。前者では、パイロット光を音響光学素子を用いて周波数をずらし、波長分割多重で伝送して光注入同期により局部発振光を作る方法を考案し、位相の安定化に成功した。後者ではパイロット光を時分割伝送する手法を研究した。広帯域低雑音のホモダイン検出技術を開発し、コスタス回路と組み合わせて動作を検証した。

CVQKD と光通信との共存については、 100 波のコヒーレント光通信と CVQKD を共存させる実験に成功した。CVQKD を既設の光ファイバと多重化することで、低コストに量子鍵配送が可能であることを示した。

④秘密分散-QKD ネットワーク理論：QKD 装置における光源がもつ不完全性を考慮した安全性理論の構築を行った。検証可能かつ光源の広範囲な不完全性に対応できる安全性理論や、新たに考案した送信光の一般的な状態記述の方法に基づく安全性理論を構築した。また、CV-QKD について局部発振光がコヒーレント光である保証を要さない安全性証明のアイディアを得た。

５．今後の計画

当面は担当項目の研究を進める。技術内容には共通するものもあり、また、ネットワークと QKD システム、理論と実験の間での連携が必要なため、年 2 回の全体会合の他、随時関係する研究者間で議論しながら効率的に研究開発を進める。最終年度には成果を統合してネットワーク上での機能実証を目指す。

① ネットワーク構築技術

2020 年度では Tokyo QKD Network 上での長期安定性試験と、スループット計測を実施する。また実用性を向上するためのソフトウェアの改良を進める。その後は、秘匿計算の充実を図り、量子鍵配送ネットワークを用いた、安全なデータの二次利用を可能とする機能の実装を図る。

② 長距離 QKD 技術

2020 年度にプロトコル実証のための量子もつれ光源を開発する。原理実証の後、鍵蒸留部を整備し、QKD システム動作を検証する。

MDI-QKD では送信部を構築する。同時に位相ずれの検出と補償を行う PLL を設計試作し、パルス同期を実証する。

実験的な安全性保証では量子状態計測法を確立する。また、光子数分布の評価系を開発する。

③ 近距離高速 QKD 技術

局部発振器の独立に関して、光注入同期による方式では、信号光を一光子以下の微弱なレベルで動作させるとともに、過剰雑音を定量的に評価し、理論計算と動作パラメータを合わせることにより、実際に安全な鍵の生成を 2020 年度内に実現すること目指す。

コスタス回路を用いる方式は高速化に有利と考えられるので、高速化のための研究を進め、やはり単一光子レベル以下での QKD 動作の実証を行う。また、制御装置と自動運転プログラムの整備を進める。

光通信との共存については、これまでの原理実証実験の問題点を改善し、安定性の向上などの研究開発を行う。

④ 秘密分散-QKD ネットワーク理論

これまでに構築した光源の不完全性に対する安全性理論を測定装置無依存型量子鍵配送（MDI-QKD）への拡張を行う。また、パルス数が有限な場合に拡張する。

また、局部発信器を独立させた高速 QKD リンクの安全性証に関しては考案したアイディアの適用可能範囲を明確化する。

６．これまでの発表論文等（受賞等も含む）

○ “State preparation robust to modulation signal degradation by dual parallel modulator for high-speed BB84 quantum key distribution systems,” W. Zhang, Y. Kadasawa, A. Tomita*, K. Ogawa, and A. Okamoto, Optics Express, to be published (2020).

○ “Quantum key distribution with flawed and leaky sources,” M. Pereira*, M. Curty, and K. Tamaki, npj Quantum Inf **5**, 62 (2019).

○ “Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels,” T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada and M. Sasaki, Communications Physics **2**(1), 9 (2019).

他 5 件

知的財産権等：光秘匿通信システム，中沢 正隆，吉田 真人，廣岡 俊彦，平野 琢也，特許第 6471903 号，登録年月日 2019/2/1

招待講演：“Implementation Security Certification of Quantum Key Distribution Devices,” Akihisa Tomita, Topical Conference on Quantum Communication and Security, Kyoto, December (2019). 他 6 件

国際会議 11 件，国内学会発表 6 件

7．ホームページ等（準備中）