様式 C-19

科学研究費補助金研究成果報告書

平成２１年６月２２日現在

研究種目：若手研究（Ｂ）
研究期間：2006～2008
課題番号：18760291
研究課題名（和文）　量子情報セキュリティ技術を取り入れた情報基盤設計のための基礎研究

研究課題名（英文）　Quantum Information Security, As a Practical Tool

研究代表者 今福健太郎（IMAFUKU KENTARO）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・物理解析研究チーム・チーム長
研究者番号：10298169

研究成果の概要：
本研究では、技術的に成熟期を迎えつつある量子暗号について、情報セキュリティ技術として導入するために必要な検討課題の抽出、およびその検討、さらに検討を精緻化するために必要な研究課題の洗い出しを行った。いわゆる暗号理論における安全性証明とは別に、想定する安全性を達成するために装置が満たしているべきと考えられる仕様(いわゆるセキュリティ要件)について、量子暗号装置についても整理することを提案、整理の仕方について議論を行った。また、いわゆる量子鍵配送とは別に、量子状態を使って古典情報を直接量子状態の中に秘匿して一方向コミュニケーションでやりとりする方式について､秘匿通信におけるシャノン限界で、量子論的なアドバンテージが消滅することを示し報告、さらに、このような方式について新しい提案の安全性を確認に用いることができる要件をチャートの形で整理した。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
2006 年度	1,000,000	0	1,000,000
2007 年度	700,000	0	700,000
2008 年度	700,000	210,000	910,000
年度			
年度			
総　計	2,400,000	210,000	2,610,000

研究分野：工学
科研費の分科・細目：電気電子工学・通信・ネットワーク工学
キーワード：量子情報セキュリティ

１．研究開始当初の背景

人々の社会活動の根幹を支える金融、電力、交通などの重要インフラに対し、その制御・管理を行う情報通信システムは、その「神経系」としての役割を日々増大させている。このような広域情報通信システムは、いわば「インフラのためのインフラ」として位置づけられ、サイバーテロなどに代表されるある種の攻撃への耐性を考慮したシステムの構築が、安全で安定した社会の実現に向け大きな課題の一つとなっている。
一方、近年、究極の安全性を効率よく達成するとされるいわゆる量子暗号技術の研究開発は、その基本的成果が徐々に開花しつつあり、商品化を含めた競争的研究開発が加速している状況にある。量子光学技術の著しい発

展を背景とし、ある種の量子鍵配送プロトコル（ＢＢ８４）が、実験室レベルを超えフィールドレベルにおいて実装されるまでに至った。またこのようなシステムについては、すでに商品化され販売が行われているだけでなく、それらを対象とした輸出入規制に関する国際的な議論が、ワッセナーアレンジメントの枠組みで行われている状況にある。現在のところ、さまざまな技術的制約により、理論的に「無条件」安全性を達成することができる物理的状況は、せいぜい通信距離 40km 程度（速度は最大で１Mbps 程度）ではあるが、これらの数字は、理論的に最も強い攻撃者を想定したものであり、実際には、攻撃者にも技術的制約が存在することを考えると、より高い性能と安定性を以って安全な鍵配布を達成していることが期待できる。
このような背景のもと、実際に実現可能な物理パラメータにより実装されたＢＢ８４システムを用いて鍵配送センター網を構築し、既存の情報通信システムへの鍵供給センターとして組み込むことにより、全体として広域情報セキュリティ基盤を構築していこうとするアイディアが、既にいくつかの視点から提案されている。このアイディアの実用的利点は、暫定的には無条件安全性を達成しないまでも、現在調達可能な量子暗号技術を有効に活かすことにより高度な安全性を提供しつつ、今後達成されるであろう技術革新に応じてシステム全体のアップグレードを行うことにより、無条件安全性を満たす情報セキュリティ基盤への段階的な移行を穏やかに促進することができる点にある。一方、このようなアイディア、特に暫定的に達成された状況について、暗号学的位置付けを行うことは、きちんとした安全性の根拠を与えるために必要不可欠な課題である。

２．研究の目的
上記の背景のもと、現在国内外で開発が進められているＢＢ８４プロトコルや類似のプロトコルを調査し、攻撃者の現実的な攻撃能力に依存した「条件付」安全性について量子情報理論的な立場から定義を与える。さらにその安全性を保証する物理パラメータの最適化を行う。以上のタスクにより、量子暗号技術の発展的組込みによる情報セキュリティ基盤の設計という大きなゴールに向け、暫定的で実用的な状況について、理論的な裏打ちのある安全性規準を与えることが本研究の目的とする。本研究の最大の革新性は、それが「持続的に安全性の向上が可能な情報インフラシステムの設計」という、より普遍的で大きなプログラムの中に位置づけられることにあると考えている。これまで、量子暗号技術の研究は、無条件安全性を満たす究極の暗号としての一面が強調され、実際の情報インフラへの組み込みについての方法論や、その実用的な利点などが系統的に研究されることがなかった。その結果、要素技術各論における知見は十分に発展してきたが、それらの技術の社会的貢献の可能性が過小評価され、実際には現在において有用な技術が蓄積されつつあるにもかかわらず、その運用が促進されてこなかった。このような状況に対し、本研究は、現在の技術に基づいた量子暗号をどのように組み込めば、（暫定的であるが当面は十分な）「条件付」安全性を確保することができるかという短期的視点と量子暗号技術周辺の将来的な技術発展を組み込むことにより、段階的に無条件安全性を達成することが可能な情報インフラシステムをどのように設計すべきか，という将来的展望の二つを与えることを目的とし，運用・設計・評価技術を具体的かつ系統的に開発しようとするものである。これらの問題意識に基づいた議論は、従来情緒的に行われるのがせいぜいであり、実際の科学技術やその発展が具体的に検討されることは皆無であった。本研究では、研究開発課題自体が既に科学的に十分なレベルで記述されており、具体的な成果が期待できる点も際立った特徴である。
本研究のこのような革新性は、本研究開発の成果が、量子暗号技術そのものの発展に寄与することだけでなく、今後量子暗号技術について想定される国際標準化や運用規定の決定の際に、具体的基準として参照されるにふさわしいだけの内容を持っている点にも現れているだろう。安全性解析技術の開発としてだけでなく、量子暗号技術を使って安全な情報社会を構築する具体的な方法論を提供するものとして、新規性・独創性・革新性のいずれも備えた優れた研究開発課題であると自負している。本研究からの成果は、国内における暗号実装関連技術等の調査・検討を行う暗号モジュール委員会/CRYPTREC への貢献や、今後急激に進むことが想定される量子暗号技術に関する国際的な標準化活動にも非常に大きな影響を及ぼすことが期待できる。

３．研究の方法
量子暗号プロトコル（BB84 など）に対し、攻撃者の現実的な攻撃能力に依存した「条件付」安全性を議論するために必要なモデル化を実際のシステムを特徴づける物理パラメータを考慮して行う。ここで考察されるべき物理パラメータは、大別して次のような二つに分類することができる。
(A) プロトコル、および正規ユーザ（アリスとボブ）の技術的制約を特徴づける物理パラメータ
　具体例としては、光子状態（例えば弱コヒーレント状態の平均光子数），光ファイバ

の透過パラメータ，受信部の量子効率，量子通信路の距離、ビットフリップ確率、具体的なプロトコルで決定される誤り訂正および秘匿性増強の効率等々を挙げることができる。（これらで決定されるパラメータ空間を形式的に P と書く）。

(B)攻撃者（イブ）の攻撃手法、および技術的制約を特徴づける物理パラメータ
イブが用いる受信部の量子効率実際に行うことができるデコヒーレンス制御（あるいは、これら等で決定される実行可能な量子操作および測定行為）イブがバイパスとして用意することができる光ファイバの透過パラメータイブの計算機の能力等々を挙げることができる。（これらで決定されるパラメータ空間を形式的に Q と書く。）
このとき、本研究課題の「攻撃者の現実的な能力に依存した「条件付」安全性を保証する量子鍵配送プロトコルの物理パラメータの最適化」とは、「与えられたパラメータ空間 P と Q に対し、秘密鍵生成レート R を最大にするようなパラメータ（∈P）を見つける」こととして、整理することができる。
より具体的には、
１．要素技術に対する技術的到達点、および、それらの組み合わせにより評価される正規ユーザと攻撃者の技術的制約を検討し、上記パラメータ空間 P、および Q の具体的な選定
２．上記で決定される物理パラメータを具体的に導入した CP マップ、および量子状態を用いた量子暗号プロトコルの書き下し
などが、一つのアプローチとして考えられる。

４．研究成果
(1)量子暗号（量子鍵配送）技術の実用化に向けた課題の抽出。
　量子暗号技術の実用化に向けた技術的仕様策定について、他の現代暗号技術との比較により仕様策定に必要な技術課題の抽出を行った。図１．は、現代暗号が実用化される場合のフローを技術的視点から整理したものである。このフローの分析を行い、物理装置としての安全性についてコンセンサスを得るために必要な仕様として、３つの異なる

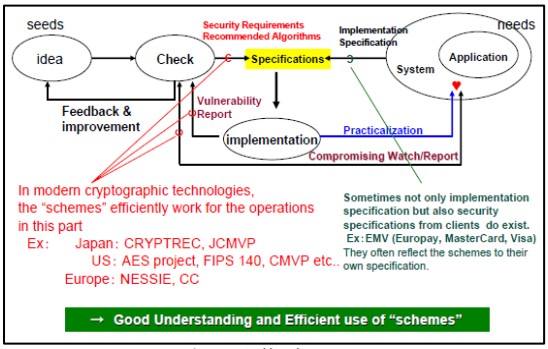

図１．暗号技術実用化フロー

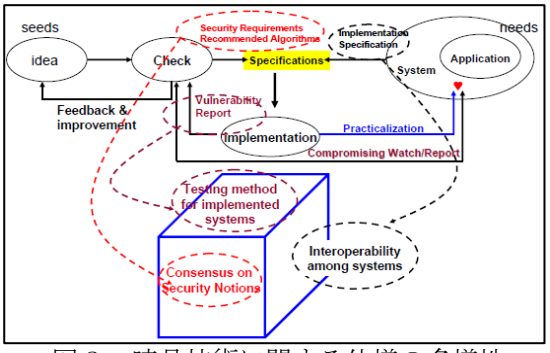

図２．暗号技術に関する仕様の多様性

仕様（安全性の概念（Security Notion）に関する仕様，実機の実装の検証技術に関する仕様、相互接続性に関する仕様）に分解し、特に安全性概念の仕様を整理することを行った。

(2)量子状態を用いた一方向秘匿暗号通信に関する整理。
　量子鍵配送以外の量子論のセキュリティへの応用として、量子状態に直接メッセージをエンコードし情報を秘匿する方式が議論されていることを受け、これらの安全性解析を行うとともに、このような暗号方式が、暗号学的にどのような安全性を持つかについて、利用している物理状態の特性を用いてチェックを行うことができるチャート図の作成を行った。

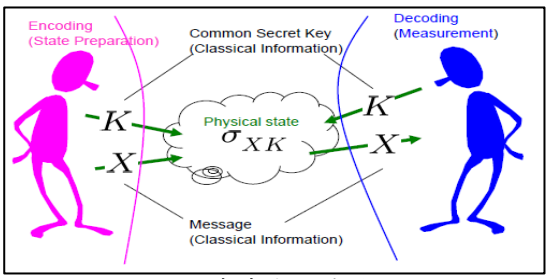

図３．考察する暗号系

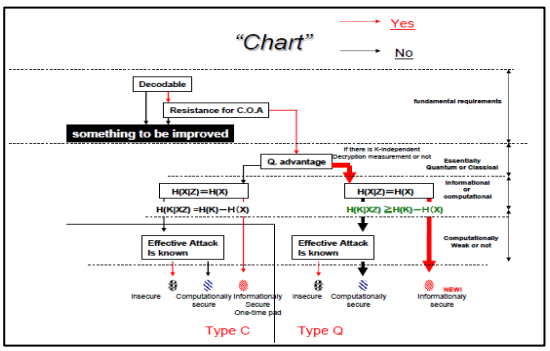

図４．チャート図

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔学会発表〕（計６件）

① 今福健太郎、今井秀樹、古典系としては正しく機能するように見えるが実は脆弱性を持つワンタイムパッドの実装、暗号と情報セキュリティシンポジウム（ＳＣＩＳ２００９）、2009.01.20、大津
② Kentaro Imafuku 、A Complex Approach to "Updated" Quantum Cryptography、量子暗号国際会議（ＵＱＣ２００８）、2008.12.02、東京
③ Kentaro Imafuku 、Benefits and Requirements (and Challenge!) on Quantum Data Encryption in Optical System、量子暗号国際会議（ＵＱＣ２００８）、2008.12.01、東京
④ 伊藤由季子、今福健太郎、今井秀樹、国際量子暗号会議 UQC2007 の開催報告と今後の展開、暗号と情報セキュリティシンポジウム（ＳＣＩＳ２００８）2008.01.24、宮崎
⑤ Kentaro Imafuku 、UQC approach toward Approved QKD function – Framework、量子暗号国際会議（ＵＱＣ２００7）、2007.10.01、東京
⑥ Kentaro Imafuku 、UQC approach toward Approved QKD function – Building Block、量子暗号国際会議（ＵＱＣ２００7）、2007.10.02、東京

６．研究組織
(1)研究代表者
今福　健太郎（IMAFUKU KENTARO）
独立行政法人産業技術総合研究所・情報セキュリティ研究センター・物理解析研究チーム・チーム長
研究者番号：10298169