量子鍵配送ネットワークの鍵管理システム

Key Management System for Quantum Key Distribution Networks

友田　正憲 TOMODA Masanori

量子鍵配送（QKD）ネットワークにおいて，鍵管理システム（KMS）は，QKDリンクで光ファイバーなどを通じて共有した量子鍵を用いて，暗号鍵を安全に共有し，暗号通信装置に提供する役割を担っている。

東芝デジタルソリューションズ（株）は，2019年からKMSの製品化を進めており，商用利用でのニーズに応えるために国内・海外での実証実験へ適用し，今後必要とされる機能の開発に生かしている。

In a quantum key distribution (QKD) network, the key management system is responsible for securely sharing cryptographic keys through the use of quantum keys, which are shared among the QKD devices via optical fiber, and providing these cryptographic keys to the encryption devices.

Toshiba Digital Solutions Corporation has been promoting the practical application of key management systems since 2019, in response to market demand for the commercial use of QKD networks. Utilizing the results obtained through various demonstration tests in Japan and other countries, we have been developing vital functions for future key management systems.

1. まえがき

KMSは，QKD装置で生成・共有した乱数列（量子鍵）を用いて，暗号鍵の生成とKMS間での共有を行い，暗号鍵を暗号通信装置（暗号を活用するアプリケーションなど）に提供する。この暗号鍵は，暗号・復号処理に用いるものであり，暗号通信装置の間で安全に共有されなければならない。

複数の拠点から構成されるQKDネットワークでは，直接接続されていない拠点間で暗号鍵を共有する必要がある。しかし，QKD装置では，直接接続された拠点間でしか量子鍵を共有できないため，KMSは，QKD装置から得た量子鍵を用いて暗号鍵を中継し，QKDネットワーク内の任意のノードに安全に暗号鍵を提供する[(1)]。

ここでは，KMSが提供する基本的な機能と，暗号鍵を用いた暗号文の通信方式について述べる。

2. KMSのアーキテクチャーと動作

2.1 QKDネットワークの構成

QKDネットワークは，QKD装置を用いて複数の拠点間で暗号鍵を提供するシステムである（**図1**）[(2)]。

QKDネットワークは，複数のQKDノードから構成される。QKDノードには，QKD装置，KMS，及びQKDネットワークコントローラーが含まれる。QKDネットワークは，QKD装置及びQKDリンク（光ファイバーなどで直接接続される）から成る量子鍵配送システム，並びにQKDネットワークコントローラー，KMS，及びKM（鍵管理）リンクから成る暗号鍵流通レイヤーの二つに分かれている。

量子鍵配送システムでは，QKDリンクで接続された二つのQKD装置が，量子鍵を共有する（三つ以上のQKD装置が，同じ量子鍵を共有することはない）。QKD装置は，共有した量子鍵を，同じノード内のKMSに提供する。KMSは，量子鍵を利用して，量子鍵を共有したQKDノードのKMSと暗号鍵を共有する。

2.2 暗号鍵の生成・共有・中継

QKDリンクで直接接続されていないQKDノード間で暗号鍵を共有し，アプリケーションに暗号鍵を提供するために，KMSが暗号鍵を生成・共有・中継する方式（図1で，QKDノードAからQKDノードCへ）を，次に述べる[(3)–(5)]。

① QKD装置は，QKDリンクで直接接続されたQKDノードの間で，量子鍵を共有する。図1の例では，QKDノードAとQKDノードBのQKD装置が量子鍵ABを，QKDノードBとQKDノードCのQKD装置が量子鍵BCを，それぞれ共有する。

② QKD装置は，同じQKDノードのKMSに量子鍵を提供する。

③ KMS Aは，QKDノードAからQKDノードCに暗号通信するための，暗号鍵ACを生成する。

④ KMS Aは，量子鍵ABを利用してワンタイムパッド暗号などの安全な通信方法を用い，KMリンクを通じて，

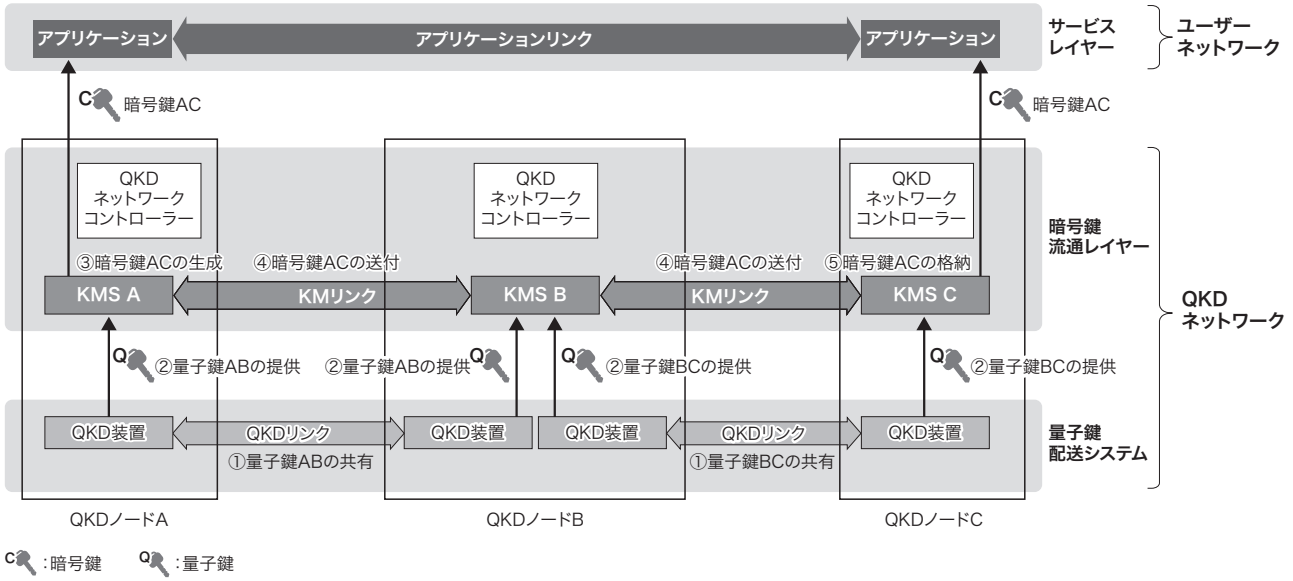

図1. QKDネットワークの構成

QKDネットワークは，複数のQKDノードで構成される。量子鍵配送システムで量子鍵を，暗号鍵流通レイヤーで暗号鍵を共有する。

Configuration of QKD network

暗号鍵ACをKMS Bに送付する。更にKMS Bは，量子鍵BCを利用して，暗号鍵ACをKMS Cに送付する。この際，中継に必要な経路（ここではKMS Bを経由する）は，QKDネットワークコントローラーが決定する。

⑤ KMS Cは，受領した暗号鍵ACを格納する。

アプリケーションは，QKDネットワークで生成・共有された暗号鍵を得て，アプリケーション間で暗号文の送受信，及び暗号・復号処理を行う。

2.3 暗号鍵を用いた暗号文の暗号・復号処理

図2を用いて，アプリケーションDがアプリケーションEへ暗号文を送付する例を示す[6]。

① アプリケーションDは，暗号文送付先のアプリケーションID Eを指定して，QKDノード内のKMS Dの鍵提供機能に暗号鍵を要求する。

② KMS Dの鍵提供機能は，暗号鍵格納機能からQKDノードEに対応する暗号鍵DEと鍵ID xを得て，アプリケーションDに返す。

③ アプリケーションDは，暗号鍵DEを使って平文を暗号化して暗号文を作成し，鍵ID xとともに，アプリケーションEに送付する。

④ アプリケーションEは，アプリケーションID Dと鍵ID xを指定して，KMS Eの鍵提供機能に暗号鍵を要

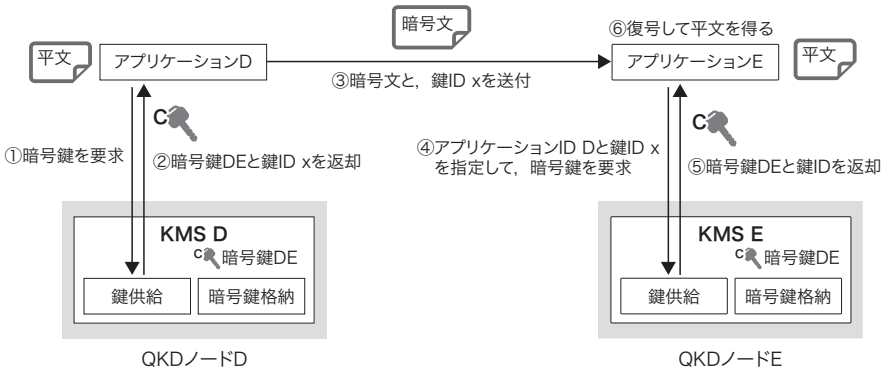

図2. 暗号文の暗号・復号処理

KMSが，直接接続されていないQKDノードに暗号鍵を共有し，アプリケーションが暗号鍵を用いて暗号・復号処理を行う。

Encryption and decryption of ciphertext

求する。

⑤　KMS Eの鍵提供機能は，暗号鍵格納機能から暗号鍵DEと鍵IDを得て，アプリケーションEに返す。

⑥　アプリケーションEは，暗号鍵DEと鍵IDを用いて暗号文を復号し，平文を得る。

3. あとがき

東芝グループは，2019年からKMSの製品開発・実証実験を進めている。実証実験で得られた要望や知見を基に，機能を拡張していく予定である。

今後，暗号鍵の提供にとどまらず，多種多様な暗号通信装置からの利用に対応するための研究開発を進めていく。

文　献

⑴ 谷澤佳道，高橋茉里香．量子鍵配送技術に基づくセキュアネットワーク．東芝レビュー．2014，**69**，1，p.35–38.

⑵ ITU-T Y.3800: Overview on networks supporting quantum key distribution. <https://www.itu.int/rec/T-REC-Y.3800>, (accessed 2022-07-21).

⑶ ITU-T Y.3801: Functional requirements for quantum key distribution networks. <https://www.itu.int/rec/T-REC-Y.3801>, (accessed 2022-07-21).

⑷ ITU-T Y.3802: Quantum key distribution networks - Functional architecture. <https://www.itu.int/rec/T-REC-Y.3802>, (accessed 2022-07-21).

⑸ ITU-T Y.3803: Quantum key distribution networks - Key management. <https://www.itu.int/rec/T-REC-Y.3803>, (accessed 2022-07-21).

⑹ ETSI GS QKD 014 V1.1.1:2019. Quantum Key Distribution (QKD); Protocol and data format of REST-based key delivery API. <https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf>, (accessed 2022-07-21).

友田　正憲　TOMODA Masanori
東芝デジタルソリューションズ（株）
ICTソリューション事業部 QKD事業推進室
情報処理学会会員
Toshiba Digital Solutions Corp.