2009-IOT-4（1）
2009 / 3 / 5

ストリーム暗号を用いたパケット中継装置の実装評価

竹内 清史† 辻村 達徳†

†三菱電機株式会社 情報技術総合研究所 〒247-8501 神奈川県鎌倉市大船 5-1-1

E-mail: †Takeuchi.Kiyofumi@bp.MitsubishiElectric.co.jp, Tsujimura.Tatsunori@da.MitsubishiElectric.co.jp

あらまし ストリーム暗号は、その暗号化方式の特性上、大量のデータを一括して暗復号するのに適しており、パケット単位で暗復号することとなるパケット中継装置への適用は一般的に困難である。この問題を解決するにあたり、我々はパケット処理ごとに暗復号処理部の内部状態を一時的にメモリ等に保持するストリーム暗号の実装方式を考案し、実際にこの方式をパケット中継装置の H/W（FPGA）に実装して性能評価を行った。その結果、平文パケット長が 128Byte 以上の暗号通信において 1Gbps のスループットを達成することを確認した。

キーワード ストリーム暗号，暗号通信，VPN

Implementation and Evaluation of Packet Processing with Stream Encryption

Kiyofumi TAKEUCHI† Tatsunori TSUJIMURA†

† Information Techonology R&D Center, Mitsubishi Electric Corporation
5-1-1 Ofuna, Kamakura, Kanagawa, 247-8501 Japan

E-mail: †Takeuchi.Kiyofumi@bp.MitsubishiElectric.co.jp, Tsujimura.Tatsunori@da.MitsubishiElectric.co.jp

Abstract It is difficult to apply stream encryption to communication devices because of that's encryption method. But we considered a new implementation method to clear the problem. Then we implemented it to communication devices, and evaluated it. On the throughput test, we achieved 1Gbps when the plain text packet length was over 128 bytes.

Keyword Stream Encryption, Encrypt Communication, Virtual Private Network

1. はじめに

共通鍵を用いた暗号化方式は、ブロック暗号とストリーム暗号に大別される。ブロック暗号は一定のブロックサイズ（64, 128bit が一般的）単位で暗号化するのに対し、ストリーム暗号は 1bit あるいは 1Byte 単位で暗号化する。

ネットワーク上のパケットをルータ等の中継装置で暗号化する方式としては、ブロック暗号を用いた IPsec が知られている。しかしブロック暗号はブロックサイズを一致させるためのパディングが必要なため、暗号化データが平文データより大きくなってしまう。一方でストリーム暗号は、基本的にパディングが不要なため伝送効率が高いといった利点がある。

本稿では、パケット中継装置へのストリーム暗号の適用可能性を検討した結果、および検討した方式を実装して評価した結果を報告する。

2. ストリーム暗号の構成と制御

ストリーム暗号を用いた一般的な暗号通信の概念図を図 1 に示す。暗号化側では、秘密鍵と初期ベクトル IV から鍵系列を生成し、生成した鍵系列と平文を XOR（排他的論理和）することで暗号文を生成して送信する。復号側においても同様に、共有している秘密鍵と IV を元に鍵系列を生成し、これを暗号文と XOR することで平文を得る。また、秘密鍵を定期的に更新することでセキュリティを維持する。

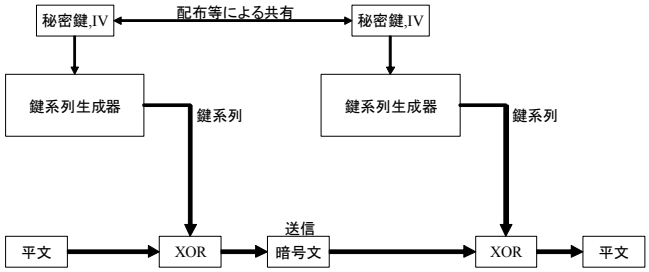

図 1. ストリーム暗号通信イメージ

図 1 における鍵系列生成器の一般的な内部の構成を図 2 に示す。ここでは秘密鍵と IV を入力として鍵系列を生成するにあたり、攪拌関数を繰り返し使用する。この攪拌関数 1 回の処理をラウンド処理と呼び、各ラウンドの入力となる中間データを中間鍵と呼ぶ。

ストリーム暗号におけるセキュリティの強度は、鍵系列生成器で生成される鍵系列の乱数性に依存する。

このため秘密鍵と IV の入力直後には初期攪拌と呼ばれる長時間の攪拌を行い、以降で生成する鍵系列に十分な強度を持たせている。初期攪拌実行後は高スループットで鍵系列の生成が可能なため、ストリーム暗号は莫大なデータ量を一括して暗号化するといった用途に適している。

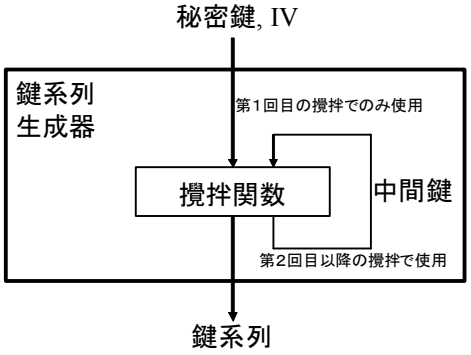

図 2．鍵系列生成器の内部構成

3. ストリーム暗号によるパケット中継と問題

3.1. 一般的な実装方式(その1)

ネットワークの中継装置間でストリーム暗号によってパケットを暗号化することを考える。ここでは秘密鍵と IV は暗号通信開始前に装置間で共有できているものとする。

最も単純な実装方式として、パケットごとに秘密鍵と IV を入力し初期攪拌を行う方法が考えられる（図３）。

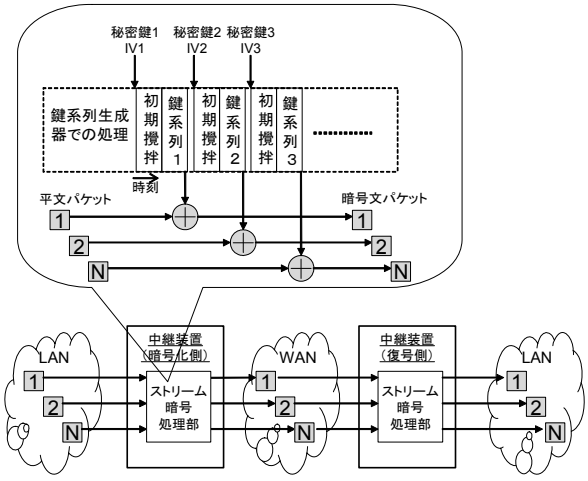

図 3．ストリーム暗号の一般的な実装方式（その１）

暗号化側の中継装置は、平文パケットを受信後、秘密鍵と IV を鍵系列生成器に入力し、初期攪拌行って暗号化に必要なサイズの鍵系列を生成する。以降のパケットについても同様、１パケットごとに初期攪拌を行って鍵系列を生成するが、初期攪拌の時間が長く通信速度が期待できない。また、この方法ではパケット１個ごとに秘密鍵と IV を消費するため、事前に大量の秘密鍵と IV を準備しなければならないといった問題がある。

3.2. 一般的な実装方式(その2)

次に、同一の秘密鍵と IV で生成した単一の鍵系列で複数パケットを順に暗号化する方法を考える（図 4)。

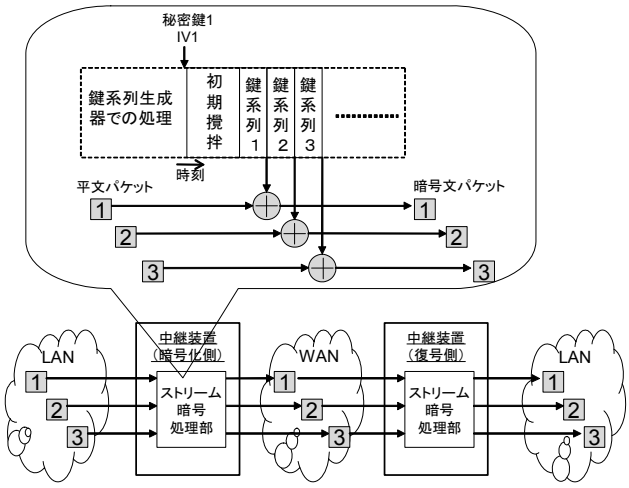

図 4．ストリーム暗号の一般的な実装方式（その２）

この場合、暗号通信開始前に初期攪拌を実行しておくことで遅延は回避できるが、以下の問題がある。

第一に、セキュリティ強度の観点から中継装置ごと等で異なる鍵と IV で生成した複数の鍵系列でパケットを逐次暗号化できることが望ましいが、このためには装置内に鍵系列と同数の鍵系列生成器を有し、各々が常々の中間鍵を維持して乱数を即時生成可能な状態を保つ必要がある。これは実装効率が悪く現実的でない（図 5)。

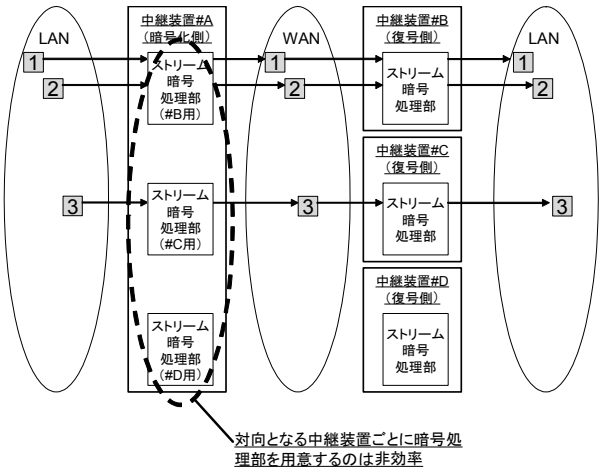

図 5．単一の鍵系列で通信する方式の問題点１

第二に、パケットをネットワークで転送している最

中に、何らかの原因で暗号化側と復号側でパケットの到着順序が入れ替わる、あるいはパケットが消失する可能性がある。この場合、復号側では鍵系列を取り出す位置がずれてしまう（図 6）。これを防ぐには復号側の鍵系列生成器が鍵系列の生成順序を入れ替える必要があるが、中間鍵を一度攪拌して遷移させてしまうと以前の状態に戻すことが困難である。

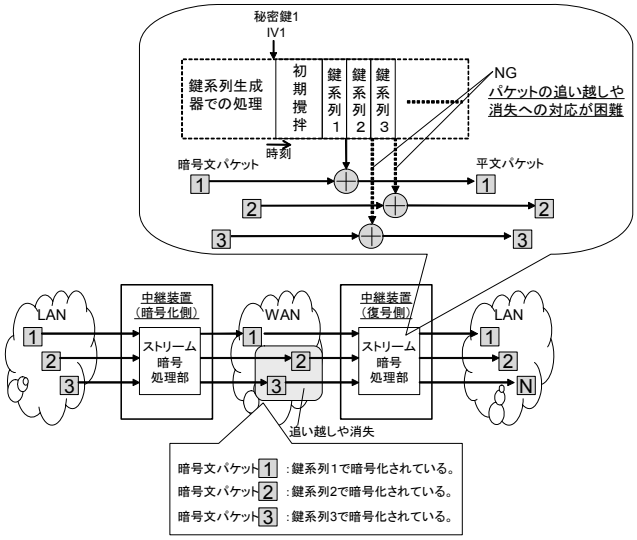

図 6. 単一の鍵系列で通信する方式の問題点 2

4. 新方式の提案

先に述べた一般的な実装方式（その 2）の課題を解決する方式として、中間鍵の入出力が可能な鍵系列生成器を考える。

初期攪拌後、もしくは各パケットで必要な鍵系列を生成した後で、鍵系列生成器から中間鍵を出力してメモリに保存する。その後、同系の鍵系列が必要なときは、メモリから中間鍵を読み出し、これを鍵系列生成器に入力することで必要な鍵系列を短時間で得られる。これにより、異なる鍵と IV で生成した複数の鍵系列でパケットを逐次暗号化できるため、第一の課題を解決することができる。

また、同一の中継装置間でも複数の鍵系列を使用する方式を考える。鍵系列が異なる場合は、復号の順序に制限がなくなるため、一定時間に到着順序が逆転し得るパケットの個数で鍵系列を多重化することで第二の課題も解決することが可能となる。提案方式における復号時の動作イメージを図 7 に示す。

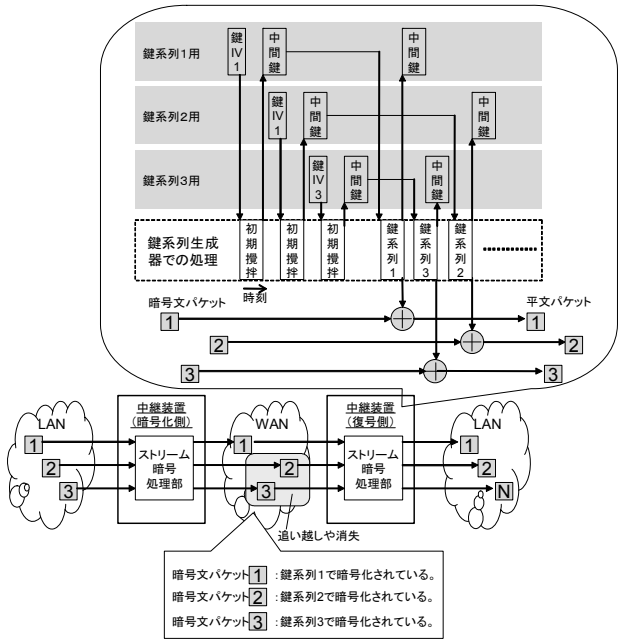

図 7. 提案方式の復号イメージ

5. 提案方式の実装と評価

5.1. IPsec の適用

中継装置間でストリーム暗号通信を行うにあたっては IPsec を適用した。一般的に IPsec ではブロック暗号を用いることが多いが、ストリーム暗号を適用することも可能である。なお、暗号側から復号側へは鍵系列の ID を通知する必要があり、それには ESP ヘッダの IV フィールドを利用することとした。

5.2. 実装対象 H/W

提案方式は FPGA で実装した。FPGA を含む中継装置全体の構成を図 8 に示す。

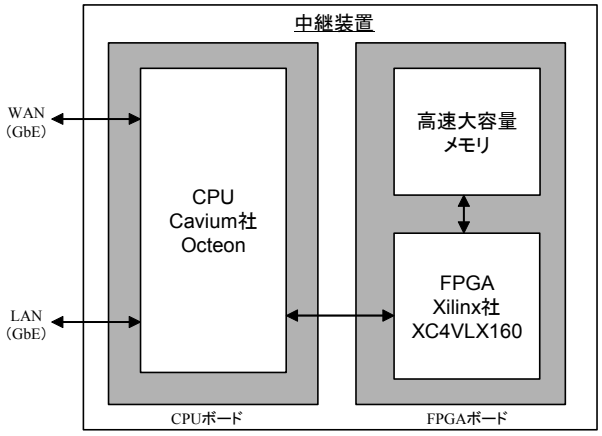

図 8. パケット中継装置の内部構成

CPU ボードには Cavium 社のマルチコア CPU Octeon を、FPGA ボードには Xilinx 社の FPGA を搭載してい

る。CPU ボードは、LAN/WAN のパケット送受信制御、パケットの IPsec エンカプセル／デカプセル処理、FPGA ボードとのパケット送受信制御を主に行う。FPGA ボードは、CPU ボードから受信したパケットに対してストリーム暗号処理を行い、暗号／復号後のパケットを CPU ボードに送信する。

5.3. 目標性能

我々は、提案方式を実装する上で目標性能を 1Gbps に定めた。1Gbps を実現する対象の平文パケットサイズは、鍵系列生成器の性能とパケット単位で鍵系列生成部に入出力する中間鍵のサイズを考慮して 128～1452Byte とした。

今回の提案方式では、1 パケットごとに固定サイズの中間鍵を鍵系列生成器に入出力する。この処理は暗号化対象のパケットサイズに依存しないため、同じ 1Gbps であっても測定対象となるパケットのサイズが小さいほど 1 パケットあたりに許容される処理(転送)時間が短く性能の達成が困難となる。なお、パケット長の上限に設定した 1452Byte は、IPsec エンカプセル後のパケット長が 1518Byte で、IP フラグメントが発生しない最大長である。

続いて、ネットワークの持つ最大通信速度ワイヤスピードについて定義する。暗号通信性能 1Gbps のワイヤスピードを単位時間あたりの転送パケット数 pps（Packet Per Second）で表す。例えば、平文パケット長 128Byte に ESP ヘッダや認証データ等を加えた IPsec パケット 194Byte のワイヤスピードは 584,112pps となる。

6. 実装評価

6.1. 評価方法

スループット測定時のシステム構成を図 9 に示す。試験用パケットの生成と測定には Smartbits を使用した。Smartbits により特定長の IP パケットを 1Gbps のワイヤレートで連続して生成する。それを中継装置#1 に入力し暗号化して出力し、対向の中継装置#2 で復号する。このとき、図 9 中の(A)におけるパケット数を Smartbit で測定した。

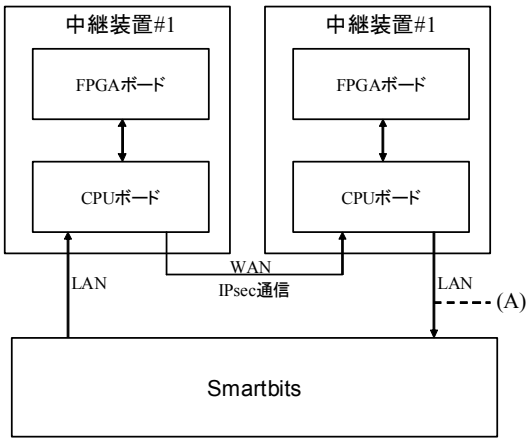

図 9. 評価環境のシステム構成

6.2. 測定結果

性能評価の測定結果を図 10 に示す。横軸が平文パケット長、縦軸が単位時間あたりのパケット数 pps を示している。

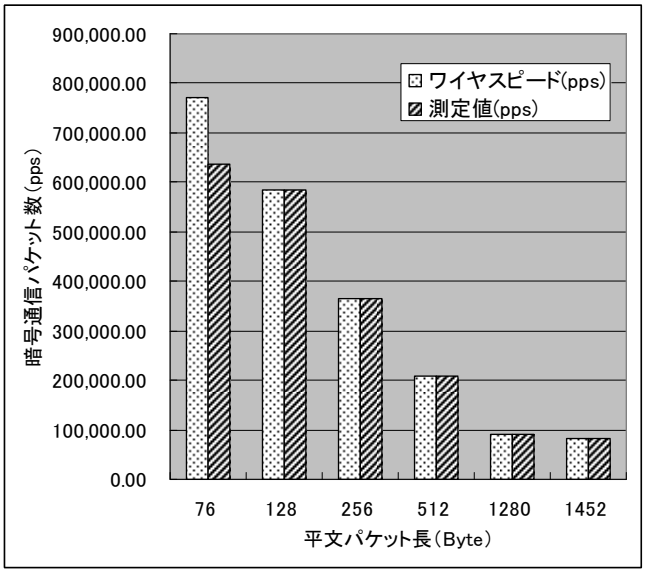

図 10. 性能測定結果

目標としていた平文パケット長 128Byte 以上では、ワイヤスピードと同じパケット数で暗号通信しており、1Gbps のスループットを達成していることが分かる。また、測定した最小の平文パケット長 76Byte 時（Smartbits で設定可能な IPv6 通信での最小パケットサイズ）の性能は、通信スループットに換算すると約 827Mbps となる。

7. まとめ

一般的にパケット中継装置への適用が困難なストリーム暗号について実装方式を提案し、FPGA に実装

して実機での評価を行った。結果、今回の実装では、パケット長が128Byte以上であるときに1 Gbpsのスループットを達成可能であることが分かった。

今後は、更に短いパケット長での達成に向けて検討を進めていく予定である。また、現状は実機でパケット到着順序を変化させたときや、パケットロスを発生させたときのスループット測定は実施できていないため、今後の課題とする。

8. 参考文献

[1] 小貫淳史，竹内清史，稲田徹，“ストリーム暗号を用いたパケット中継装置の検討”，信学全会，Mar.2008

[2] 辻村達徳，竹内清史，“マルチコア CPU によるIPsec の実装検討”，インターネットアーキテクチャ研究会，Mar.2009

[3] 馬場達也 著、「マスタリング IPsec 第 2 版」、株式会社オライリー・ジャパン（2006）