量子鍵配送技術の利用・運用のための技術を概観できる！

量子鍵配送

ー基礎と活用法ー

監修：佐々木 雅英
編者：一般社団法人 量子 ICT フォーラム 量子鍵配送技術推進委員会
仕様：A5 判・並製・印刷版モノクロ / 電子版一部カラー・本文 144 頁
印刷版・電子版価格：2,700 円（税抜）
ISBN（カバー付単行本）：978-4-7649-0669-3 C3042
ISBN（POD）：978-4-7649-6070-1 C3042
発行：近代科学社 Digital
発売：近代科学社

内容紹介

本書は、量子鍵配送技術の概要とその利用および運用に必要な内容をまとめたものです。

第 1 章では、量子鍵配送 (Quantum Key Distribution：QKD) の基礎と技術開発動向を概観します。第 2 章では暗号技術を取り巻く現状について整理し、その上で QKD の活用法について述べます。第 3 章では、QKD の原理と仕組み、およびネットワークの構成法について説明し、QKD プラットフォームというサービス基盤の概念を導入します。第 4 章ではすでに試験運用の段階まで来ている QKD プラットフォームを活用したセキュリティアプリケーションの事例を紹介します。最後に、第 5 章では、将来の応用に向けた展望と課題、特に分野連携で長期的に取り組むべき課題をまとめています。

全国の書店・ネット書店にてお求めいただけます。お取り扱い店は以下のウェブページをご覧ください。

https://www.kindaikagaku.co.jp/book_list/detail/9784764960701/

著者紹介

●監修者
佐々木 雅英（ささきまさひで）
国立研究開発法人情報通信研究機構オープンイノベーション推進本部

●編者
一般社団法人量子 ICT フォーラム量子鍵配送技術推進委員会
量子情報通信技術（ICT）の健全な発展を支援することを目的として、最新の研究開発成果や技術動向に関する情報交換、産学官連携と人材交流の促進、研究開発推進戦略の討議と提言を目指す団体。

お問い合わせ先
株式会社近代科学社
〒101-0051 東京都千代田区神田神保町 1-105
神保町三井ビルディング
電子メール：contact@kindaikagaku.co.jp

近代科学社Digital
https://www.kindaikagaku.co.jp/kdd/

近代科学社Digitalは、株式会社近代科学社が推進する21世紀型の理工系出版レーベルです。デジタルパワーを積極活用することで、オンデマンド型のスピーディで持続可能な出版モデルを提案します。

目　次

第 1 章　QKD の基礎

1.1 量子鍵配送 (QKD) の技術開発動向
1.2 QKD とは
1.3 QKD ネットワークとは
1.4 QKD の標準化

第 2 章　暗号技術を取り巻く現状と QKD の活用法

2.1 情報通信インフラに対するセキュリティ脅威
2.2 耐量子安全性暗号
2.3 QKD の想定用途とメリット

第 3 章　QKD の技術的概要

3.1 暗号技術の安全性
3.2 QKD の原理と仕組み
3.3 QKD プラットフォーム

第 4 章　QKD を活用したセキュリティ強化の具体例

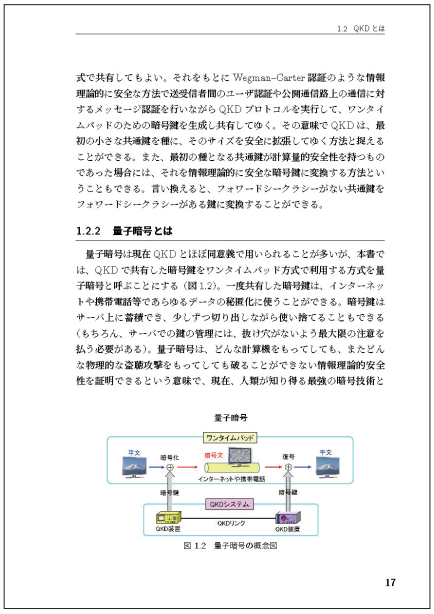
4.1 ネットワーク階層モデル
4.2 レイヤ 1 のセキュリティ強化
4.3 レイヤ 2 のセキュリティ強化
4.4 レイヤ 3 のセキュリティ強化
4.5 移動通信システムのセキュリティ強化

第 5 章　QKD の情報通信インフラへの応用

5.1 情報通信インフラのセキュリティについて
5.2 フォトニックネットワークとセキュリティ脅威
5.3 セキュアフォトニックネットワーク
5.4 ストレージネットワークへの展開
5.5 次世代多層防御セキュリティ技術に向けた今後の検討課題

付　録

A.1 暗号技術の概要
A.2 BB84 プロトコルで使われる 4 つの量子信号の状態表現
A.3 多層防御セキュリティ
A.4 次世代ネットワーク (NGN)



1.2　QKD とは

式で共有してもよい。それをもとに Wegman–Carter 認証のような情報理論的に安全な方法で送受信者間のユーザ認証や公開通信路上の通信に対するメッセージ認証を行いながら QKD プロトコルを実行して、ワンタイムパッドのための暗号鍵を生成し共有してゆく。その意味で QKD は、最初の小さな共通鍵を種に、そのサイズを安全に拡張してゆく方法と捉えることができる。また、最初の種となる共通鍵が計算量的安全性を持つものであった場合には、それを情報理論的に安全な暗号鍵に変換する方法ということもできる。言い換えると、フォワードシークラシーがない共通鍵をフォワードシークラシーがある鍵に変換することができる。

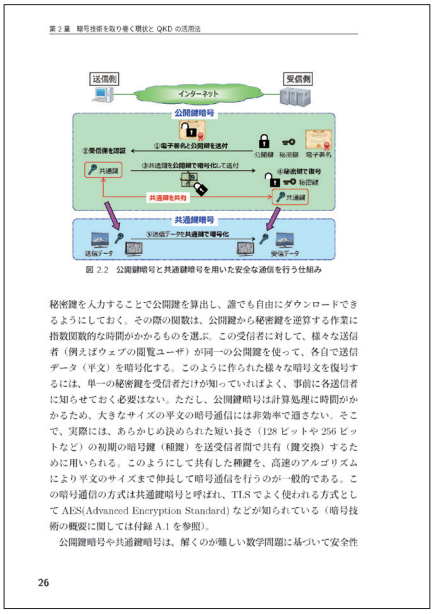
1.2.2　量子暗号とは

量子暗号は現在 QKD とほぼ同意義で用いられることが多いが、本書では、QKD で共有した暗号鍵をワンタイムパッド方式で利用する方式を量子暗号と呼ぶことにする（図 1.2）。一度共有した暗号鍵は、インターネットや携帯電話等であらゆるデータの秘匿化に使うことができる。暗号鍵はサーバ上に蓄積でき、少しずつ切り出しながら使い捨てることもできる（もちろん、サーバでの鍵の管理には、抜け穴がないよう最大限の注意を払う必要がある）。量子暗号は、どんな計算機をもってしても、またどんな物理的な盗聴攻撃をもってしても破ることができない情報理論的安全性を証明できるという意味で、現在、人類が知り得る最強の暗号技術と

図 1.2　量子暗号の概念図

17

量子鍵配送の基礎と最近の開発動向を概観



第 2 章　暗号技術を取り巻く現状と QKD の活用法

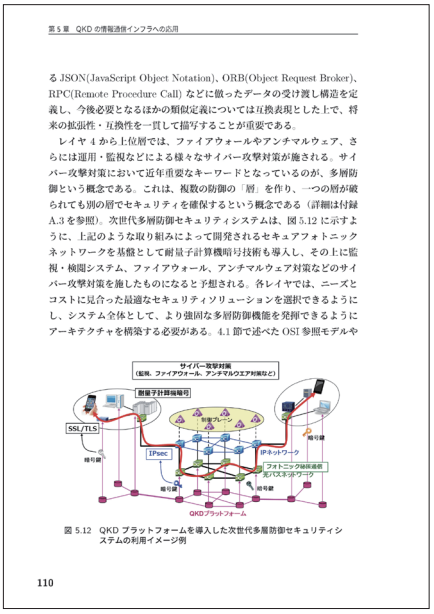
図 2.2　公開鍵暗号と共通鍵暗号を用いた安全な通信を行う仕組み

秘密鍵を入力することで公開鍵を算出し、誰でも自由にダウンロードできるようにしておく。その際の関数は、公開鍵から秘密鍵を逆算する作業に指数関数的な時間がかかるものを選ぶ。この受信者に対して、様々な送信者（例えばウェブの閲覧ユーザ）が同一の公開鍵を使って、各自で送信データ（平文）を暗号化する。このように作られた様々な暗号文を復号するには、単一の秘密鍵を受信者だけが知っていればよく、事前に各送信者に知らせておく必要はない。ただし、公開鍵暗号は計算処理に時間がかかるため、大きなサイズの平文の暗号通信には非効率で適さない。そこで、実際には、あらかじめ決められた短い長さ（128 ビットや 256 ビットなど）の初期の暗号鍵（種鍵）を送受信者間で共有（鍵交換）するために用いられる。このようにして共有した種鍵を、高速のアルゴリズムにより平文のサイズまで伸長して暗号通信を行うのが一般的である。この暗号通信の方式は共通鍵暗号と呼ばれ、TLS でよく使われる方式として AES(Advanced Encryption Standard) などが知られている（暗号技術の概要に関しては付録 A.1 を参照）。

公開鍵暗号や共通鍵暗号は、解くのが難しい数学問題に基づいて安全性

26

暗号技術によるセキュリティ強化の具体例を収録



第 5 章　QKD の情報通信インフラへの応用

る JSON(JavaScript Object Notation)、ORB(Object Request Broker)、RPC(Remote Procedure Call) などに散ったデータの受け渡し構造を定義し、今後必要となるほかの類似定義については互換表現とした上で、将来の拡張性・互換性を一貫して描写することが重要である。

レイヤ 4 から上位層では、ファイアウォールやアンチマルウェア、さらには運用・監視などによる様々なサイバー攻撃対策が施される。サイバー攻撃対策において近年重要なキーワードとなっているのが、多層防御という概念である。これは、複数の防御の「層」を作り、一つの層が破られても別の層でセキュリティを確保するという概念である（詳細は付録 A.3 を参照）。次世代多層防御セキュリティシステムは、図 5.12 に示すように、上記のような取り組みによって開発されるセキュアフォトニックネットワークを基盤として耐量子計算機暗号技術も導入し、その上に監視・検閲システム、ファイアウォール、アンチマルウェア対策などのサイバー攻撃対策を施したものになると予想される。各レイヤでは、ニーズとコストに見合った最適なセキュリティソリューションを選択できるようにし、システム全体として、より強固な多層防御機能を発揮できるようにアーキテクチャを構築する必要がある。4.1 節で述べた OSI 参照モデルや

図 5.12　QKD プラットフォームを導入した次世代多層防御セキュリティシステムの利用イメージ例

110

量子鍵配送の長期的に取り組むべき今後の課題も解説