様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３０　年　　６　月　１４　日現在

機関番号：　１４６０３
研究種目：　挑戦的萌芽研究
研究期間：　2015～2017
課題番号：　１５Ｋ１１９８３

研究課題名（和文）オープンフロー時代に適した情報理論的に安全な秘密鍵共有

研究課題名（英文）Information-theoretically secure secret key sharing suitable for open flow networks

研究代表者

林　優一（Hayashi, Yuichi）

奈良先端科学技術大学院大学・情報科学研究科・教授

研究者番号：６０５５１９１８

交付決定額（研究期間全体）：（直接経費）　　2,800,000円

研究成果の概要（和文）：本研究では、以下の要素技術について検討を行い、通信経路を動的に変更可能な公衆ネットワークにおいて、情報理論的に安全な秘密鍵の生成を可能とし、得られた秘密鍵を用いて安全な情報通信を可能とした。要素技術1：OpenFlowスイッチ及びOpen vSwitchを用いたセキュリティモデルを実現するための仮想的秘匿通信路を確立する技術の開発、要素技術2：鍵共有グラフにSTフロープロトコルを適用し、盗聴者に秘密鍵が漏えい する確率を最小値に抑えるための手法の開発、要素技術3：要素技術2に基づいた多人数で共通の秘密鍵を公衆ネットワーク上で共有する手法の開発

研究成果の概要（英文）：In this research, we developed the following key technologies. As a result, in the public network where the communication paths can be changed dynamically, we achieved information theoretically secure secret key generation. Then, using the obtained secret keys, secure information communication paths can be established on a public network. Key Technology 1: We developed a technique to establish a virtual secret communication path using OpenFlow switch and Open vSwitch. Key Technology 2: We applied the ST flow protocol to the secret key sharing graph and developed a method to minimize the probability of leakage of secret keys to eavesdropper. Key Technology 3: Developed a multiparty method to share a common secret key on a public network based on Key Technology 2.

研究分野：　情報学基礎理論

キーワード：　秘密鍵共有　秘匿通信路　セキュア通信　SDN

１．研究開始当初の背景

本研究の着想のきっかけとなったOpenFlow（オープンフロー）は，2008 年頃よりスタンフォード大学を中心として開発が進められている次世代ネットワーク制御技術で、一般にはまだあまり知られていないが，インターネットを構成している世界中のネットワーク機器を全て置き換えてしまう程の潜在的インパクトを持っている。

一方、これまで研究代表者のグループは，RSA 公開鍵暗号や AES ブロック暗号などのように計算の難しさに安全性の根拠を置こうとする暗号方式とは一線を画く研究ストリーム、すなわち，情報理論的に安全な暗号プロトコルの研究開発に取り組んできた。情報理論的に安全な暗号方式は、世界中で多くの研究者により長い間研究が進められているが、実用的には様々な理由によりあまり世の中に普及してないのが実状である。

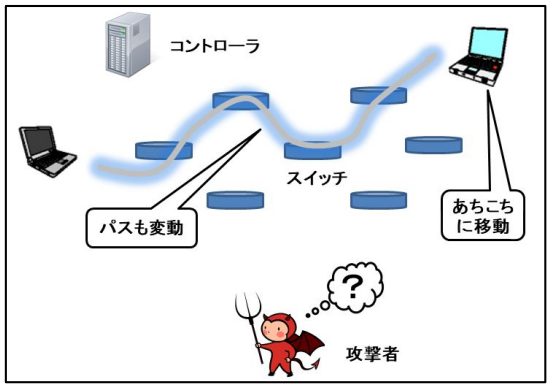
我々研究グループは、OpenFlow がこのような状況を打開する鍵となるのではないか、すなわち、OpenFlow が実ネットワークに普及すれば、情報理論的に安全な暗号が大規模に実装できるのではないかと考え、本研究の着想に至った。

また、本研究は、OpenFlow そのものの安全性を高める研究ではなく、OpenFlow を利用者の立場から活用して、情報通信の安全性を確保しようとする、ユニークな着想である。安全性の担保は計算量ではなく情報理論に基づく。

２．研究の目的

インターネットに代表されるネットワークの世界において，注目されている技術がOpenFlow（オープンフロー）であり、一般社会にはあまり知られていないが、世界中のネットワーク機器を一新するぐらいの潜在能力を十分に持っている。本研究は，研究課題名「オープンフロー時代に適した情報理論的に安全な秘密鍵共有」が示すように、これから OpenFlow の技術が世の中の実ネットワークに普及していくであろうという時期において、その機能・性質を利用者の立場から俯瞰的に眺め、解析し、オープンフロー時代を迎えるからこそ可能になる情報理論的に安全な秘密鍵共有の枠組みやプロトコルを開発し学理追及する。

もう少し具体的には、上図のように，２台の PC を結ぶパス（通信路）をコントローラにより柔軟に作り、しかもそのパスを頻度高く切り替えつつ、PC 自体もユビキタスに移動することにより、攻撃者からその両者を結



ぶパスを秘匿できることが期待できる。これにより、攻撃者が“辿り着けない”通信路、すなわち、「仮想的秘匿通信路」を構成できると考えられる。このような通信路で共有できる秘密鍵の安全性を増幅することを主要な目的としている。

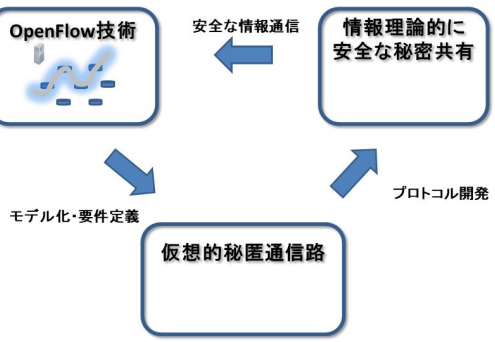
３．研究の方法

本研究を構成する大きな三つの要素は、「OpenFlow 技術」、「仮想的秘匿通信路」および「情報理論的に安全な秘密共有」であり、これらを互いに有機的に結合させることで、従来の安全性とは異なった、新しい視点でのセキュア情報通信技術を開発する。すなわち、OpenFlow 技術を活用することにより仮想的秘匿通信路を創出し、その仮想的秘匿通信路をうまく利用することにより情報理論的に安全な秘密鍵を生成するためのプロトコルを開発し、得られた秘密鍵を用いて安全な情

報通信を OpenFlow 上のネットワーク（インターネット等）で実現する。このような循環サイクルを効果的に回す。

４．研究成果

本研究では、OpenFlow 技術を活用することにより、通信経路を動的に変更可能な公衆ネットワークにおいて、情報理論的に安全な秘密鍵の生成を可能とし、得られた秘密鍵を用いて安全な情報通信を可能とした。本研究課題を実現する上で実施した研究及び得られた要素技術は以下の通りである。



(1)　Open Flow スイッチと Open vSwitch を用い、OpenFlow を利用者の立場から俯瞰し、セキュリティモデルを確立するためのネットワークトポロジについての検討を行った。

(2)　前項で得られたセキュリティモデルに基づき、スーパーコンピュータを使ったシミュレーションを行いつつ、情報理論に基づく安全性評価軸を検討し、その下での秘密鍵共有を行うための基礎知見を与えた。

(3)　秘密鍵の共有状況に関するグラフ理論的モデル化や定式化を行うとともに、上記二つの項目を受けたセキュア通信プロトコルの基礎を開発した。

(4)　Open Flow 上に構築された仮想的秘匿通信路により得られる事前鍵共有グラフが一様漏えい鍵共有完全グラフである場合を想定し、本研究課題の分担者らが開発した st-フロープロトコルをそのような鍵共有グラフに適用した場合、その上で適切な鍵選択を行うための基盤として、盗聴者への漏えい確率の最小値を求める漸化式を示し、具体的に漏えい確率を求めることが可能になるなど効果的な鍵選択を行うための検討を行った。

(5)　既存研究では、漏えい鍵共有グラフが与えられたときに、2 者間で秘密鍵を共有させる問題だけが検討されていたが、ここではこれを一般化し、多人数で共通の秘密鍵を共有する問題に取り組み、それを実現するいつかの効率的なプロトコルを提案した。

(6)　漏えい鍵共有グラフが直並列グラフの場合を扱い、ネットワーク信頼度の問題との関連性を見出し、盗聴者への漏えい確率の最小値を効率的に求める手法を提案した。

(7)　漏えい鍵共有グラフがスプリットグラフのときを検討し、盗聴者への漏えい確率の最小値を効率的に求める手法を提案した。

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）

〔雑誌論文〕（計 2 件）

1. Tatsuya Sasaki, Bateh Mathias Agbor, Shingo Masuda, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Secret Key Amplication from Uniformly Leaked Key Exchange Complete Graph, Algorithms and Computation (WALCOM 2018), Lecture Notes in Computer Science, Springer, vol.10755, pp.20-31, 2018.3 (査読有り).

2. Shoichi Ando, Yuichi Hayashi, Takaaki Mizuki, Hideaki Sone, “Basic Study on the Method for Real-Time Video Streaming with Low Latency and High Bandwidth Efficiency,” COMPSAC WorkShop MidCCI, pp. 79-82, DOI 10.1109/COMPSAC.2015.217, 2015.7 (査読有り).

〔学会発表〕（計 8 件）

1. Bateh Mathias Agbor, Tatsuya Sasaki, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, Multiparty Key Agreement Scheme Using Partially Leaked Key Exchange Graphs, 2018年暗号と情報セキュリティシンポジウム(SCIS2018)予稿集, 2A4-2, 朱鷺メッセ, 2018.1.24.

2. 佐々木達也, 林優一, 水木敬明, 曽根秀昭, 漏えい鍵共有直並列グラフからの鍵生成について, コンピュータセキュリティシンポジウム 2017 論文集, pp.98-105, 山形国際ホテル, 2017.10.23.

3. 佐々木達也, 林優一, 水木敬明, 曽根秀昭, 一様漏えい鍵共有完全二部グラフに関する一考察, 2017 年電子情報通信学会総合大会, 基礎・境界/NOLTA 講演論文集, p.84, 名城大学天白キャンパス, 2017.3.23.

4. 佐々木達也, 林優一, 水木敬明, 曽根秀昭, 漏えい鍵共有グラフから生成される秘密鍵の秘匿性について, 2017 年度夏の LA シンポジウム, pp.15.1-15.9, 山形天童温泉ほほえみの宿滝の湯, 2017.7.20.

5. 増田真吾, 林優一, 水木敬明, 曽根秀昭, 漏えい鍵共有グラフにおける効果的な鍵選択に関する考察,コンピュータセキュリティシンポジウム 2016 (CSS2016)論文集, pp.1276-1283, 札幌コンベンションセンター, 2016.10.13.

6. 安藤翔一, 林優一, 水木敬明, 曽根秀昭, “帯域情報付加パケットによるネットワーク輻輳回避手法の評価,”電子情報通信学会総合大会, B-16-8, p. 496, 2016.3.16.

7. 増田真吾, 林優一, 水木敬明, 曽根秀昭,“一様漏えい鍵共有完全グラフに対する二者鍵共有の限界”電子情報通信学会総合大会, 情報・システムソサイエティ特別企画学生ポスターセッション予稿集, p.131, 2016.3.15.

8. 安藤翔一, 林優一, 水木敬明, 曽根秀昭,“宛先アドレスに基づく複数経路制御による映像配信の利用帯域効率化の実証評価,”電子情報通信学会ソサイエティ大会, B-16-7, p. 332, 2015.9.10.

〔図書〕(計　　件)

〔産業財産権〕

○出願状況(計　　件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況(計　　件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
林　優一(HAYASHI Yuichi)
奈良先端科学技術大学院大学・情報科学研究科・教授
研究者番号：６０５５１９１８

(2)研究分担者
曽根　秀昭　(SONE, Hideaki)
東北大学・サイバーサイエンスセンター・教授
研究者番号：４０１３４０１９

水木　敬明　(MIZUKI, Takaaki)
東北大学・サイバーサイエンスセンター・准教授
研究者番号：９０３２３０８９

(3)連携研究者
(　　)

研究者番号：

(4)研究協力者
(　　)