TTC標準
Standard

JT-Y3802

量子鍵配送ネットワーク – 機能アーキテクチャ

Quantum key distribution networks - Functional architecture

第 1.1 版

2021 年 6 月 11 日制定

一般社団法人
情報通信技術委員会

THE TELECOMMUNICATION TECHNOLOGY COMMITTEE

目　次

＜参考＞

1. 国際勧告などとの関連

本標準は量子鍵配送ネットワークの機能アーキテクチャについて規定しており、2020 年 12 月に ITU-T SG13 において発行された ITU-T 勧告 Y.3802 に準拠している。

2. 上記勧告などに対する追加項目など

2.1 オプション選択項目

なし

2.2 ナショナルマター決定項目

なし

2.3 その他

なし

2.4 原勧告との章立て構成比較表

章立てに変更なし

3. 改版の履歴

版数	発行日	改版内容
第 1 版	2021 年 5 月 20 日	制定
第 1.1 版	2021 年 6 年 11 日	図中表記の和訳化、誤記訂正

4. 工業所有権

本標準に関わる「工業所有権の実施の権利に係る確認書」の提出状況は、TTC ホームページでご覧になれます。

5. その他

(1) 参照している勧告、標準など

TTC 標準　　JT-Y3800, JT-Y3801

6. 標準作成部門

Network Vision 専門委員会

1. 規定範囲

本標準では、量子鍵配送ネットワーク(QKDN)の機能アーキテクチャを規定する。

特に、本標準の規定範囲は以下を含む：

- 機能アーキテクチャモデル
- 機能要素と参照点
- アーキテクチャ構成
- 基本動作手順

注 - 本標準では、[ITU-T Y.3800]に示されている概念構造と[ITU-T Y.3801]の機能要求条件に基づいて、QKDN の機能アーキテクチャを扱う。

2. 参考文献

以下に列挙する ITU-T 勧告およびその他の参考文献は、この本文中の参照を通して、本標準を構成する規定を含む。発行時点では、示された版は有効であった。すべての勧告及び他の参考文献は改訂の対象である。したがって、本標準の利用者は、以下に列挙する勧告及び他の参考文献の最新版を適用する可能性を調査することが推奨される。現在有効な ITU-T 勧告のリストは定期的に発行されている。本標準が文献を参照することは、その文献がそれ単体で勧告となる地位をその文献に与えるものではない。

[ITU-T Y.3800]　　ITU-T Y.3800(2019)、量子鍵配送ネットワークの概要

[ITU-T Y.3801]　　ITU-T Y.3801(2020)、量子鍵配送ネットワークの機能要求条件

3. 用語定義

3.1. 本標準以外で定義された用語

本標準では、本標準以外で定義された次の用語を使用する。

3.1.1. 鍵マネージャ (KM) [ITU-T Y.3800]：鍵管理レイヤ内で鍵管理を実行する機能モジュールで、QKDノード内に配置される。

3.1.2. 鍵マネージャリンク[ITU-T Y.3800]：鍵マネージャ(KM) を接続し、鍵管理を行う通信リンク。

3.1.3. 量子鍵配送(QKD)[b-ETSI GR QKD007]：量子情報理論に基づく情報理論的セキュリティを用いて対称暗号鍵を生成および配送する手順または方法。

3.1.4. QKD リンク[ITU-T Y.3800]：QKD を動作させるための 2 つの QKD モジュール間の通信リンク。

注：QKD リンクは、量子信号を送受信する量子チャネルと、同期と鍵蒸留のために情報を交換する古典チャネルから構成される。

3.1.5. QKD モジュール[ITU-T Y.3800]：暗号機能と、QKDプロトコル、同期、鍵生成のための蒸留などの量子光プロセスを実装するハードウェアおよびソフトウェアコンポーネントのセット。定められた暗号境界内に含まれる。

注： QKD モジュールは、QKD リンクに接続され、鍵を生成するエンドポイントモジュールとして動作する。QKD モジュールには 2 つのタイプ、すなわち送信器 (QKD-Tx) および受信器 (QKD- Rx) がある。

3.1.6. QKD ネットワーク (QKDN) [ITU-T Y.3800]： QKD リンクを介して接続された 2 以上の QKD ノードとから構成するネットワーク。

注： QKD ネットワーク (QKDN) では、QKD リンクで直接接続されていない QKD ノード間でも、鍵リレーによって鍵を共有できる。

3.1.7. QKDN コントローラ[ITU-T Y.3800]：QKDN を制御するために QKDN制御レイヤに位置する機能モジュール。

3.1.8. QKDN マネージャ[ITU-T Y.3800]：QKDN を監視および管理するために QKDN管理レイヤに位置する機能モジュール。

3.1.9. QKD ノード[ITU-T Y.3800]：許可されていない当事者による侵入および攻撃から保護されている1つ以上のQKDモジュールを含むノード。

注：QKD ノードは、鍵マネージャ(KM)を含むことができる。

3.1.10. ユーザネットワーク[ITU-T Y.3800]： QKDN によって供給される鍵を暗号アプリケーションが利用するネットワーク。

3.2. 本標準で定義された用語定義

本標準では、次の用語を定義する。

3.2.1. 鍵管理エージェント(KMA)：QKDノード（トラステッドノード）内の１つまたは複数のQKDモジュールによって生成された鍵を管理するための機能要素。

注 - KMA は、1 つまたは複数の QKD モジュールから鍵を取得し、同期、サイズ変更、フォーマット、および格納を行う。また、鍵管理エージェント(KMA)リンクを介して鍵のリレーを行う。

3.2.2. 鍵管理エージェント(KMA)リンク：鍵管理エージェント(KMA)を接続して鍵リレーと鍵管理のための通信の実行する通信リンク。

3.2.3. 鍵供給エージェント(KSA)：鍵管理エージェント(KMA)と暗号アプリケーションの中間に位置し、暗号アプリケーションに鍵を供給する機能要素。

注 - 暗号アプリケーション用のアプリケーションインタフェースは、KSA に実装される。KSA は鍵を同期し、暗号アプリケーションに鍵を供給する前に KSA リンクを介してその完全性を検証する。

3.2.4. 鍵供給エージェント(KSA)リンク：鍵供給エージェント(KSA)を接続して鍵同期と完全性検証を実行する通信リンク。

3.2.5. QKD-鍵：1対のQKDモジュールによって生成される一対の対称ランダムビット列。特に、鍵マネージャでサイズ変更およびフォーマットされる前のランダムビット列を指す。

4. 略語

本標準は、以下の略語を使用する。

AES	高度暗号化標準（Advanced Encryption Standard）
API	アプリケーションプログラミングインタフェース（Application Programming Interface）
FCAPS	障害、構成、課金、パフォーマンス、およびセキュリティ(Fault, Configuration, Accounting, Performance and Security)

HMAC	ハッシュベースメッセージ認証コード（Hash based message authentication code）
ID	識別子（Identifier）
IPsec	インターネットプロトコルセキュリティ(Internet Protocol Security)
IT-secure	IT セキュア（Information-theoretically secure）
KM	鍵マネージャ（Key Manager）
KMA	鍵管理エージェント(Key Management Agent)
KSA	鍵供給エージェント(Key Supply Agent)
NTP	ネットワークタイムプロトコル (Network Time Protocol)
OTP	ワンタイムパッド（One-Time Pad）
PTP	高精度タイムプロトコル(Precision Time Protocol)
QBER	量子ビットエラー率（Quantum Bit Error Rate）
QBN	量子鍵配送バックボーンネットワーク(QKD Backbone Network)
QKD	量子鍵配送（Quantum Key Distribution）
QKDN	量子鍵配送ネットワーク（QKD Network）
QKD-Rx	量子鍵配送-受信機(QKD Receiver)
QKD-Tx	量子鍵配送-送信機(QKD Transmitter)
QoS	クオリティオブサービス（Quality of Service）
QRNG	量子乱数生成器(Quantum Random Number Generator)
RNG	乱数生成器(Random Number Generator)
SPD	光子検出器(Single Photon Detector)
TLS	トランスポートレイヤセキュリティ(Transport Layer Security)

5. 表記法

無し。

6. 機能アーキテクチャモデル

QKDN の設計上の考慮事項、ネットワーク能力、概念的構造、および基本機能は[ITU-T Y.3800]で規定されている。QKDN の機能要求条件は[ITU-T Y.3801]で規定されている。

[ITU-T Y.3800]の図 3 に示された QKDN の概念的構造および[ITU-T Y.3801]で明らかにされた QKDN の機能要求条件に基づいて、QKDN の機能アーキテクチャモデルを図 1 に示す。図 1 には、以下に示すアーキテクチャの核心をなす要素が含まれている。

- [ITU-T Y.3800]で定義されたレイヤ構造：量子レイヤ、鍵管理レイヤ、QKDN 制御レイヤ、QKDN 管理レイヤ、サービスレイヤ、ユーザネットワーク管理レイヤ。
- [ITU-T Y.3800]で定義された基本機能とリンク：QKDN 内の QKD モジュール、鍵マネージャ(KM)、QKDN コントローラ、QKDN マネージャ、QKD リンク、KM リンク、およびユーザネットワーク内の暗号アプリケーション、ユーザネットワークマネージャ、アプリケーションリンク。
- 本標準が定義する機能要素：各基本機能に含まれるサブ機能(例えば、 QKDN コントローラのルーティング制御機能)
- 本標準が定義する詳細な参照点

これらの機能要素および参照点の詳細な説明は、それぞれ 7 章および 8 章に記載されている。

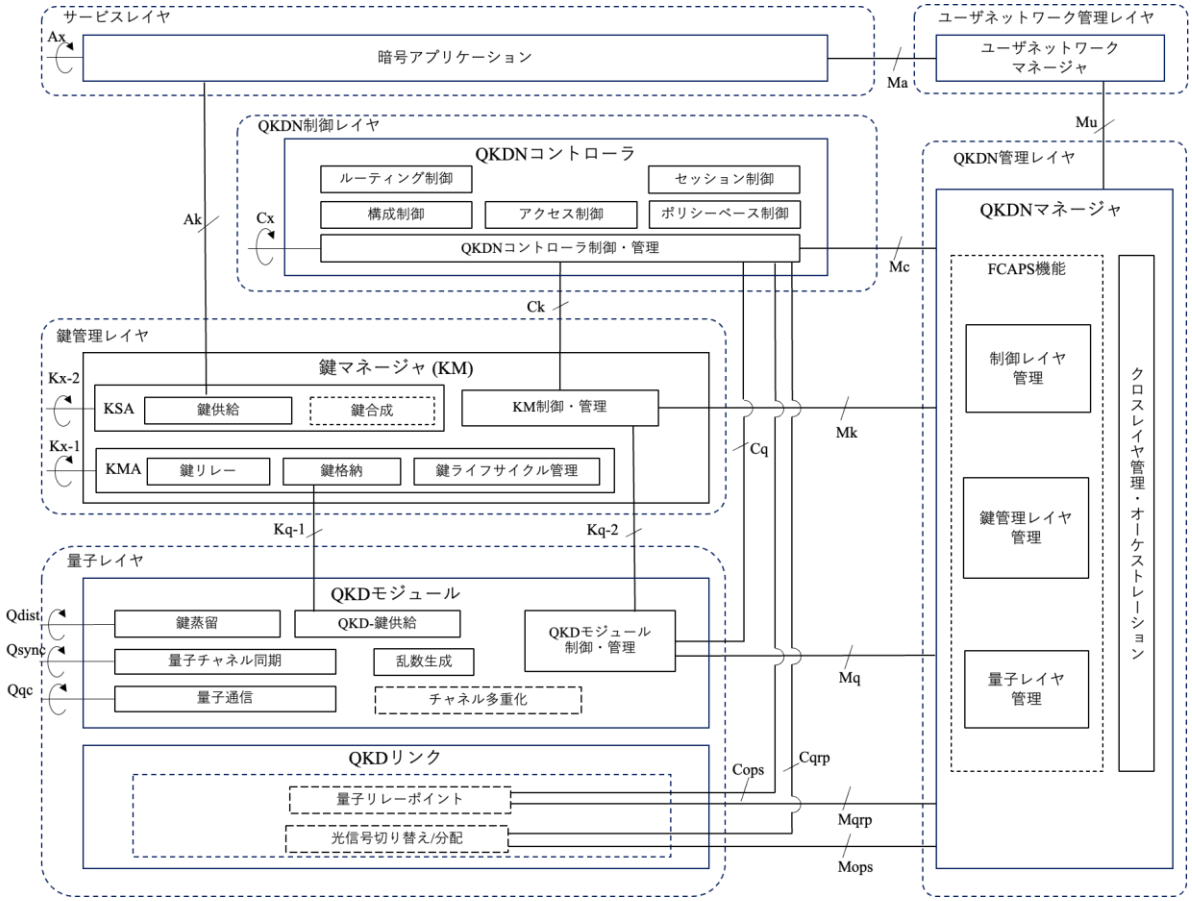

図１　QKDN の機能アーキテクチャモデル

7.　機能要素

7.1.　量子レイヤの機能要素

量子レイヤでは、QKD リンクによって接続された一対の QKD モジュールが、QKD プロトコルを使用して QKD-鍵を生成する。

QKD モジュールは、以下の機能要素で構成される。

- 量子通信機能：量子信号を用意し、伝送、測定を行う。

注１ - “prepare-and-measure”方式と呼ばれる QKD プロトコルの場合、QKD モジュールは送信機か受信機のいずれかである。[ITU-T Y.3800]で言及されている MDI-QKD や TF-QKD のような測定支援方式に基づく QKD プロトコルの場合、QKD モジュールは送信器であり、受信器は量子チャネル上の中間点に位置する。量子もつれベースの QKD プロトコルの場合、QKD モジュールは受信器であり、量子もつれ状態の量子信号の送信器は量子チャネル上の中間点に位置する。

- 量子チャネル同期機能：量子チャネルのクロックとタイミングの同期を、量子信号の伝送と測定をサポートするのに十分な精度で提供する。この機能は、クロックおよびタイミングの同期を提供するために、後述する量子通信機能および/または鍵蒸留機能と連携することがある。

- 鍵蒸留機能：一般的には以下の古典データ処理を行う。

a)　QKD モジュール間の変調及び/又は測定の基底情報を一致させるための鍵シフティング。

b) セキュリティを確保し、以下に記述する誤り訂正及び秘匿性増強を行うパラメータ設定を可能とするための量子チャネルのパラメータ推定。

c) QKD モジュール間で同一かつ安全な鍵を確立するための誤り訂正及び秘匿性増強。

注２ - 上述の古典データ処理は併用しても良い。

- QKD-鍵供給機能：鍵管理エージェント(KMA)から QKD-鍵要求を受け取り、QKD-鍵を KMA に安全に供給する。
- 乱数生成器(RNG)機能：乱数を生成し、量子通信機能と鍵蒸留機能に提供する。

注 3 - RNG は、非決定論的であるべきである。これは、[b-ISO/IEC18031]に規定されているような従来の物理的雑音に基づく方式、又は量子原理に基づく方式(QRNG)で実現することができる。

- QKD モジュール制御・管理機能：QKD モジュール内の機能要素を全体的に制御、管理し、KM、QKDN コントローラ、QKDN マネージャなど他のレイヤの機能と通信する。
- 光チャネル多重化機能：QKD モジュール間で量子及び古典チャネルの波長分割多重を可能とする。

QKD リンクは、鍵蒸留および同期のための量子信号伝送および古典通信に加えて、オプションで以下の機能要素を含む。

- 光信号切り替え/分配機能：マルチポイントネットワーク内の一対の QKD モジュール間で量子チャネルトラフィックおよび／または量子チャネル同期信号と蒸留チャネルトラフィックを切り替えまたは分配して、同一の鍵を異なるユーザ間にオンデマンドで形成することを可能とする。
- 量子リレーポイント機能：QKD リンクの中間点としてふるまい、量子信号と古典信号をリレーして QKD の距離を伸ばすことを支援する。

注 4 - 光信号切り替え/分配機能および量子リレーポイント機能は、QKD モジュールに含まれていてもよく、QKDN コントローラおよび QKDN マネージャとのインタフェースを有していなくてもよい。それは実装に依存する。

7.2. 鍵管理レイヤの機能要素

鍵管理レイヤの KM 機能は、QKD モジュールと QKD リンクで生成された鍵を受信して管理し、鍵をリレーして暗号アプリケーションに提供する。KM は鍵管理エージェント(KMA)、鍵供給エージェント(KSA)、KM 制御・管理機能からなる。また [ITU-T Y.3800]で定義された KM リンクは、各々独立した役割を持つ KMA リンク(Kx-1)と KSA リンク(Kx-2)に分割される。これらはさらに以下の機能要素から構成される。

1) KMA

- 鍵格納機能：QKD モジュールから鍵を受信し、同期および認証し、サイズ変更(結合または分割)し、鍵 ID、鍵サイズ、鍵種別、世代タイムスタンプ等のメタデータを用いて再フォーマットし、処理された鍵とメタデータを格納する。
- 鍵リレー機能：ワンタイムパッド（OTP）[b-Shannon 1949]が推奨される IT セキュア暗号を用いた高度に安全な方法で、KMA リンクを介して QKDN 内をエンドツーエンドに鍵をリレーする。
- 鍵ライフサイクル管理機能：KM による鍵の受信から暗号アプリケーションによる鍵の利用までの鍵ライフサイクルを管理する。また、鍵管理ポリシーに応じて、鍵格納機能における鍵の削除や保存を管理する。

2) KSA

- 鍵供給機能：KSA リンクを介してエンドツーエンドの KSA 間で共有される鍵を同期および認証し、オンデマンドで暗号アプリケーションに鍵を供給する。
- 鍵合成機能：オプションの機能要素。QKD で生成された鍵と他の鍵交換法(例えば、ポスト量子暗号)によって生成された鍵を合成する。

3) KM 制御・管理機能

- KM 制御・管理機能：KM 内の機能要素の全体的な制御と管理を担当し、QKD モジュール、QKDN コントローラ、QKDN マネージャなどの他のレイヤの機能と通信する。

7.3. QKDN制御レイヤの機能要素

QKDN 制御レイヤの QKDN 制御機能は、QKDN のリソースを制御し、QKDN の安全で、安定し、効率的で、堅固なオペレーションを保証する。QKDN 制御機能はさらに以下の機能要素から構成される。

- セッション制御機能：KMA をサポートし、鍵リレーのセッション手順を制御する。
  また、KSA が複数の暗号アプリケーションに鍵を提供することをサポートする。
- ルーティング制御機能：KM の 2 つのエンドポイント間の適切な鍵リレールートを提供し、また、鍵リレーおよび鍵供給の継続を保証するために、量子レイヤおよび/または鍵管理レイヤの障害、性能、および/または可用性の状態に応じて、鍵リレーの再ルーティングを実行する。
- 構成制御機能：QKD モジュール、QKD リンク、KM、および KM リンクの構成情報と、これらのコンポーネントの状態(例えば、稼働中、停止中、待機中、予約済み)の取得を実行する。故障診断結果を含むアラームが通知されると、QKD リンクおよび KM リンクの再構成を行う。
- ポリシーベース制御機能：QoS および暗号アプリケーションへの課金ポリシーに基づいて QKDN リソースを制御する。
- アクセス制御機能：QKDN コントローラによる制御およびサポートの下で、機能および機能要素が主張する識別情報を検証し(認証)、許可前の機能および機能要素の活動または役割を、適用されるポリシーに基づくアクセス権に従って制限する(許可)能力を提供する。
- QKDN コントローラ制御・管理機能：QKDN コントローラ内の機能要素の全体的な制御と管理を担当し、QKD モジュール、KM、QKDN マネージャなどの他のレイヤの機能と通信する。

7.4. QKDN管理レイヤの機能要素

QKDN 管理レイヤの QKDN マネージャ機能は、QKDN 全体の障害、構成、課金、パフォーマンス、およびセキュリティ（FCAPS）を管理し、ユーザネットワーク管理をサポートする。次の機能要素を含む。

- 障害管理機能：QKDN が管理するリソースの障害の監視、検出、根本原因分析を含む診断、および修復を実行する。また、障害時に必要となる、鍵リレーのルーティングと再ルーティング制御のために QKDN コントローラをサポートする。
- 構成管理機能：QKDN リソースのプロビジョニングを管理し、QKDN トポロジを収集および管理する。その管理役割には、QKDN リソースのプロビジョニング、構成、およびディスカバリーが含まれる。また、QKDN が鍵リレーをサポートする場合は、鍵リレールートのプロビジョニングのために QKDN コントローラをサポートする。

- 課金管理機能：暗号アプリケーションによる鍵利用の費用を決定するために、鍵供給サービスの利用を計測し、課金/請求システムをサポートする。
- パフォーマンス管理機能：QKDN が管理するリソースのパフォーマンスステータスを監視および分析する。また、QoS 保証、QoS ポリシー管理、および QKDN パフォーマンス情報の視覚化もサポートする。
- セキュリティ管理機能：QKDN からセキュリティ関連の管理情報を収集/受信し、鍵ライフサイクル管理をサポートし、QKDN 内の認証および許可全体を管理する。

QKDN 制御、鍵管理、および量子レイヤにおける FCAPS 管理には、以下の管理機能要素が存在する。

- QKDN 制御レイヤ管理機能：QKDN 制御レイヤの機能要素に FCAPS 管理機能を提供する。特に、この機能要素は、障害および/またはパフォーマンスの問題が発生した場合に、QKDN コントローラが鍵リレーパスのルーティングおよび再ルーティングおよびプロビジョニングを制御することをサポートする。
- 鍵管理レイヤ管理機能：鍵管理レイヤの機能要素に FCAPS 管理機能を提供する。さらに、この機能要素は、鍵ライフサイクル管理もサポートする。
- 量子レイヤ管理機能：量子レイヤの機能要素に FCAPS 管理機能を提供する。
- クロスレイヤ管理機能：QKDN 制御レイヤ、鍵管理レイヤ、量子レイヤの管理機能と機能要素の間で、管理上の判断と処理行動を調整する。また、外部の管理要素、特に QKDN ユーザを間接的にサポートするユーザネットワーク管理要素と管理情報を交換する。

7.5. サービスレイヤの機能要素

サービスレイヤには、次の機能要素がある。

- 暗号アプリケーション機能：QKDN によって提供された対となる共有鍵を利用し、遠隔当事者間の安全な通信を実行する。

7.6. ユーザネットワーク管理レイヤの機能要素

ユーザネットワーク管理レイヤには、次の機能要素がある。

- ユーザネットワークマネージャ機能：ユーザネットワークの FCAPS 管理機能を実行する。

8. 参照点

本章は、図 1 に示す各参照点の詳細を扱う。

セッション処理および情報交換を含む QKDN 参照点の共通機能は付録 I に示す。

8.1. QKDモジュールの参照点

次の参照点は、QKD リンク内の QKD モジュール間の接続に関連する。

- -Qqc：QKD リンク内の量子チャネルを介して 2 つの量子通信機能を接続する参照点。光ファイバまたは量子通信に必要な自由空間を介して量子状態信号を交換する。
- Qsync：QKD リンク内の古典チャネルを介して 2 つの量子チャネル同期機能を接続する参照点。量子チャネルの同期に必要な情報を交換する。

- Qdist：QKD リンク内の古典チャネルを介して 2 つの鍵蒸留機能を接続する参照点。鍵蒸留に必要な、QKD プロトコルにおけるシフティング、パラメータ評価、誤り訂正およびプライバシー強化に関する情報を交換する。

注 1 - QKD レイヤにおける最小の接続構成は、QKD モジュール A、QKD リンク、および QKD モジュール B のセットである。QKD リンクの両端のインタフェース仕様は同じであると仮定されるので、この最小構成内に Qqc、Qsync および Qdist を 1 つずつ規定すれば充分である。

注 2 - Qsync 及び Qdist は、9 章の QKDN 構成に関する図では、簡略化のために単一の参照点 Qx で示されている。

8.2. KMの参照点

次の参照点は、KM リンク内の KM との接続に関連する。

- Kq-1：KMA 内の鍵格納機能と QKD モジュール内の QKD-鍵供給機能を接続する参照点。QKD モジュールによって生成された QKD-鍵を KM に転送する。
- Kq-2：KM 内の KM 制御・管理機能と QKD モジュール内の QKD モジュール制御・管理機能を接続する参照点。QKD モジュールが QKD リンクパラメータを KM に送信できるようにし、KM が QKD モジュールの動作を制御できるようにする。
- Kx-1：KMA リンクを介して各 QKD ノード内の KMA を相互に接続する参照点。KMA 間の鍵リレー、鍵同期、および認証に必要な操作と情報を交換する。
- Kx-2：KSA リンクを介して各 QKD ノード内の KSA を相互に接続する参照点。KSA 間で共有される鍵の同期と認証に必要な操作と情報を交換する。
- Kx'：KM リンクを介して各 QKD ノード内のローカル KM と集中型 KM を接続する参照点。集中型鍵リレーを行うために必要な操作と情報を交換する。(9 章の図 5 参照)

注 - Kx-1 および Kx-2 は、9 章の QKDN 構成に関する図では、簡略化のために単一の参照点 Kx として示されている。

8.3. QKDNコントローラの参照点

次の参照点は、QKDN コントローラの通信に関連する。

- Ck：QKDN コントローラ内の QKDN コントローラ制御・管理機能と KM 内の KM 制御・管理機能を接続する参照点。QKDN コントローラが KMA 及び KSA と制御情報の通信を行う。
- Cq：QKDN コントローラ内の QKDN コントローラ制御・管理機能と QKD モジュール内の QKD モジュール制御・管理機能を接続する参照点。QKDN コントローラが QKD モジュールと制御情報の通信を行う。
- Cops：QKDN コントローラ内の QKDN コントローラ制御・管理機能と、QKD リンク内の光信号切り替え/分配機能を接続する参照点。QKDN コントローラが QKD リンクと光信号切り替え/分配に関する制御情報の通信を行う。
- Cqrp：QKDN コントローラ内の QKDN コントローラ制御・管理機能と、QKD リンク内の量子リレーポイント機能を接続する参照点。QKDN コントローラが QKD リンクと量子リレーポイントの制御情報の通信を行う。
- Cx：各 QKD ノード内の QKDN コントローラ制御・管理機能を相互に接続する参照点。2 つの QKDN コントローラが相互に制御情報の通信を行う。

8.4. QKDNマネージャの参照点

次の参照点は、QKDN マネージャの通信に関連する。

- Mq：QKDN マネージャと QKD モジュール内の QKD モジュール制御・管理機能を接続する参照点。QKDN マネージャが QKD モジュールと管理情報の通信を行う。
- Mops： QKDN マネージャと QKD リンク内の光信号切り替え/分配機能を接続する参照点。QKDN マネージャが QKD リンクと管理情報の通信を行う。
- Mqrp：QKDN マネージャと QKD リンク内の量子リレーポイント機能を接続する参照点。QKDN マネージャが QKD リンクと量子リレーポイントの管理情報の通信を行う。
- Mk：QKDN マネージャと KM 内の KM 制御・管理機能を接続する参照点。QKDN マネージャが KMA および KSA と管理情報の通信を行う。
- Mc：QKDN マネージャと QKDN コントローラ内の QKDN コントローラ制御・管理機能を接続する参照点。QKDN マネージャが QKDN コントローラと管理情報の通信を行う。
- Mu：ユーザネットワーク内のユーザネットワークマネージャと QKDN 内の QKDN マネージャを接続する参照点。QKDN マネージャがユーザネットワークマネージャと管理情報の通信を行う。

8.5. ユーザネットワークマネージャの参照点

- Ma：ユーザネットワーク内の暗号アプリケーションとユーザネットワークマネージャを接続する参照点。暗号アプリケーションの管理を行う。

8.6. 暗号アプリケーションの参照点

次参照点は、ユーザネットワークの暗号アプリケーションの通信に関連する。

- Ak：KSA 内の暗号アプリケーションと KSA 内の鍵供給機能を接続する参照点。暗号アプリケーションから KSA への鍵要求の送信、暗号アプリケーションと KSA 間の認証の実行、および KSA から暗号アプリケーションへの鍵供給を行う。
- Ax：ユーザネットワーク内の 2 つの暗号アプリケーションを接続する参照点。2 つの暗号アプリケーションが通信プロトコルに基づいて情報交換を行う。

注- Ax で使用される通信プロトコルには、インターネットプロトコルセキュリティ(IPSec)[b-RFC4301]、トランスポート層セキュリティ(TLS)[b-RFC8446]、またはその他の専用の暗号プロトコルなどがある。

9. アーキテクチャ上の構成

QKDN アーキテクチャ内でサポートされているさまざまな機能要素を相互接続するために、複数のネットワーク構成が可能である。

6 章で定義された機能アーキテクチャモデルの下で、QKDN は、以下に示されるように、異なる構成の様々な機能を含む異なるタイプのノードから構成される。

注 - この章で定義されるノードは、QKDN 内で個別に識別可能な論理的機能要素である。論理的対象物のため、そのようなノードは、物理オブジェクトにマップされることもされないこともある。

9.1. 構成1：分散型QKDN

分散型 QKDN の構成を、構成 1 として図 2 に示す。

構成 1 では、QKDN はタイプ 1 の QKD ノードで構成される。

各タイプ 1QKD ノードは、集中型ネットワークコントローラに依存することなく、分散方式で QKDN 機能を実行することができる。

タイプ 1 の QKD ノードは、QKD モジュール、KM および QKDN コントローラの機能を含む。

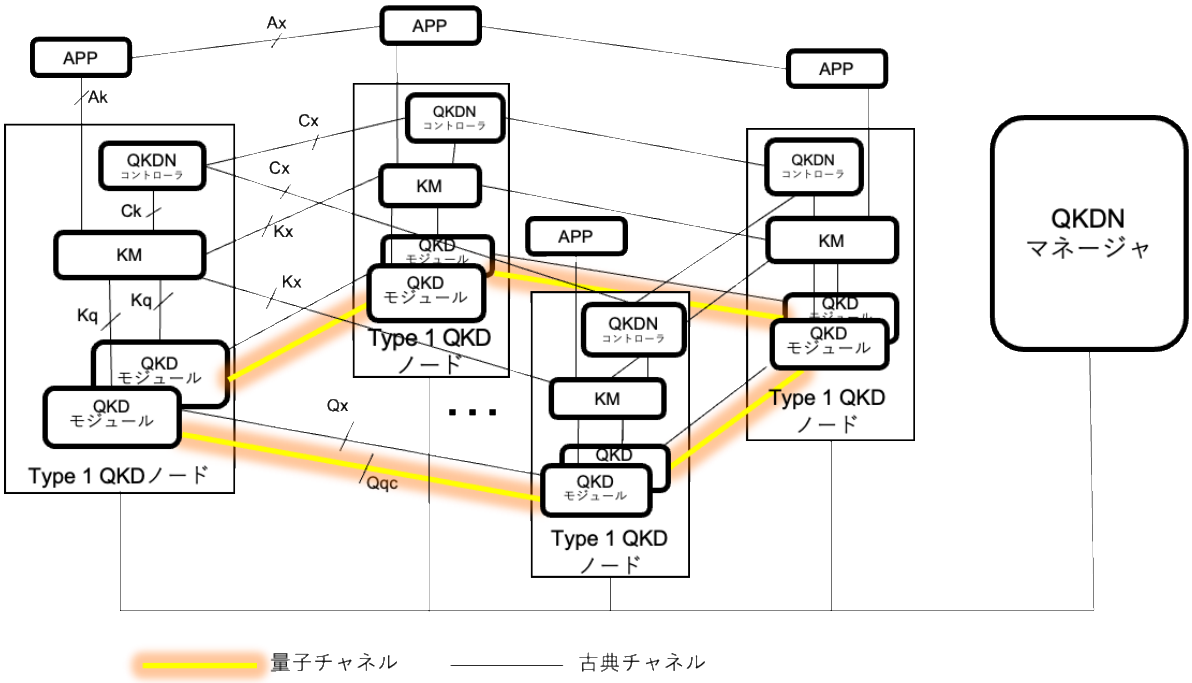

図 2 構成 1： 分散型 QKDN

注 – 9 章の図で用いられている略語 APP は、暗号アプリケーションを意味する。

9.2. 構成2：集中型QKDN

QKDN の効率的な管理をサポートするためには、ネットワーク制御効率が改善されるよう QKDN 制御機能を集中化することが典型的なアプローチである。

集中型 QKDN の構成を、構成 2 として図 3 に示す。

構成 2 では、QKDN はタイプ 2 の QKD ノードと、集中化された 1 つ以上の QKDN コントローラで構成される。

タイプ 2 の QKD ノードは、QKD モジュールおよび KM の機能を含む。

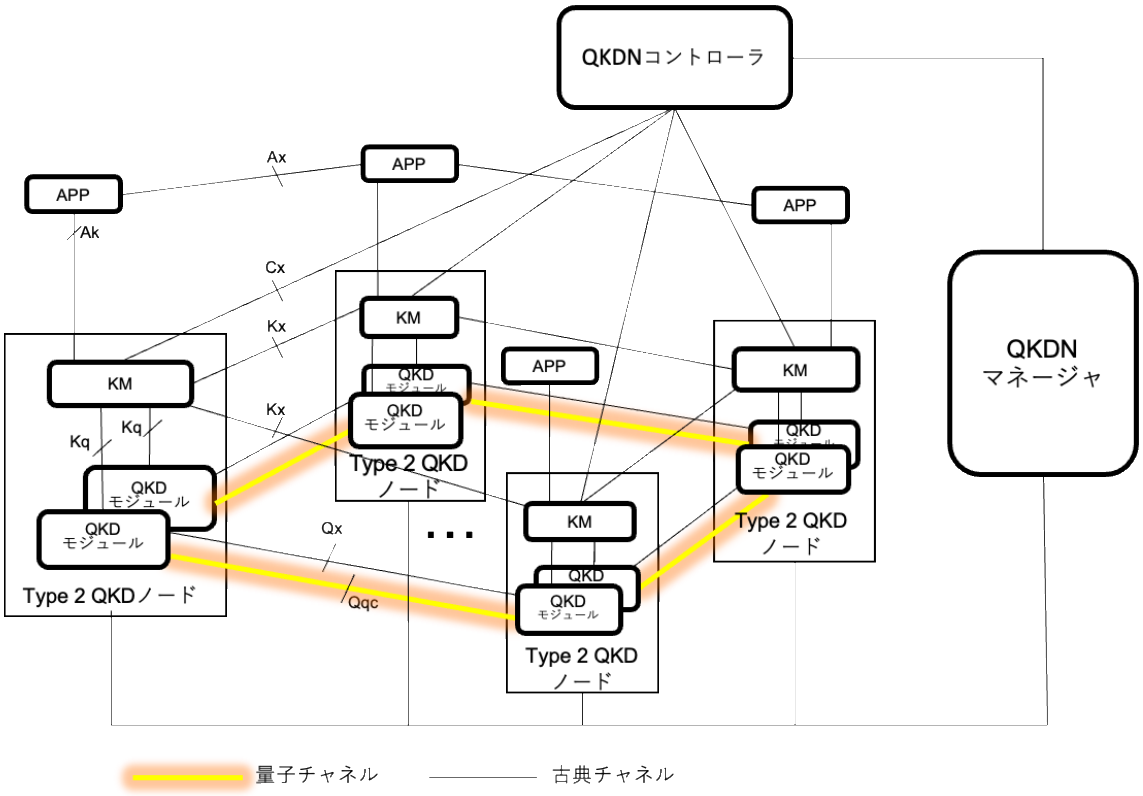

図 3　構成 2：集中型 QKDN

9.3.　構成3：階層QKDノードを持つ集中型QKDN

広域 QKDN の展開と運用をサポートするために、9.2 節に示したタイプ 2 の QKD ノードを、その役割により QKDN ユーザノード、QKDN アクセスノード、QKDN リレーノードの 3 種類のノードに分類することができる。階層 QKD ノードを有する集中型 QKDN の構成を、構成 3 として図 4 に示す。

1)　QKDN ユーザノード

QKDN ユーザノードは、QKD ユーザ側に位置するトラステッドノードである。QKDN から鍵を取得し、安全な通信のために特定の暗号アプリケーションに対応する鍵を提供する。ユーザノードは、QKD モジュールと KM で構成される。ユーザノードは、ユーザ装置のコストを低減するために、1 つの QKD-Tx のみを含むことが一般的である。ユーザノードの KM は、鍵格納、鍵供給、および鍵リレー機能を実行する。

2)　QKDN アクセスノード

QKDN アクセスノードは、接続するユーザノードの鍵リレーサービスフローを集約し、鍵リレースキームに従ってリモート QKD ノードに転送するトラステッドノードである。ユーザノードは、直接または光スイッチを介してアクセスノードに接続する。光スイッチは、複数のユーザノードからの量子信号を同時に受信するために複数の量子チャネルを統合する、アクセスノードの 1 つのオプションの構成要素である。

アクセスノードは、関連するユーザノードの信号を処理するため高性能な QKD-Rx を含むことが一般的である。チャネルリソースを複数の関連するユーザノードにそれぞれ割り当てるために、マルチユーザスケジューリング機能が統合される。

さらに、アクセスノードは、鍵リレーのためにリモート QKD ノード(例えば、リレーノード)に接続する追加の QKD モジュールを含むことができる。

アクセスノードの KM は、鍵格納および鍵リレー機能を実行する。

3)　QKDN リレーノード

QKDN リレーノードは、QKD 量子チャネルの制限を越えて QKD 距離を拡張する目的で鍵リレールートを設定するために使用されるトラステッドノードである。リレーノードには通常、QKD リンクで少なくとも 2 ホップの接続をするために、少なくとも 1 対の QKD-Tx と QKD-Rx が含まれる。リレーノードの KM は、鍵格納および鍵リレー機能を実行する。

ユーザノード、アクセスノード、およびリレーノードの組み合わせによって、このアーキテクチャ構成は柔軟な QKDN トポロジをサポートできる。例えば、複数のユーザノードと接続するアクセスノードによって、大都市圏を網羅するのに適した QKD アクセスネットワーク(QAN)を形成できる。また複数のリレーノードで QKD バックボーンネットワーク(QBN)を形成し、広域を網羅するために複数の QAN を接続できる。

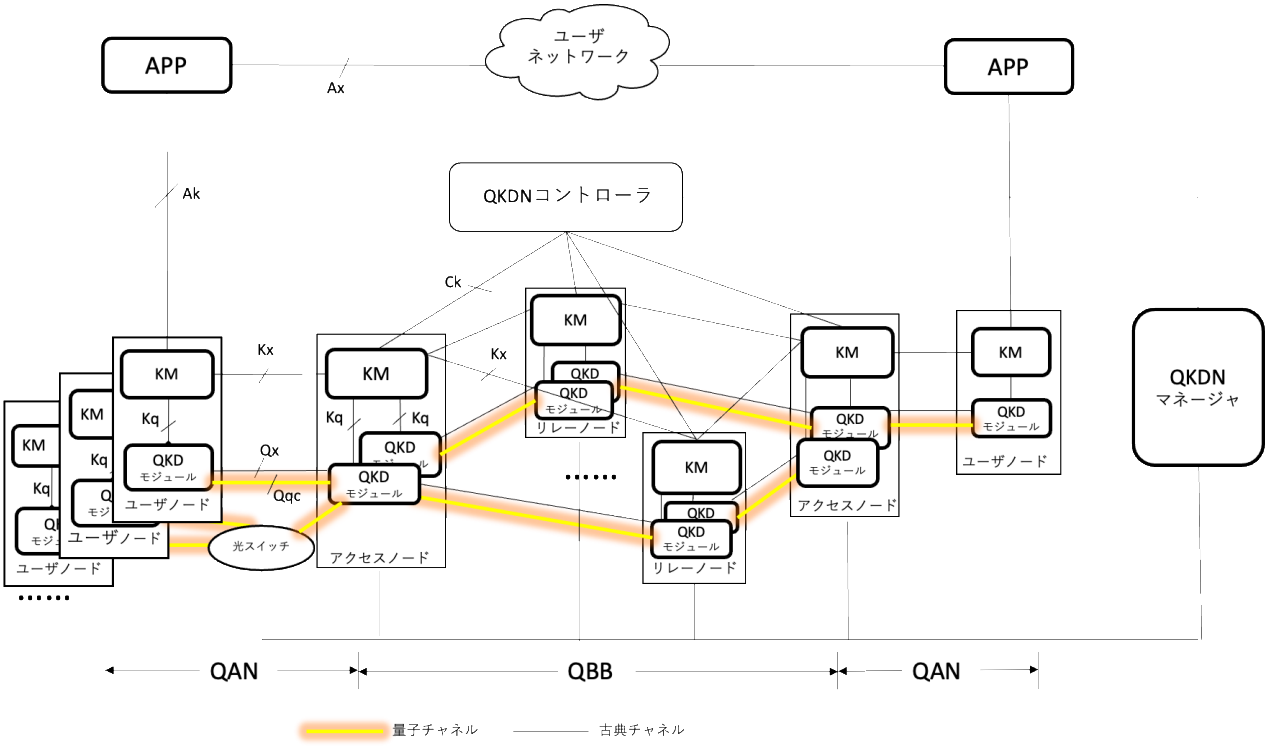

図 4　構成３：階層 QKD ノードを有する集中型 QKDN

9.4.　構成4：集中型鍵リレーを行う集中型QKDN

構成 4 として、集中型 QKDN の構成のバリエーションがある。構成 4 では、図 5 に示すように、KM の鍵リレー機能が集中化され、集中化された QKDN コントローラと共存させることができる。

このようにすると、KM リンク内の QKD ノード間の、ピアツーピアでやり取りを行うためのインタフェースを省略することができる。したがって、QKD ノードの複雑さをさらに低減することができ、ネットワークのオーバーヘッドも低減される。

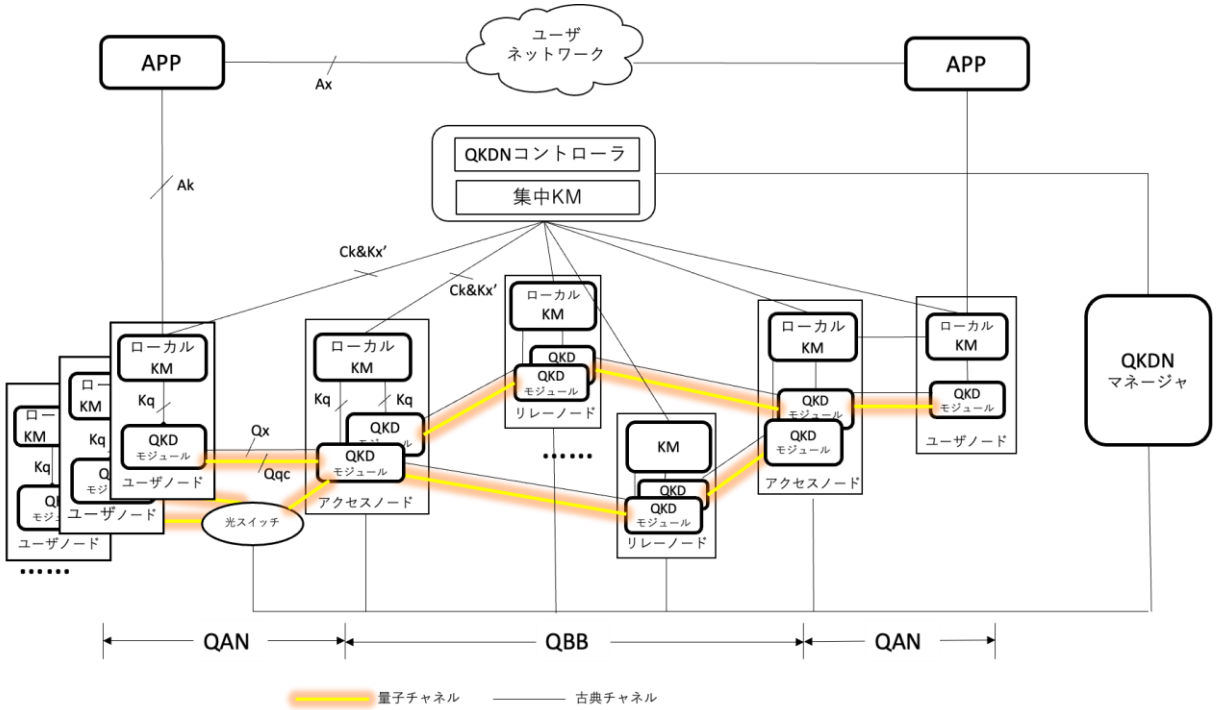

図 5　構成 4 ：集中型鍵リレーを行う集中型 QKDN

10.　QKDN機能の基本動作手順

6 章で定義された機能アーキテクチャモデルに基づいて、この章では基本動作手順について記述する。

10.1.　サービスプロビジョニングとシステム初期化手順

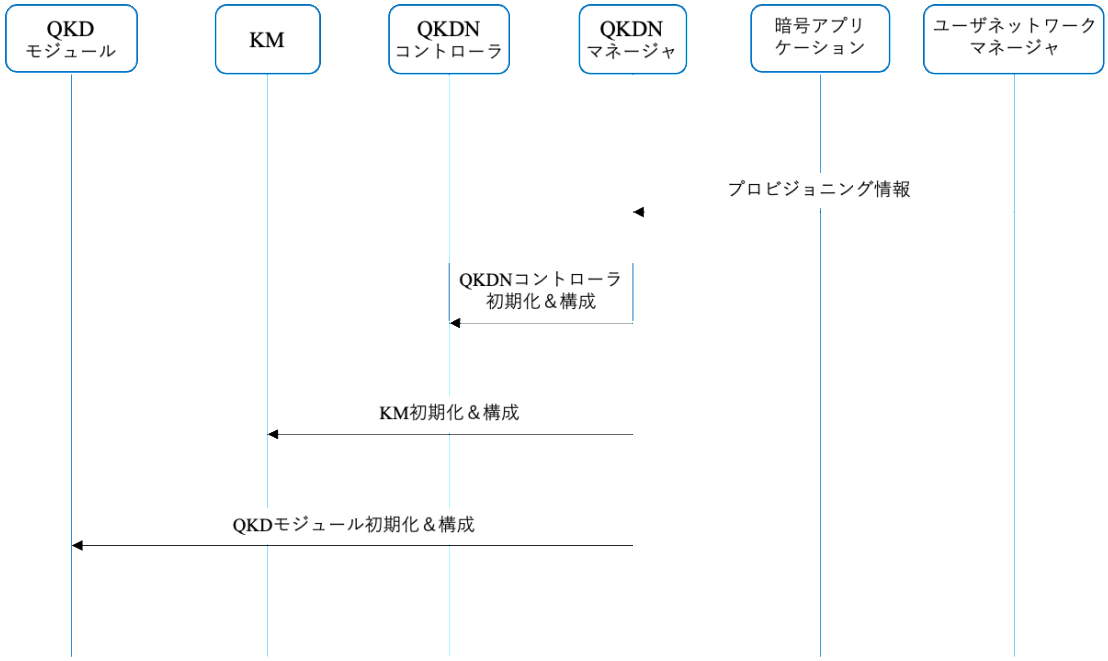

図 6　サービスプロビジョニングとシステム初期化手順

図 6 は、サービスプロビジョニングとシステム初期化手順を示している。

サービスプロビジョニングには 2 つの選択肢がある。

ユーザネットワークマネージャがサービスプロビジョニングを担当する場合、ユーザネットワークマネージャは、暗号アプリケーションのプロファイルを含むサービスプロビジョニング情報を QKDN マネージャに提供する。

一方、QKDN マネージャが独立してサービスプロビジョニングを担当する場合、QKDN マネージャは、自身のサービスプロビジョニング情報を直接使用する。

プロビジョニング情報に従って、QKDN マネージャは、QKDN コントローラ、KM、および QKD モジュールを動作させ、QKDN を初期化して構成する。QKDN コントローラ、KM、および QKD モジュールの初期化と構成管理の順序は任意である。

10.2. 鍵生成手順

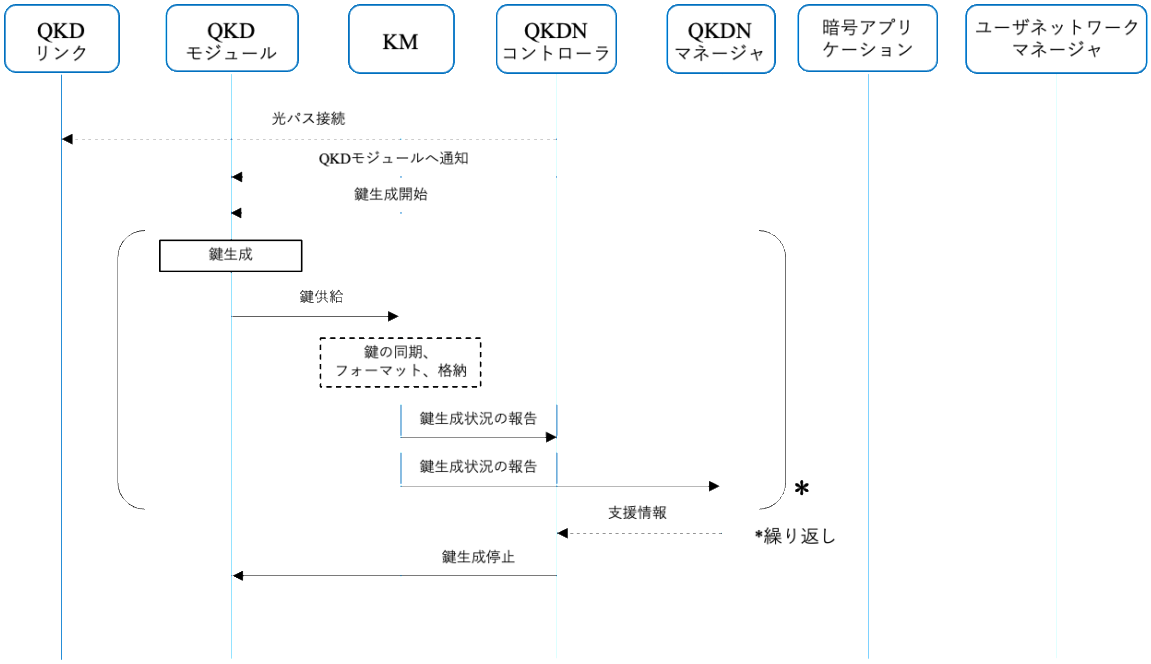

図 7　鍵生成手順

図 7 は、次のステップを含む鍵生成手順を示している。

1) QKDN コントローラは、必要に応じて QKD リンクにおける光パスの接続開始を指示し、QKD モジュールにその結果を通知する。

2) QKDN コントローラは、QKDN モジュールに鍵生成の開始を要求する。

3) QKD モジュールは量子信号を送受信し、量子信号の同期と鍵生成のための鍵蒸留を行う。

4) QKD モジュールは、生成された鍵を KM に供給する。

5) KM は、必要に応じて、これらの鍵を同期し、フォーマットし、格納する。

6) KM は、鍵生成の状況を、QKDN コントローラ及び QKDN マネージャに報告し、それぞれの制御と管理機能に用いられる。

7) ステップ 3 からステップ 6 までのシーケンスは、十分な数の鍵が生成されるまで繰り返すことができる(多くの場合、並行して実行される)。

8) QKDN マネージャは、必要に応じて QKDN コントローラに支援情報を送る。

9) QKDN コントローラは、鍵生成が完了した等の理由により、QKD モジュールへ鍵生成の停止を要求する。

10.3. 鍵要求と供給手順

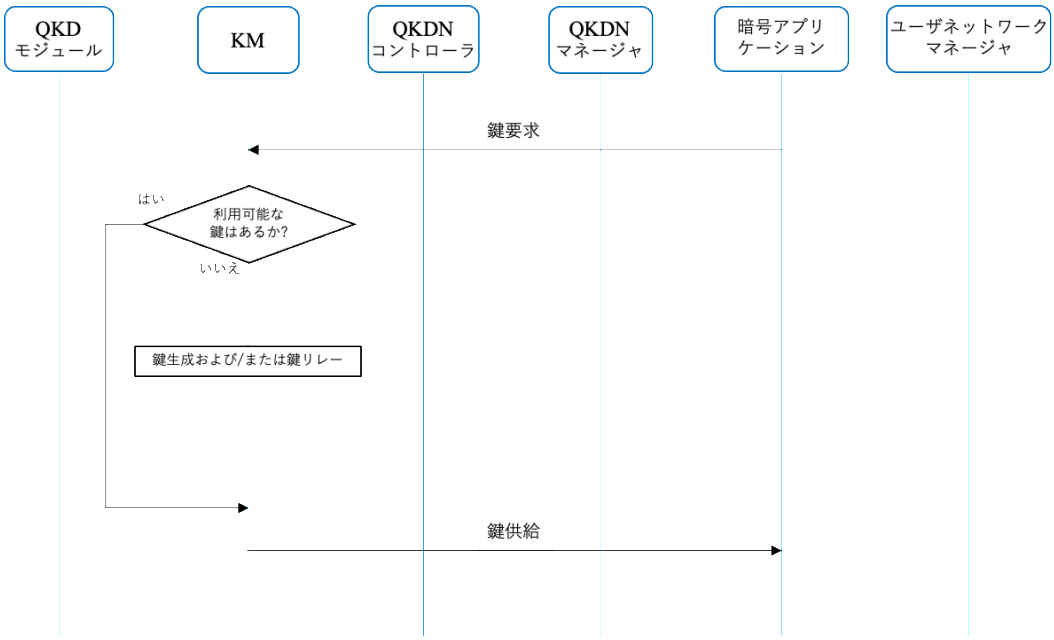

図 8　鍵要求と供給手順

図 8 は、次のステップを含む鍵要求および供給の一般的な手順を示している。

1) ユーザネットワーク内の暗号アプリケーションは、QKDN 内の対応する KM へ安全な鍵を要求する。

2) KM は、組となる暗号アプリケーションに対応するもう一方の KM との間で共有する鍵が利用可能かチェックする。

   a) KM が十分な量の利用可能な鍵を有する場合、ステップ 3 に進む。

   b) KM が利用可能な鍵を持たない場合、KM は鍵生成および/または鍵リレープロセスを通じて利用可能な鍵を得る。

3) KM は、要求元の暗号アプリケーションに鍵を供給する。

10.4. 鍵リレー手順

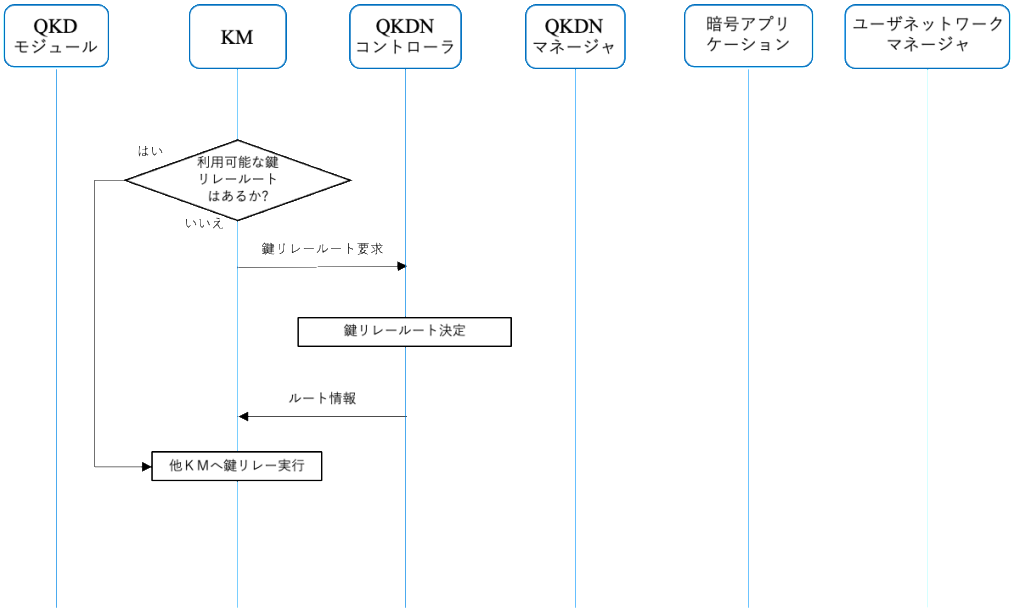

図 9　鍵リレー手順

図 9 は、次のステップを含む鍵リレーの手順を示している。

1) 鍵リレーが必要な場合、KM は鍵リレールートが利用可能かチェックする。

   a) KM が鍵を他の KM にリレーするために利用可能な鍵リレールートを確認した場合、ステップ 3 に進む。

   b) KM が鍵をリレーするための利用可能な鍵リレールートを有していない場合、KM は、QKDN コントローラに鍵リレールートを要求することができる。

2) QKDN コントローラは、鍵リレールートを決定し、ルート情報を KM に送る。

3) KM は鍵リレーを実行する。

10.5. 鍵リレー再ルーティング制御手順

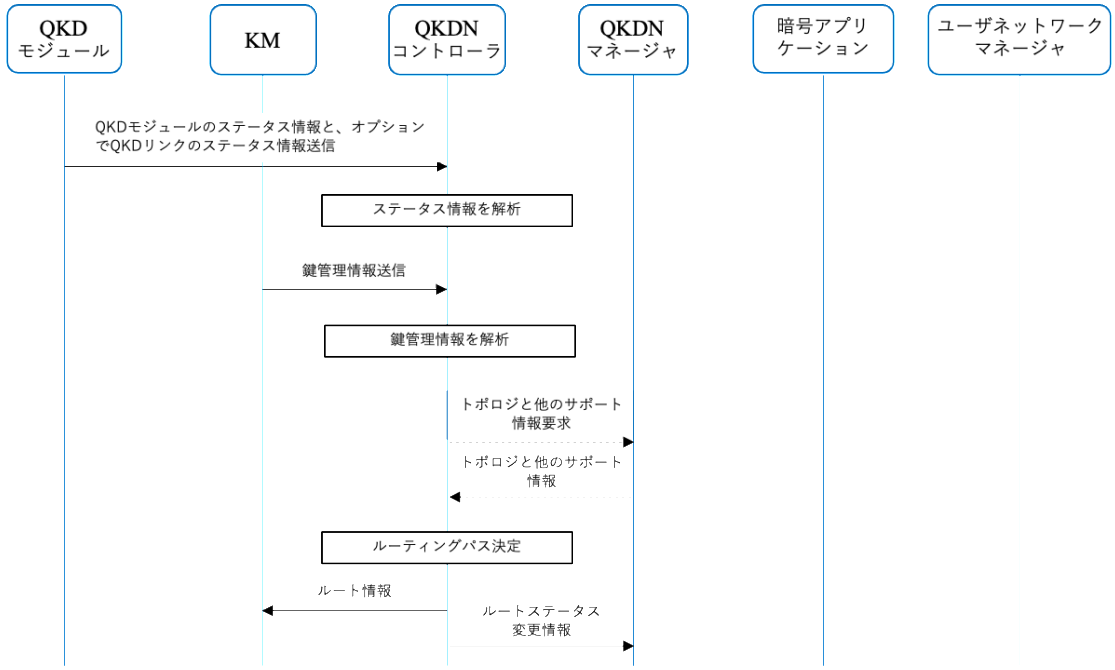

図 10　鍵リレー再ルーティング制御手順

図 10 は、以下のステップを含む QKDN コントローラによる鍵リレーの再ルーティング制御の手順を示す。

1) QKD モジュールは、QKD モジュールのステータス情報（例えば障害、パフォーマンス、可用性）と、オプションで QKD リンクのステータス情報を QKDN コントローラに送信する。

2) KM は鍵管理に関する情報を QKDN コントローラに送信する。

ステップ 1 およびステップ 2 におけるこれらの情報は、QKDN コントローラが QKD リンク、QKD モジュール、KM リンクおよび KM のステータスを連続的に監視できるように、QKD モジュールおよび KM によって定期的に更新される。

3) QKDN コントローラは、提供された情報を解析し、鍵リレーの再ルーティングが必要か否かを判断する。

4) QKDN コントローラは、更新されたルート情報を KM に送信し、QKDN マネージャに対してルートの状態変更情報を報告する。

11. QKDN同期機能に関する考慮事項

既存の他のタイプの通信ネットワークと同様に、QKDN も周波数および時刻の同期をサポートする必要がある。

QKD モジュール間の量子状態光信号の同期を実現するためには、量子チャネル同期機能が必要である。それは極めて高い精度(ピコ秒レベル)を必要とし、最近までに標準化された既存のネットワークベースの同期技術では実現できない。

量子チャネル同期を除いて、他の QKDN 機能のための同期は、従来のネットワークベースの同期技術によってサポートできる。

注 1 - ネットワークタイムプロトコル(NTPv3[b-RFC1305]または NTPv4[b-RFC5905])は、ミリ秒精度の同期をサポートしている。これは QKDN の古典チャネル同期の要求条件を満たすために使用できる。

注 2 - QKDN 同期機能の要求条件及びこれをサポートする技術については、付属資料 II においてさらに分析する。

12. セキュリティ上の考慮事項

セキュリティ上の脅威及び潜在的な攻撃を緩和するために、機密性、完全性、真正性、否認防止、可用性及び追跡可能性の問題に対処する必要があり、また、QKDN、ユーザネットワーク及びこれら 2 つのネットワーク間のインタフェースにおいて適切なセキュリティ及びプライバシー保護スキームが考慮されるべきである。詳細は本標準の範囲外である。

付録A
量子レイヤの機能要素
（この付録は本標準の不可欠な一部を構成する）

図 A-1 は、量子レイヤにおける機能要素間の関係を示す。図 A-1 では、例として集中型 QKDN コントローラモデルを採用している。

QKD リンク内の光信号切り替え/分配および量子リレーポイントは、オプションの機能要素であり、トラステッドである必要はない。実装に応じて、これらの機能要素は、特定の参照点を介して QKDN コントローラおよび QKDN マネージャに接続することができる。参照点 Qdist、Qsync、および Qqc の定義は、QKD リンクの実装によって異なる場合がある。一般的な実装例を次に示す。

- QKD リンクの中間に機能要素が無い：

この場合、2 つの QKD モジュールは直接接続される。Qdist、Qsync、および Qqc は、2 つの QKD モジュール間の単なる参照点である。

- QKD リンク内に光信号切り替え/分配がある:

光信号切り替え/分配機能要素は、一般的には、同期のために量子チャネルおよび古典チャネルを切り替え/分配でき、オプションとして、同一ファイバ内で同期のための量子チャネルおよび古典チャネルと多重化される場合に、鍵蒸留のための古典チャネルを切り替え/分配することができる。

この場合、これらのチャネルは光信号切り替え/分配機能要素を介して接続されるものの、Qdist、Qsync、および Qqc は依然として 2 つの QKD モジュール間の参照点として扱われる。

- QKD リンク内に量子リレーポイントがある:

量子リレーポイント機能要素は、いくつかの QKD プロトコルに使用されるか、[ITU-T Y.3800]の 6.2 章に図示されているように、完全な量子ネットワークにおける量子リピータとして機能する。TF-QKD および MDI-QKD プロトコルでは、量子リレーポイントは、QKD モジュールから送信された量子信号を受信する中間測定ステーションとして機能する。量子もつれベースの QKD プロトコルでは、量子リレーポイントは、量子もつれ光子対を QKD モジュールに分配する量子もつれ光源である。

これらの場合、Qqc および Qsync は、QKD モジュールと量子リレーポイントとの間の参照点である。TF-QKD および MDI-QKD プロトコルの場合、Qdist は 2 つの参照点に分割される。1 つは QKD モジュールと量子リレーポイントの間にあり、もう 1 つは 2 つの QKD モジュールの間にある。量子もつれベースの QKD プロトコルでは、Qdist は QKD モジュール間の参照ポイントである。

完全な量子ネットワークでは、量子リレーポイントは量子リピータとして機能する。量子リピータの主な役割は、量子もつれを抽出し、QKD モジュールへ分配することである。この場合、Qqc および Qsync は、QKD モジュールと量子リレーポイントとの間の参照点である。Qdist は、2 つの参照点に分割される。1 つは QKD モジュールと量子リレーポイントの間にあり、他は 2 つの QKD モジュール間にある。これらの 2 つの参照点は、QKD モジュールと量子リレーポイントとの間の量子もつれ蒸留のための古典チャネルとして使用され、必要であれば、QKD モジュール間の鍵蒸留にも使用される。これらの機能および参照点を介して交換される情報の詳細は、量子リピータのプロトコルおよびその実装に依存して異なる場合がある。

注 – 量子もつれ蒸留は、局所量子演算と古典通信によって、分配された量子信号から量子もつれを蒸留するためのプロトコルである。古典通信は、基準点 Qdist を介して行うことができる。局所量子演算は参照点を必要としない。

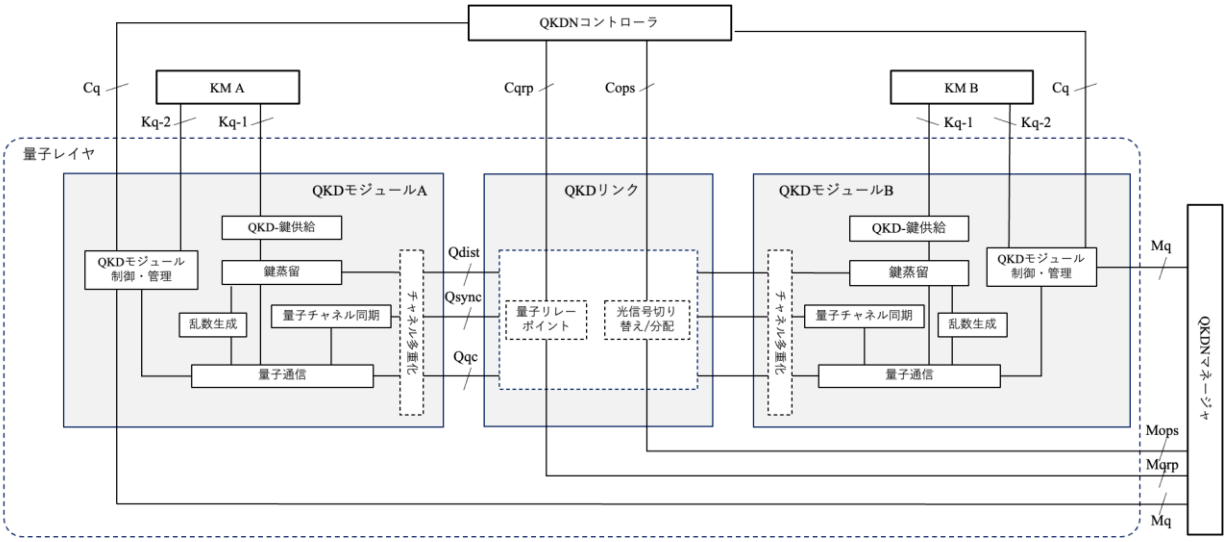

図 A-1 量子レイヤのサブ機能間の関係

付属資料I
参照点の共通機能

（この付属資料は本標準の不可欠な一部を構成しない）

8 章に示した参照点において、QKDN は以下の共通機能を有することができる:

1. セッション処理機能

参照点を介して行われるセッション操作の信頼性と性能を保証するために、QKDN によって以下の機能が提供されることが期待される：

- 過負荷制御：交換される情報メッセージのオーバーフローを防ぐために、過負荷制御をサポートする。
- 同期と監査：セッションステータスの同期と監査をサポートし、リカバリと運用情報の統計および監査をサポートする。
- セッションのメンテナンス：ソフトステートまたはハードステートのアプローチを使用して、セッションステータスを維持できるようにする。

2. 情報交換機能

参照点には、次の情報交換機能が提供される。

- 要求-応答トランザクション：要求する機能または機能要素が、応答する機能によって実行されるトランザクションを要求し、関連する応答を取得できるようにする。
- 通知：2 つのレイヤの機能間での非同期イベントの通知をサポートする。
- 信頼性の高い配信：信頼性の高いメッセージ配信を提供する。
- 能力評価：対応するレイヤの機能の適切な能力を決定する。
- クロスレイヤセキュリティ：認証されていないソースからの要求を実行できないように、また各レイヤが通知を送信するソースを確認できるように、2 つのレイヤ間の認証をサポートする。

付属資料II
QKD ネットワークにおける同期機能と実装
(この付属資料は本標準の不可欠な一部を構成しない)

周波数や時刻同期などの同期技術は、QKDN をはじめとする ICT ネットワークの基盤的な役割を担っていると考えられる。

実装コストと技術成熟度の間のトレードオフを考慮して、同期要件に適合する同期技術を選択することが望ましい。例えば、既存の情報通信ネットワークにおける構成クエリ/配信、ライフサイクル管理、情報の更新、および故障診断の同期要件は、通常、数十ミリ秒レベルの精度である。ほとんどの場合、ネットワークタイムプロトコル(NTP)技術でこの同期要求条件を満たすことができる。NTP は IP ネットワークで一般的に利用されている。

典型的な“prepare-and-measure”方式ベースの離散変数 QKD システムでは、同期のための送信器は、同期チャネルを介して量子信号に同期された光パルスを受信器に送信する。周波数および位相回復を伴う検出された同期信号は、受信器における単一光子検出器(SPD)のトリガーとして使用される。ガウス変調を伴う送信器およびコヒーレント検出を伴う受信器に基づく典型的な連続変数 QKD の場合、物理レイヤ同期チャネルはオプションである。

量子信号の典型的なパルス幅および有効 SPD 検出応答時間ウィンドウは、約 100 ピコ秒レベルであり、これらの信号および応答のジッタは通常数百ピコ秒に制限される。これは、送信機と受信機との間の周波数同期の精度要求条件が、サブマイクロ秒レベルを達成することを意味する。

現在のネットワークベースの周波数同期ソリューションはこの精度要求条件を満たすことができず、したがって、ポイントツーポイントの同期チャネルベースの周波数同期が現実的なソリューションとなる。

QKDN における鍵供給では、対応する鍵のメタデータにデバイス ID などの必要な情報とともに QKD-鍵の生成時刻情報を付加する必要がある。市販の QKD システムの QKD-鍵の生成速度は通常数十 Kbit/秒であり、QKD-鍵の生成時刻情報は数十ミリ秒単位で更新される。そのため、NTP ベースのネットワーク周波数同期は、この精度要求条件に適している。

将来的に QKD-鍵の生成率を大幅に向上させることができれば、これらの鍵のタイミング精度を向上させる必要があり、高精度タイムプロトコル(PTP)などの他の種類のネットワーク時刻同期ソリューションを使用することができる。さらに、NTP によって提供される絶対時刻情報は、アラームおよびパフォーマンス監視のために QKDN 制御ユニットで使用することもできる。

鍵管理レイヤにおいて、KM は、QKD モジュールによって生成されたポイントツーポイント鍵ペアを格納し、鍵リレー機能によってエンドツーエンド鍵を提供する。鍵格納と鍵リレーのプロセスでは、鍵認証、バックアップ、破棄、格納時刻管理などのセキュリティ要求条件に従って、鍵ライフサイクルを管理する必要がある。数十ミリ秒の精度のタイミング基準を持つ NTP ベースのネットワーク時間周波数同期情報を QKD-鍵のメタデータに付加して、生成時刻、リレー時刻、格納時刻、プロビジョニング時刻、破棄時刻などのタイムスタンプ情報を示すことができる。また、KM でのアラーム・性能情報の監視・報告のためには、QKDN がネットワーク全体の時間領域管理を一元化できるように、KM の主制御部において NTP によるミリ秒精度の時刻同期をサポートする必要がある。QKDN 管理レイヤでは、マスタークロックを QKDN の QKDN マネージャ内に共存させることができる。マスタークロックは QKDN の一元化された時間領域管理を実現するために、他の機能への基準タイミング情報を提供できる。これに基づいて、QKDN マネージャおよび/または QKDN コントローラは、QKDN 内の QKD モジュールおよび KM のアラーム情報および性能パラメータ、ならびにネットワークリンクステータスおよび障害の診断および識別を監視することができ、さらに、QKDN とユーザネットワークとの間の相互作用に必要な時刻基準情報を提供することができる。

参考文献

[b-ETSI GR QKD 007] ETSI Group Report GR QKD 007 (2018), *Quantum Key Distribution (QKD); Vocabulary.*

[b-ISO/IEC 18031] ISO/IEC 18031, *Information technology — Security techniques — Random bit generation.*

[b-RFC 1305] IETF RFC 1305 (1992), *Network Time Protocol (Version 3) Specification, Implementation and Analysis.*

[b-RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol.*

[b-RFC 5905] IETF RFC 5905 (2010), *Network Time Protocol Version 4: Protocol and Algorithms Specification.*

[b-RFC 8446] IETF RFC 8446 (2018), *The Transport Layer Security (TLS) Protocol Version 1.3.*

[b-Shannon 1949] Shannon, Claude, 1949, *Communication Theory of Secrecy Systems, Bell System Technical Journal*, vol. 28, pp. 666–682.