L-036

量子暗号通信のための セキュア鍵共有ルーティングプロトコルの提案

A Routing Protocol for Secure Key Exchange in Quantum Key Distribution Networks

高橋 莉里香† Ririka Takahashi
谷澤 佳道† Yoshimichi Tanizawa
佐藤 英昭† Hideaki Sato
川村 信一† Shinichi Kawamura

概要

量子暗号通信における制約を考慮して，効率的にセキュア鍵を共有するためのルーティングプロトコルを提案する．本プロトコルは，盗聴の検出が可能な暗号鍵共有技術である量子鍵配送を行うノードをネットワーク接続した量子暗号通信ネットワークに適用できるものである．量子暗号通信ネットワークでは，任意のノード間でセキュアに暗号鍵を共有できるものの，量子鍵配送技術の鍵共有速度などの制約から，従来のルーティングプロトコルを用いた経路選択では必ずしも効率的に暗号鍵を共有できるとは限らない．本プロトコルでは，量子鍵配送技術の制約を考慮するため，量子鍵配送による鍵の生成量をメトリックとし，システム全体で消費される鍵の総量を最小化する経路選択を行う．

1. はじめに

現在利用されている暗号方式は，解読アルゴリズムの発明や量子コンピュータの開発などにより危殆化するリスクがある．本稿では，危殆化リスクのない量子鍵配送技術を用いた量子暗号通信ネットワークにおいて，暗号鍵を共有する際の制約を考慮した効率的な鍵配送ルーティングプロトコルを提案する．

まず，量子暗号通信ネットワークの概要と課題について説明する．そして，量子暗号通信ネットワーク上で効率的に鍵配送を行うためのルーティングプロトコルの設計を提案し，具体的な適用例を示す．

2. 量子暗号通信ネットワーク

光ファイバーで接続された送信者と受信者が単一光子通信を用いて，暗号通信で利用する乱数（暗号鍵）を共有する技術を量子鍵配送技術という．量子力学の理論に基づき，通信路上での盗聴を検出できることから，究極の暗号通信技術として知られている．ここでは，量子鍵配送技術を利用して共有した暗号鍵を用いて，暗号通信を行うネットワークのことを量子暗号通信ネットワークとよぶ．量子暗号通信ネットワークは，量子鍵配送技術による暗号鍵の共有手法をネットワークにまで拡張するものである[1].

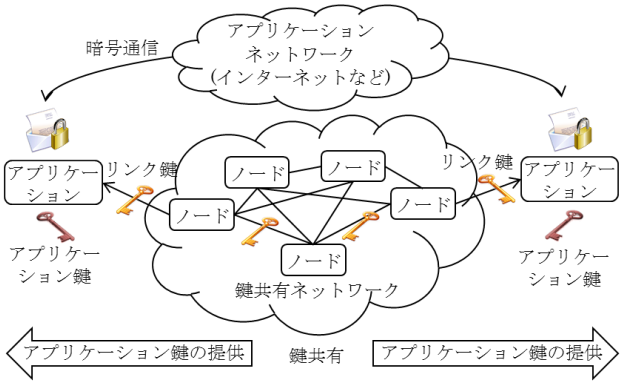

図 1 量子暗号通信ネットワークの構成

† 株式会社 東芝 研究開発センター，Corporate Research & Development Center, TOSHIBA Corporation

図 1 のように，量子暗号通信ネットワークは暗号通信に利用するアプリケーションネットワークと，暗号鍵を共有するための鍵共有ネットワークからなる．

鍵共有ネットワークでは，複数のノードが相互に光ファイバーで接続されており，隣接するノード同士は量子鍵配送技術により乱数（リンク鍵）を共有する．各ノードはさらに，アプリケーションネットワークにおいて共通鍵暗号方式でデータを送受信するときに用いる乱数（アプリケーション鍵）を別途生成する．ノードは，リンク鍵を用いてアプリケーション鍵を暗号化・復号しながらノードを介して転送することで，離れたノードとの間で安全にアプリケーション鍵を共有することができる．アプリケーションはノードに接続し，必要に応じてアプリケーション鍵を取得し，インターネットなどのアプリケーションネットワーク上で，アプリケーション鍵を用いた暗号通信を行う[2].

量子暗号通信ネットワーク上のノードが，任意のノードとの間でアプリケーション鍵を共有するためには，鍵共有ネットワーク上でルーティングプロトコルを適用する必要があり，ルーティングプロトコル OSPF（Open Shortest Path First）を導入する方法が知られている[1]. OSPF は，経路を選択するためのメトリックとしてコストの合計値を利用する．ここで，メトリックとは各パスに割り当てられる評価値のことであり，コストは各リンクに割り当てられる帯域幅などの値のことである．

3. 既存のルーティングプロトコルの課題

鍵共有ネットワーク上でアプリケーション鍵を交換する際，各リンク上ではリンク鍵を用いて暗号化・復号を行う．よって，各リンク上のリンク鍵の生成速度，および，残量に応じて，アプリケーション鍵の転送速度が律速される．これを考慮して，リンク鍵を枯渇させずに円滑にアプリケーション鍵の交換を実現する経路が選択されるべきである．

一方，選択される経路上のリンク数が多いほど，システム全体において消費するリンク鍵の総量は増加する．量子暗号通信ネットワークにおいて，リンク鍵は貴重なシステムリソースであるため，リンク数の少ない経路を選択し，消費するリンク鍵の総量を抑えることが望ましい．

以上で述べた二つの要求を満たす，量子暗号通信ネットワーク向けの効率的なルーティングアルゴリズムを設計す

ることを課題とする．

4. 提案手法

本章では，第 3 章の課題を解決する鍵共有ネットワーク向けの効率的なルーティングプロトコルを提案する．本プロトコルは，OSPF をベースとして，動的に変化するリンク鍵の生成量をメトリックとして採用し，ノード間で生成する鍵の量が多い経路，かつ，暗号鍵の共有によってノード間で消費される鍵の総量を最小化する経路を選択する．提案するルーティングプロトコルを利用することで，リンク鍵生成速度とリンク鍵保有量を一定の値以上に保ち，アプリケーションネットワークにおけるデータ通信速度を律速することなく，システム全体の鍵消費を抑制するルーティングが可能となる．

4.1. ルーティングアルゴリズム

鍵消費を抑制するルーティングプロトコルでは，コストとして，リンク鍵生成速度とリンク鍵保有量を考える．リンク鍵生成速度とはノード間で量子鍵配送を行うことでリンク鍵を共有する速度を表すものであり，動的に変化し続ける．リンク鍵保有量とはノード間で共有した鍵の中で未使用の鍵の量のことであり，使用量に応じて変化する．

高いビットレートで暗号通信を行うためには，保有するリンク鍵の量が最も少ないリンク，あるいは，リンク鍵の生成速度が遅いリンクといったボトルネックとなるリンクを避けて，アプリケーション鍵を共有したい．さらにシステム全体では，経由するリンクが少ない経路を選択し，リンク鍵の消費量を抑えたい．そこで本プロトコルでは，パスにおいてボトルネックとなるリンクのコスト（以下，ボトルネックコスト）と送信元ノードから宛て先ノードまでのパスのホップ数をメトリックの算出に用いる．

以上より，鍵消費抑制ルーティングプロトコルは以下のステップとアルゴリズムからなる．

記法：

s：始点，V：グラフ全体の点の集合，VP：ボトルネックが確定した点の集合，$V \setminus VP$：ボトルネックが未確定の点の集合，$BN[n]$：点 n までのボトルネック，$hop[n]$：点 n までのホップ数，$cost[l]$：辺 l のコスト，$path[n] = l$：点 n への経路が辺 l

アルゴリズム：

1. 始点 s を選び，$VP := \emptyset$, $BN[s] := 0$, $hop[s] := 0$ $(path[s] := 0)$ とし，s 以外の点 v に対しては， $BN[v] := -1, hop[v] := 0$ $(path[v] := -1)$ $(v \notin V \setminus \{s\})$ とする．
2. $V = VP$となるまで以下を繰り返す．
   a. $BN[w] = \max\{BN[v] | v \in V \setminus VP\}$ となる点 w を求める．
   b. $VP := VP \cup \{w\}$ とする．w を始点とする各辺 $e = (w, v)$ に対して以下の操作を行う．

   if $BN[w] > co\quad t(e) > BN[v]$
   　then $BN[v] := cost(e)$,
   　　$hop[v] := hop[w] + 1$ $(path[v] := e)$
   if $cost(e) > BN[v] = BN[w]$ and $hop[v] > hop[w] + 1$
   　then $BN[v] := BN[w]$,
   　　$hop[v] := hop[w] + 1$ $(path[v] := e)$
   if $BN[w] \geq BN[v] = cost(e)$ and $hop[v] > hop[w] + 1$
   　then $BN[v] := cost(e)$,
   　　$hop[v] := hop[w] + 1$ $(path[v] := e)$
   if $cost(e) > BN[v] = BN[w]$ and $hop[v] > hop[w] + 1$
   　then $BN[v] := BN[w]$,
   　　$hop[v] := hop[w] + 1$ $(path[v] := e)$

4.2. プロトコル適用例

鍵消費抑制ルーティングプロトコルの適用例として，図 2 のネットワークで，表 1 のパス a，パス b，および，パス c を考える．リンクに振られた番号をリンクのコストとする．

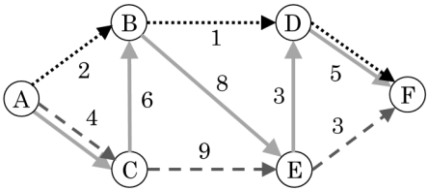

図 2　適用例

表 1　各パスのボトルネックコストとホップ数

パス	通るノード	ボトルネックコスト	ホップ数
a (⇢)	ABDF	1	3
b (→)	ACBEDF	3	5
c (⇢)	ACEF	3	3

ボトルネックコストを考慮すると，ボトルネックコストが 3 であるパス b とパス c が鍵を転送する経路の候補となる．さらに，パスに含まれる各リンクにおいてリンク鍵を消費すると考えると，ホップ数 5 であるパス b に比べ，ホップ数 3 であるパス c は鍵消費を抑えることができる．このようにして選択されたパス c に沿って鍵を転送することで，ボトルネックを避けつつ，鍵消費を抑えるルーティングが可能となる．

5. おわりに

本稿では，量子鍵配送技術を用いた量子暗号通信ネットワークの鍵共有ルーティングの設計例を示した．動的に変化する鍵の生成量や保有量をメトリックとして経路を選択し，かつ，ノード間で消費される鍵の総量が小さい経路を選択することで，暗号通信の速度を律速することなく，システム全体の鍵消費を抑制するルーティングが可能となる．本設計に基づくノードを，量子鍵配送装置のエミュレータ上に実装し，ビデオアプリケーションを OTP（One Time Pad）暗号で動作させ検証を行った．今後は，鍵消費をより抑えるために他のメトリックの導入や組合せの検討を行うとともに，実機接続によるシステム評価を目指す．

参考文献

[1] Dianati, M., et al. “Architecture and protocols of the future European quantum key distribution”, Security and Communication Networks Volume 1, Issue 1 (2008).

[2] 谷澤佳道ほか，量子鍵配送技術をモチーフとしたセキュアネットワークの一提案，電子情報通信学会　2012 ソサイエティ大会，富山大学 (2012).