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

令和　６ 年　 ５ 月 ２２ 日現在

機関番号：１４４０１
研究種目：挑戦的研究（萌芽）
研究期間：2021～2023
課題番号：２１Ｋ１９７７１

研究課題名（和文）プログラマブルスイッチを用いた超高速セキュリティミドルボックス構成法

研究課題名（英文）An Approach to High-speed Security Middleboxes based on Programmable Data Planes

研究代表者
小泉　佑揮（Koizumi, Yuki）

大阪大学・大学院情報科学研究科・准教授

研究者番号：５０５５２０７２

交付決定額（研究期間全体）：（直接経費）　　5,000,000円

研究成果の概要（和文）：本プロジェクトは、プログラマブルスイッチを用いた超高速なミドルボックス実現を目的とし、まず、セキュリティーミドルボックスの核となる暗号技術のスイッチ上での実装法を設計した。ChaChaをスイッチ上で実装し、1 Tbpsを越える暗号処理を達成した。また、完全性を担保するメッセージ認証のスイッチ上での実装法も設計した。これらの成果の集大成として、セキュリティーミドルボックスのプロトコルの例として、軽量匿名通信プロトコルに注目し、それをスイッチ上で実装する方法を提案した。実装したミドルボックスは、1 Tbps以上の速度でパケット転送を実現した。成果の多くはGitHub上でオープンソース化した。

研究成果の学術的意義や社会的意義
学術的意義は、プログラマブルスイッチを用いた暗号・メッセージ認証、および、軽量匿名通信プロトコルの実装を通じて、テラビット級の高速データ転送と高度なセキュリティを両立する新しいアーキテクチャを実証した点にある。社会的意義としては、高速性と安全性を両立する通信が可能になることで、従来は難しかった大容量通信に対するセキュリティーミドルボックスの適用が可能になる点が挙げられる。現在も、これらの技術のTLSやQUICなどの現代的なプロトコルへの応用を目指して研究を継続しており、より広範なネットワーク環境での安全な通信の実現に貢献することが期待される。

研究成果の概要（英文）：This project aimed to develop ultra-high-speed security middleboxes using programmable switches. Initially, we designed implementation methods for ciphers, which is a a core cryptographic technology, on the switches, including the ChaCha algorithm, achieving encryption and decryption processing speeds exceeding 1 Tbps. Additionally, we implemented message authentication on the switches. Highlighting these achievements, we proposed methods for implementing a lightweight anonymous communication protocol on switches as an example of security middlebox protocols. The implemented middleboxes achieved packet transfer speeds over 1 Tbps. Many of the project's results have been open-sourced on GitHub.

研究分野：情報ネットワーク

キーワード：プログラマブルスイッチ　セキュリティー　暗号　匿名通信　P4　Tofino　ChaCha　ミドルボックス

１．研究開始当初の背景

インターネットにおけるセキュリティ上の脅威は深刻化しており、侵入検知機器などのセキュリティミドルボックスの重要性は高まる一方である。しかし、専用の ASIC を備えたセキュリティミドルボックスでも、ルーターやスイッチなどに比べて 2〜3 桁パケット転送速度が遅く、ネットワーク性能のボトルネックとなっている。

２．研究の目的

本プロジェクトの目的は、パケット転送に特化したプログラム可能な ASIC を備えたスイッチ（プログラマブルスイッチ）を用い、100 Gbps 級のセキュリティミドルボックスを開発することである。プログラマブルスイッチは、IP パケット転送に必要なテーブル探索とヘッダ処理をするユニットを連結したパイプライン構成になっている。個々のユニットの処理は単純かつ既存の ASIC よりも処理速度が遅いものの、パイプライン化により Tbps 級の高いパケット処理速度を達成している。セキュリティミドルボックスにはバッファリング処理やハッシュ関数や暗号化処理が必要であり、セキュリティミドルボックスをプログラマブルスイッチ上で実現することを考えたときに、プログラマブルスイッチが、1) パケット転送処理中に動的に読み書きすることができるメモリの容量が小さいこと、2) 算術演算や論理演算などの基本的な演算器しか持たないことの 2 点が大きな制約となる。本課題はこれらの制約をふまえた上で、100 Gbps 級のセキュリティーミドルボックスを開発することである。

３．研究の方法

本プロジェクトでは、上記の目的の達成のため、秘匿性担保のための暗号技術の高速な実装法の設計、完全性担保のためのメッセージ認証の高速な実装法の設計、これらの技術を応用した高度なセキュリティープロトコルをプログラマブルスイッチ上での実装法の設計に取り組んだ。

４．研究成果

本プロジェクトにおける主要な成果は以下の 3 点である。

1. 秘匿性担保のための暗号技術の高速な実装法の設計
2. 完全性担保のためのメッセージ認証の高速な実装法の設計
3. 高度なセキュリティープロトコルのプログラマブルスイッチ上での実装法の設計

4.1 秘匿性担保のための暗号技術の高速な実装法の設計

本プロジェクトでは、暗号的に強度の高いハッシュ（暗号学的なハッシュとは限らない）を用いたワンタイムパッドベースの暗号と、TLS や QUIC などにも用いられるストリーム暗号である ChaCha をプログラマブルスイッチ上で実装した。ワンタイムパッドベースの暗号については、暗号プロトコルの実装とともに説明し、本章では、ChaCha の実装法を議論する。ChaCha は、高速かつセキュアなストリーム暗号であり、AES に代わる選択肢として注目されている。しかし、ChaCha をハードウェアで実装する際には、計算の効率化と依存関係の管理が課題となる。本研究では、プログラマブルスイッチ上での ChaCha の実装方法を提案し、その性能評価を行う。

4.1.1 ChaCha 暗号の概要

ChaCha 暗号は、ストリーム暗号であり、高いセキュリティと高速な計算性能を持つ。ChaCha の主な特徴は、以下の通りである：

- 軽量な計算：加算、XOR、ビットシフトといった基本的な操作のみを使用
- 高いセキュリティ： TLS や QUIC などのプロトコルの標準で使用可能
- 優れたパフォーマンス：ソフトウェアおよびハードウェアでの効率的な実装が可能

ChaCha は、20 ラウンドの変換プロセスを通じて平文を暗号化する。各ラウンドは、Quarter Round（QR）と呼ばれる 4 つの操作から構成される。QR は、4 つの 32 ビットワードに対して加算、XOR、ビットシフトを適用する。

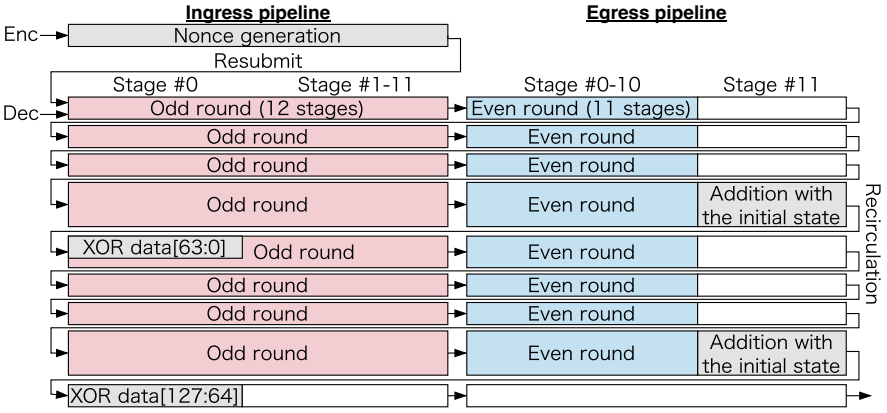
ChaCha は、以下の利点を持つ：

- 高いセキュリティ：従来の暗号方式に比べて、鍵長と初期化ベクトル（IV）の組み合わせによるセキュリティが強化されている。

- 高速な計算：軽量な計算により、ソフトウェアおよびハードウェアで高速に動作する。
- 柔軟な実装：プログラマブルスイッチのパイプラインアーキテクチャに適している。

4.1.2 実装

本研究では、Intel Tofino 2 プログラマブルスイッチを用いて ChaCha 暗号を実装した。以下に、実装の主要な技術的課題とその解決方法を示す。

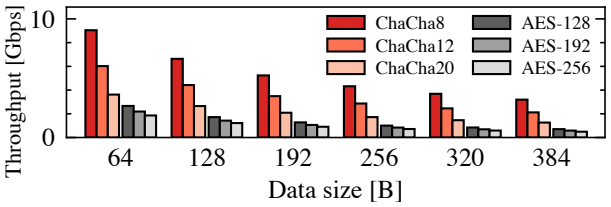


内部状態の依存関係の管理：ChaCha の実装において、QR の計算を効率的に行うためには、内部状態の依存関係を適切に管理する必要がある。本研究では、奇数・偶数ラウンドの QR 操作を分離し、パイプライン上で効率的に配置する。これにより、計算の依存関係を最小限に抑え、並列処理を最大限に活用することができる。

パイプラインステージの最適化：QR 内の演算を効率化するために、パイプラインステージの最適化を行う。具体的には、ローテート演算と加算を 1 ステージで行う特殊な命令を用いることで、全体のステージ数を削減する。これにより、暗号化・復号処理を迅速に行うことができる。

ブロック間の依存関係の解消：ChaCha 暗号では、複数のデータブロックを並行して処理することが可能である。各ブロック間の依存関係を解消するために、データブロックをリングバッファとして扱い、パイプライン上での複数ブロックへのアクセスを効率化する。このアプローチにより、各ブロック間の依存関係を排除し、全体の処理速度を向上させることができる。

4.1.3 評価



本研究の設計に基づき、ChaCha 暗号をプログラマブルスイッチ上に実装し、その性能評価を行った。評価により、ChaCha8、ChaCha12、および ChaCha20 の各実装が、AES-128、AES-192、および AES-256 と比較して 4 倍以上の高速化を達成することを示した。また、ChaCha は最大 203.1 Gbps のスループットを達成することを示した。未発表であるため詳細は割愛するが、計算方法を最適化することで、1 Tbps 以上の計算速度を達成できることを示した。

4.2 完全性担保のためのメッセージ認証の高速な実装法の設計

本研究では、ネットワーク層で匿名通信を実現し、低レイテンシーと高スループットを実現する軽量匿名通信プロトコルを対象とし、さらなる高速化を図った。具体的には軽量匿名通信プロコトルとして、PHI（Path-Hidden Lightweight Anonymity Protocol）を対象とした。これは、単一の攻撃者を想定し、ヘッダ上の経路情報を秘匿するプロトコルである。本研究では、PHI をプログラマブルスイッチ上で実装することで、従来の実装よりも高速な 1 Tbps 以上の通信を達成した。

この実装法については、4.2 章で経路情報の完全性を担保するメッセージ認証の実装を中心に説明し、4.3 章でプロトコル全体のプログラマブルスイッチ上での実装を説明する。

4.2.1 プロトコルの設計

本研究では、転送情報に対する暗号化と認証をするプロトコルを設計した。以下に、プロトコルの詳細を説明する。

経路確立フェーズ：経路確立フェーズでは、データパケットの転送に先立ってルータによる経路の確立が行われる。ルータは経路表を用いて経路を決定し、前後のルータの IP アドレスを暗号化し、認証コードを付加した転送情報を作成する。これにより、データ転送フェーズにおいて各ルータが自身が作成した転送情報を利用してパケットを転送することができる。

データ転送フェーズ：データ転送フェーズでは、経路確立フェーズで作成された転送情報を用いてデータパケットを送信する。各ルータはパケットのヘッダから転送情報を取り出し、復号と

認証コードの検証を行う。これにより、転送情報の完全性が保証され、経路上での改ざんを防ぐことができる。

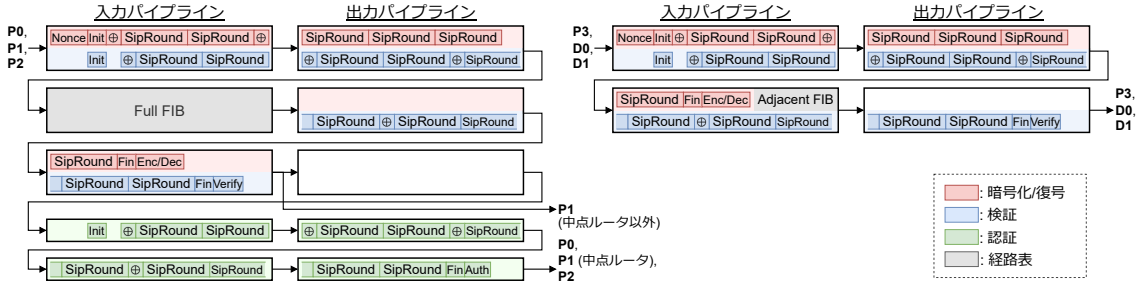
4.2.2 実装

本研究では、Intel Tofino 2 プログラマブルスイッチを用いてプロトコルを実装した。以下に、実装の主要な技術的課題とその解決方法を示す。

暗号化方式の選択：転送情報の暗号化と認証には、Tofino 2 スイッチの命令セットによる効率的な計算が可能である鍵付きハッシュ関数として HalfSipHash を用いている。このハッシュ関数は、軽量でありながら暗号学的に安全な特性を持っている。暗号化では、擬似乱数生成器により生成されたノンスの鍵付きハッシュ値を計算し、これをワンタイムパッドとして用いる。認証では、転送情報を HalfSipHash に入力することで鍵付きハッシュ値を計算し、メッセージ認証コード（MAC）として利用する。

パイプライン上でのレイアウト：認証付き暗号の実装には、MAC-then-Encrypt（MtE）と Encrypt-then-MAC（EtM）の二種類の方針が考えられるが、本研究ではセキュリティとパフォーマンスの観点から EtM を採用している。EtM では、暗号化時にメッセージ認証コードを生成し、復号時にこれを検証する。これにより、暗号化と認証を並行して行うことができ、パイプライン処理の効率が向上する。

HalfSipHash の演算はスイッチ 2 周分の計算量を要するため、パケットは経路確立フェーズとデータ転送フェーズにおいてそれぞれスイッチを 4 周、2 周して処理を受ける。これにより、達成可能な最大スループットは 6.37 Tbps となる。



4.2.3 評価

上記の設計に基づき、プロトタイプ実装し、実際のプログラマブルスイッチを用いて評価した。

スループットの評価：実験により、3.0 Tbps のスループットを達成し、高速なデータ転送と転送情報の暗号化・認証が実現可能であることを示した。このスループットは、プログラマブルスイッチのパイプライン処理能力と最適化された暗号処理により達成されたものである。特に、HalfSipHash を用いた効率的なハッシュ計算と EtM 方式の採用が、スループットの向上に寄与している。

レイテンシの評価：パケット処理のレイテンシについても評価を行った。結果として、暗号化と認証に要する時間は、プログラマブルスイッチのパイプラインステージ数に依存しており、全体のレイテンシは非常に低い値に抑えられている。これにより、高速なデータ転送と転送情報の完全性を両立させることができる。

セキュリティの評価：セキュリティ評価では、選択暗号文攻撃や経路接合攻撃に対する耐性を確認した。

4.3 高度なセキュリティープロトコルのプログラマブルスイッチ上での実装法の設計

本章では、4.2 章で説明した PHI のプロトコル全体の実装について説明する。

4.3.1 プロトコルの設計

本研究では、PHI を基盤にした軽量匿名通信プロトコルを採用している。PHI は、パケットのヘッダに経路情報を暗号化して格納することで、通信経路上のノードから送信元と宛先の情報を隠蔽することを目的としている。これにより、攻撃者が通信経路上の複数のノードを監視しても、送信者と受信者の関係を特定することが難しくなる。

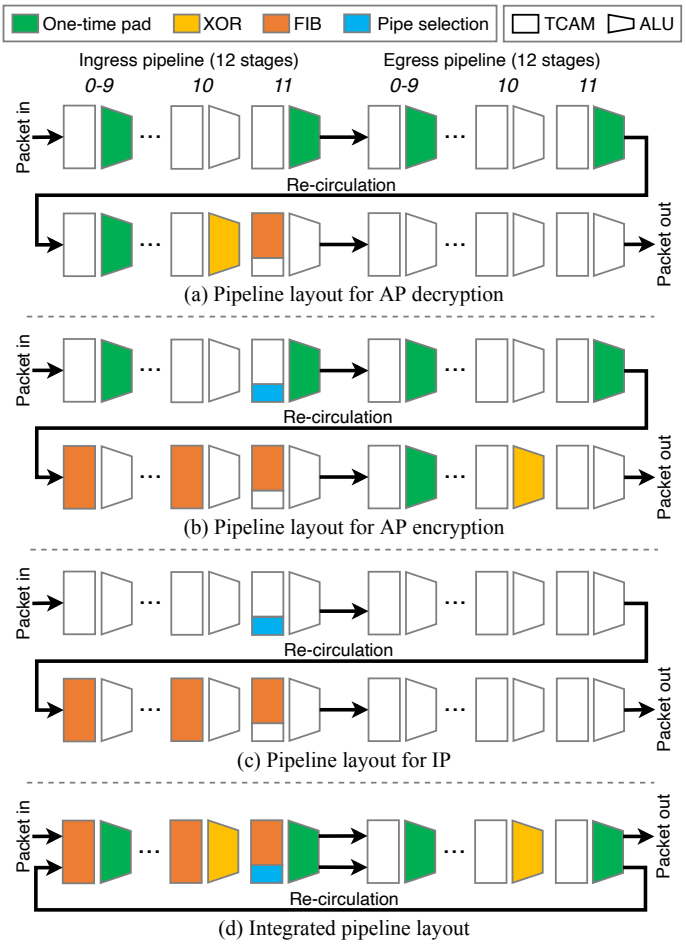
経路設定フェーズ：経路設定フェーズでは、送信者は受信者の IP アドレスを含む経路設定パケットを送信する。このパケットは、経路上の各ルータによって処理され、前後のルータの IP

アドレスを暗号化した経路情報がパケットヘッダに追加される。各ルータは、自身の秘密鍵を用いて経路情報を暗号化し、次のルータに転送する。最終的に、受信者に到達したパケットには、経路上のすべてのルータが作成した経路情報が含まれている。

データ転送フェーズ：データ転送フェーズでは、経路設定フェーズで作成された経路情報リストを用いてデータパケットを送信する。各ルータはパケットを受信すると、ヘッダから経路情報を取り出し、次のルータの IP アドレスを復号する。このプロセスにより、パケットは匿名化された経路を経由して受信者に届く。

4.3.2 実装

本研究では、Intel Tofino 2 プログラマブルスイッチを用いてプロトコルを実装した。プログラマブルスイッチは、高速なパケット処理能力と柔軟なプログラマビリティを兼ね備えており、本研究の目的に非常に適している。以下に、実装の主要な技術的課題とその解決方法を示す。



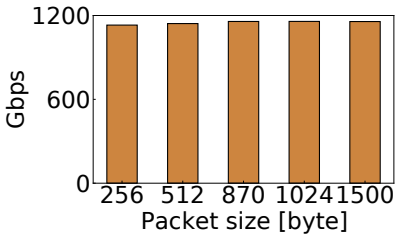
暗号化方式の選択：PHI プロトコルでは、送信元と宛先のルータアドレスを暗号化するために、鍵付き擬似乱数関数を用いたワンタイムパッド方式を採用している。この方式は、計算が軽量であり、プログラマブルスイッチのパイプライン処理に適している。具体的には、暗号化と復号の際に、秘密鍵とノンスを入力として擬似乱数を生成し、これをパッドとして使用する。パケットヘッダには、暗号化された経路情報とノンスが含まれる。

データ構造の工夫：経路情報の保持と管理には、リングバッファを用いることで動的なインデックス参照を避け、処理効率を向上させている。リングバッファを回転させることで、常に最初のスロットを参照し、次のスロットを使用する際にはパーサによる回転操作を行う。このアプローチにより、プログラマブルスイッチの計算資源を効率的に利用できる。

パイプラインの最適化：プログラマブルスイッチのパイプライン上での暗号処理を効率的に配置し、リサーキュレーションの回数を最小限に抑えることで、スループットを最大化している。具体的には、データ転送フェーズにおいて、ネクストホップの IP アドレスを決定するための暗号化・復号処理を 10 ステージ目に配置し、その後の FIB ルックアップを 11 ステージ目で行うように設計している。これにより、パケット処理の並列性を最大限に活用し、高速なデータ転送を実現している。

4.3.3 評価

本研究の設計に基づき、プロトタイプを実装し、実際のプログラマブルスイッチを用いた実験を行った。以下に評価結果を示す。



スループット：実験により、1.16 Tbps のスループットを達成し、テラビット級の匿名通信が実現可能であることを示した。このスループットは、プログラマブルスイッチのパイプライン処理能力と最適化されたデータ構造により達成されたものである。特に、リングバッファを用いた経路情報の管理と、ワンタイムパッド方式による暗号化・復号処理が、スループットの向上に寄与している。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計8件（うち招待講演　1件／うち国際学会　3件）

１．発表者名 北 健太朗，武政 淳二，小泉 佑揮，長谷川 亨
２．発表標題 コンプロマイズされたミドルボックスに耐性を持つセキュア通信プロトコルに関する一考察
３．学会等名 コンピュータセキュリティシンポジウム2022
４．発表年 2022年

１．発表者名 Yutaro Yoshinaka, Junji Takemasa, Yuki Koizumi, Toru Hasegawa
２．発表標題 On implementing ChaCha on a programmable switch
３．学会等名 International Workshop on P4 in Europe（国際学会）
４．発表年 2022年

１．発表者名 吉仲 佑太郎，河内山 深央，武政 淳二，小泉 佑揮，長谷川 亨
２．発表標題 プログラマブルスイッチ上の転送情報の暗号化と認証法の設計
３．学会等名 電子情報通信学会研究総合大会
４．発表年 2023年

１．発表者名 Shunsuke Higuchi, Yuki Koizumi, Junji Takemasa, Atsushi Tagami, Toru Hasegawa
２．発表標題 Learned FIB: Fast IP Forwarding without Longest Prefix Matching
３．学会等名 IEEE International Conference on Network Protocols（国際学会）
４．発表年 2021年

１．発表者名
Yutaro Yoshinaka, Junji Takemasa, Yuki Koizumi, Toru Hasegawa

２．発表標題
Feasibility of Network-layer Anonymity Protocols at Terabit Speeds using a Programmable Switch

３．学会等名
IEEE International Conference on Network Softwarization（国際学会）

４．発表年
2022年

１．発表者名
樋口 俊介，武政 淳二，小泉 佑揮，田上 敦士，長谷川 亨

２．発表標題
区分線形近似を応用した学習型インデックスの高速化とIP FIBへの応用

３．学会等名
電子情報通信学会技術研究報告

４．発表年
2021年

１．発表者名
小泉 佑揮，樋口 俊介，武政 淳二，田上 敦士，長谷川 亨

２．発表標題
学習型インデックス構造のIP FIBへの応用

３．学会等名
電子情報通信学会技術研究報告（招待講演）

４．発表年
2021年

１．発表者名
吉仲 佑太郎，小泉 佑揮，武政 淳二，長谷川 亨

２．発表標題
プログラマブルスイッチ上でのストリーム暗号に基づく暗号化・復号法の実装

３．学会等名
電子情報通信学会ソサイエティ大会

４．発表年
2023年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

ChaCha implementation on Tofino switches https://github.com/Hasegawa-Laboratory/ChaCha-Tofino

6．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関