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　２ 年　 ６ 月　 ５ 日現在

機関番号：１２６０１
研究種目：基盤研究(A)（一般）
研究期間：2016～2018
課題番号：１６Ｈ０１７１４

研究課題名（和文）秘匿性・改竄耐性のある超高速データ通信システムの研究

研究課題名（英文）Study on very high-speed data communications with secret and secure capability

研究代表者
平木　敬（Hiraki, Kei）

東京大学・大学院情報理工学系研究科・名誉教授

研究者番号：２０２３８３４８

交付決定額（研究期間全体）：（直接経費）　　33,730,000円

研究成果の概要（和文）：本研究では秘匿性・耐改竄性を持つ超高速データ転送システムを開発した。
（１）一対の小型サーバに各々8個のSSDを実装し、SSD間で96Gbpsを超える転送速度でローカルなデータ転送を実現し確認した。秘匿性・耐改竄性については、原データを自動分割し暗号化アクセラレータを用いることなく、ローカルな接続環境で90Gbpsを超える秘匿性・耐改竄性通信を実現した。
（２）超遠距離インターネットを用いた実証実験では、米国デンバー市からシンガポールで折り返し、再びデンバー市に戻る経路を往復する経路で86Gbpsの秘匿性・耐改竄性を持つ通信を実現した。

研究成果の学術的意義や社会的意義
超高速な秘匿性・耐改竄性をもつ通信の重要性は、最近特に高まりつつある。学術的には、少数のTCPストリームを調和的に用い、20000Kmを超える超遠距離における、暗号化、復号化、ハッシュ計算を伴うデータ転送を1台の小型サーバで実現することは非常に困難であることが知られている。本研究ではこの難しい問題を解決した。これは非常に大きな学術的意義がある。また実際に医療機関にいくことなく細胞分析を行う、遺伝子解析を行うと高い秘匿性・耐改竄性を持つ通信が必須となる。新型コロナウィルス感染の広がりはまさに我々が予想した応用形態に合致するものであり、大きな学術的意義、社会的意義を持つといえる。

研究成果の概要（英文）：In this research, we developed an ultra-high-speed data transfer system with confidentiality and tamper resistance.
(1) Eight SSDs were mounted on each of a pair of small servers, and local data transfer was realized between SSDs at a transfer rate of over 96Gbps. Regarding confidentiality and tampering resistance, we have achieved confidentiality and tampering resistance over 90 Gbps in a local connection environment without automatically dividing the original data and using an encryption accelerator.
(2) In a demonstration experiment using the ultra-long distance Internet, we realized communications with 86 Gbps confidentiality and tamper resistance by a route that returned from Denver city in the United States to Singapore and returned to Denver city again.

研究分野：超高速通信、通信システムアーキテクチャ

キーワード：超高速通信　耐改竄性　情報秘匿　100ギガビットネットワーク　超高速暗号化　超高速改竄検出

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

高性能コンピューティングを行う研究者にとって大学や研究機関の間の高速データ転送は常に重要な課題である。実験データが生成される拠点とデータを解析する拠点は地理的に離れていることも多く、国際的な共同研究も広く行われている。われわれの研究グループ Data Reservoir プロジェクトでは以前より高速ネットワーク基盤を高い効率で活用する研究を続けてきた。

長距離ネットワークでのデータ転送を利用するアプリケーションは徐々に変化してきている。研究拠点間のデータ転送では物理の実験データや天文の観測データの転送に利用されていた。それ以外にも大容量の動画や画像データの転送も利用の対象であった。最近ではそれらの利用に加えて、研究拠点間のデータ転送では DNA などの生体情報や医療データなども対象となっている。さらに、多数の IoT 機器で収集されるセンサデータなど個人情報を含むビッグデータにも対象が広がっている。このような用途では個人情報保護や生命倫理を考慮する必要があり、データ転送の暗号化が必要不可欠である。

２．研究の目的

100 Gbps ネットワークでのストレージ間暗号化データ転送で高い性能を実現するための課題は、暗号化処理の負荷、複数ファイルの処理を含むストレージ処理、100 Gbps 環境での TCP の安定性である。これらの問題を解決するために、われわれは暗号化データ転送ソフトウェアである Secure Data Reservoir を開発した。

高エネルギー物理などでは以前より大量のデータを扱っており高速データ転送の需要があった。古典的なデータ転送の手法としては ftp や scp があり現在でも広く利用されているが、ftp には性能の問題、セキュリティの問題、ポート管理の問題などが存在する。

本研究では暗号化処理自体は Intel AES-NI のアクセラレーションを活用し、ストリームの並列性で性能の向上を図っている。

３．研究の方法

われわれの研究グループでは本研究の目標を実現するために暗号化ファイル転送ツール Secure Data Reservoir を開発した。本ツールは一般的な Linux サーバで動作し、ストレージ上にある複数のファイルを暗号化データ転送する機能を備え、長距離 100 Gbps ネットワーク上でのシングルサーバ間の暗号化データ転送で高い性能を実現するものである。

Secure Data Reservoir の構成では、高速ネットワークで接続された各拠点にシングルサーバで構成される Secure Data Reservoir を設置し、拠点間で暗号化データ転送を行う利用形態となる。サーバは一般的な Linux サーバで、高い性能を実現するためにハードウェア構成としては RAID 構成の SSD によるストレージと 100 Gbps のネットワークインターフェイスカードを搭載している。

長距離ネットワーク上で高い効率でネットワークを利用するためには TCP の振る舞いを安定させることが特に重要となる。われわれの研究グループでは以前よりこの点に着目しており、ペーシング技術で TCP 送信を制御することで安定した転送を実現している。さらに超長距離のネットワークの場合には標準の TCP のウインドウ制御の限界を超えるために性能が制限されてしまうが、そのような状況においてはわれわれの開発した LFTCP プロトコルを組み合わせることで制限を回避することが可能である。

４．研究成果

Secure Data Reservoir の基本的な暗号化データ性能を評価するために、100 Gbps スイッチにサーバを直結したローカル環境で転送実験を行い、従来手法と性能を比較する。転送するデータはインターネット上で公開されている衛星画像データおよびゲノムデータを仮想的な実験データとして使用した。ファイルサイズが数 10 バイトから 1 GB 程度までの平均 20 MB のファイル約 10 万個からなる合計 2 TB のファイルデータである。

性能評価としては、合計ファイルサイズを全てのファイルを送信し終わるまでの時間で割った平均性能を測定した。比較対象とする手法は、暗号化データ転送を行う古典的な手法である scp、および現在広く用いられている手法である GridFTP とした。本研究ではデータの暗号化は本質的であるため暗号化機能を備えていない手法は比較の対象としていない。

測定結果は図 1 の通りである。GridFTP および Secure Data Reservoir については並列度を 2 のべき乗で増加させながら測定し、性能が飽和した並列度のものを測定結果とした。GridFTP については 16 並列の場合の値であり、Secure Data Reservoir については 8 並列の場合の値となっている。今回の評価では手動で並列度を指定して測定しているが、この結果は実験に使用したサーバのコア数が合計 16 コアであることから導き出せる値であり自動

的に設定することも可能である。Secure Data Reservoir についてはディスクの読み書きとネットワークの送受信でそれぞれ専用のスレッドを用いているため 8 並列 16 スレッドの状態で性能が飽和している。Scp については単一のジョブを並列に転送する機能を備えていないが、参考性能として手動でジョブを分割して並列に転送を行った場合の性能を併記した。

この評価結果から Secure Data Reservoir は複数ファイルのストレージ間転送という実用的な条件において 100 Gbps ネットワークを高い効率で活用する 84.9 Gbps という基本性能が達成できることが確認できた。また、その性能は同じ環境で古典的なツールである scp が達成する性能よりも 10 倍以上高く、広く用いられている GridFTP と比較しても 1.5 倍以上の性能が達成できることが確認できており、個人情報保護や生命倫理への対応に必要となる暗号化データ転送への注力は重要であることが実証できた。

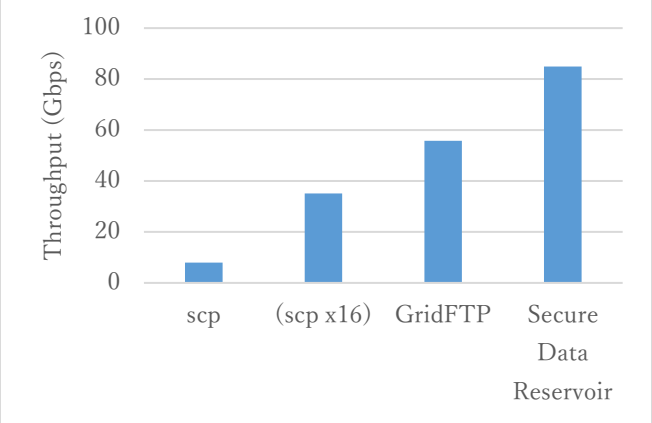

図 1: 従来手法との比較

1. 長距離ネットワーク実験環境

長距離ネットワーク上での Secure Data Reservoir の動作およびその性能を実証するために、2019 年 11 月にデンバーにて開催された SuperComputing 19 (SC19)の会場において、会場のデンバーから東京・シンガポールを経由してロサンゼルスを結ぶ太平洋を一周する 100 Gbps の長距離ネットワーク上で、暗号化データ転送の性能評価実験を行った。SuperComputing の会場では多くの関係者の協力により様々なネットワーク実験が行われており、このような世界規模の実験用高速ネットワークを利用させていただくことが可能となる。

ネットワーク構成は図 2 のような太平洋を 1 周して戻ってくる経路である。送信側および受信側の Secure Data Reservoir については双方を会場であるデンバーに設置し折り返しネットワークを用いて実験を行った。折り返し地点としては東京・シンガポール・ロサンゼルスの 3 経路を実験の対象とした。

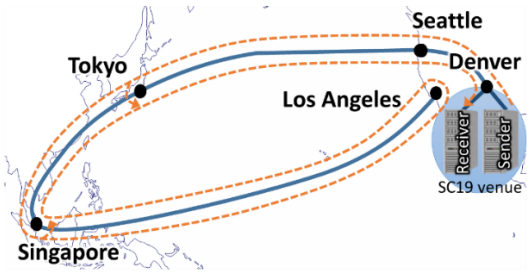

図 2: 長距離ネットワーク構成

折り返しネットワークとは、該当の経路に 2 つの VLAN を用意しルーティングを行うもので、例えば折り返し地点が東京の場合、デンバーに設置した送信側サーバからの通信は東京を経由してもう一つの VLAN を通りデンバーに設置した受信側サーバに到達する。折り返しネットワークの利用は、ネットワーク実験の両側のサーバを同じ拠点に設置することで実験の実施が容易になるとともに、データ転送のような片方向のみにトラフィックが発生する実験の場合には帯域はそのままで長さが 2 倍のネットワークとして利用することができる。本実験環境での RTT は表 1 の通りである。

経路	RTT	折り返し RTT
東京	123 ms	246 ms
シンガポール	207 ms	413 ms
ロサンゼルス	392 ms	784 ms

表 1: Round Trip Time

2. 長距離ネットワーク実験結果

測定対象としては、ネットワーク経路は東京折り返しおよびシンガポール折り返しをローカル実験の結果と比較した。ロサンゼルス折り返しについては RTT が大きすぎるため今回の実験期間内に測定に十分な安定動作を実現することができなかった。測定内容としては、性能における、長距離ネットワークの影響と、ストレージアクセスやファイル操作の影響を評価するために、暗号化メモリ間転送および暗号化ファイル転送の 2 種類の測定を行った。

実験結果は表 2 の通りである。各項目については少なくとも 5 回以上の同一の計測を行い、最も数値が高いものと低いものを除いた中間の測定値の平均値を実験結果とした。ローカル環境でのメモリ転送では 100 Gbps ネットワークをほぼ最大まで使い切っており、本システムはシングルサーバで 100 Gbps の暗号化ネットワーク送受信に十分な性能があることが確認できた。ファイル転送では 84.9 Gbps とメモリ転送よりやや低めの性能となっており、ストレージへのアクセスおよびファイル処理については一定の負荷があることが確認できる。しかし、基本性能評価において Secure Data Reservoir の暗号化ファイル転送性能は既存のツールに比べて大幅に高いことが確認できており、ファイル処理のオーバーヘッドは最小限に抑えられていると考えられる。

ローカル環境と東京折り返し経路、シンガポール折り返し経路との比較では、メモリ転送性能・ファイル転送性能ともに RTT が増大するにしたがって転送性能が低下している。TCP では利用可能な帯域が未知の状態から Slow Start アルゴリズムにより徐々に転送速度を増加させていくので、RTT が大きい環境では利用可能な最大帯域に達するまでの時間が長くなりファイル転送ジョブ全体の平均性能としては低下する。

経路	メモリ転送	ファイル転送
ローカル	98.8 Gbps	84.9 Gbps
東京	91.8 Gbps	83.7 Gbps
シンガポール	87.8 Gbps	82.6 Gbps

表 2: 長距離ネットワーク転送性能

実際の転送状況を確認するために、並列転送の各ストリームおよび転送全体の合計について、1 秒ごとの使用帯域をグラフにした。使用帯域はアプリケーション内で計測しているため、実際にはネットワーク上の使用帯域ではなくバッファにデータを投入する速度となる。バッファにデータを投入してから送信が完了して次のデータが投入されるまでには RTT の分だけ時間がかかるが、今回のような長距離ネットワークの環境では RTT が大きく測定間隔である 1 秒に近いのでグラフ上で目に見える上下の振動としてあらわれてしまう。その影響を削減するために今回は使用帯域を 3 秒の移動平均をとってグラフを作成した。

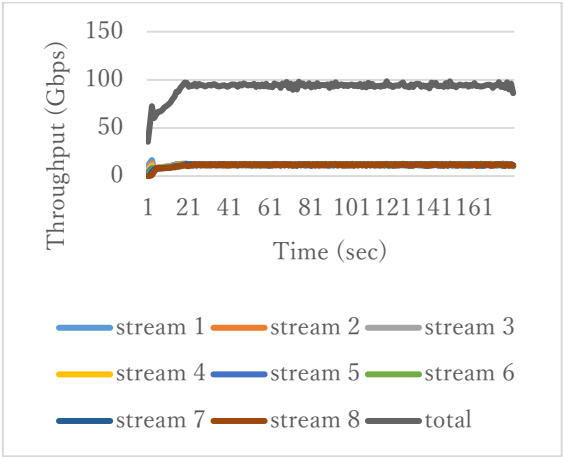

図 3: 東京折り返しメモリ転送性能

図 3 は東京折り返しのメモリ転送のグラフである。このグラフから長距離ネットワーク上でのデータ転送の基本的な動作が確認できる。各グラフは凡例の通りで、各ストリームが均等に動作しているためグラフ下方に重なって表示されている。上方の線が合計した全体性能ある。凡例については全て同様であるため以降のグラフでは省略する。

図 4 は東京折り返しのファイル転送のグラフである。転送開始から性能が最大に達成するまでの時間については長距離ネットワークの RTT に起因するものである、ファイル転送の場合でもメモリ転送と同様で東京折り返しネットワークでは 20 秒程度であることが確認できた。今回の実験では異なるファイルサイズの多数のファイルを転送しているため処理の対象によって負荷の変動があり、各ストリームの性能および合計性能にメモリ転送と比較してグラフの上下動が見られる。

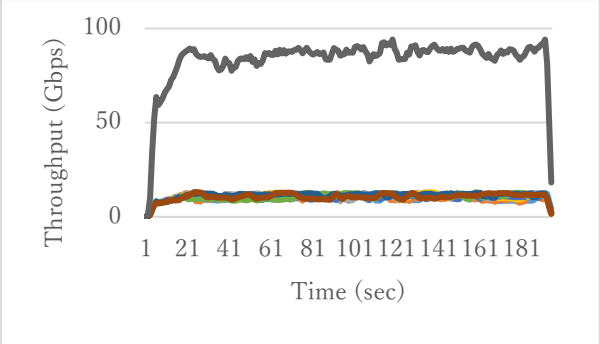

図 4: 東京折り返しファイル転送性能

図 5 はシンガポール折り返しのファイル転送のグラフである。基本的な振る舞いとしては東京折り返しと同様の結果であると言える。東京折り返しより RTT が増加した分だけ転送開始から最大性能に達するまでの時間が増加し 40 秒弱となっており、平均性能が東京折り返しと比較して低下しているのと整合性がある。

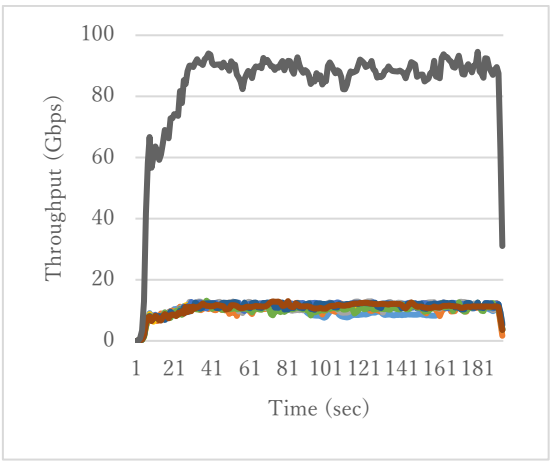

図 5: シンガポール折り返しファイル転送性能

おわりに

超高速な秘匿性・耐改竄性をもつ通信の重要性は、最近特に高まりつつある。学術的には、少数の TCP ストリームを調和的に用い、20000Km を超える超遠距離における、暗号化、復号化、ハッシュ計算を伴うデータ転送を 1 台の小型サーバで実現することは非常に困難であることが知られている。本研究ではこの難しい問題を解決した。これは非常に大きな学術的意義がある。また実際に医療機関にいくことなく細胞分析を行う、遺伝子解析を行うと高い秘匿性・耐改竄性を持つ通信が必須となる。新型コロナウィルス感染の広がりはまさに我々が予想した応用形態に合致するものであり、大きな学術的意義、社会的意義を持つといえる。

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計19件（うち招待講演　0件／うち国際学会　19件）

１．発表者名 Kenichi Koizumi,Kei Hiraki, Mary Inaba
２．発表標題 JPSC: FPGA-based Continuous Skyline Computation Accelerator for Large-Scale AI Applications
３．学会等名 HPCA 2018: 24th IEEE International Symposium on High-Performance Computer Architecture（国際学会）
４．発表年 2018年

１．発表者名 Kenichi Koizumi,Kei Hiraki, Mary Inaba
２．発表標題 FPGA-based Continuous Skyline Computation Accelerator with Delayed JR-tree Reshaping
３．学会等名 FPGA 2018: Twenty-Sixth ACM/SIGDA International Symposium on Field-Programmable Gate Arrays（国際学会）
４．発表年 2018年

１．発表者名 Kenichi Koizumi,Kei Hiraki, Mary Inaba
２．発表標題 Skyline Computation for Low-latency Image-activated Cell Identification
３．学会等名 AAAI-18: The Thirty-Second AAAI Conference on Artificial Intelligence（国際学会）
４．発表年 2018年

１．発表者名 Kenichi Koizumi,Peter Eades,Kei Hiraki, Mary Inaba
２．発表標題 BJR-tree: Fast Skyline Computation Algorithm using Dominance Relation based Tree Structure
３．学会等名 DSAA2017: International Journal of Data Science and Analytics（国際学会）
４．発表年 2017年

１．発表者名
Seongsoo Moon, Mary Inaba

２．発表標題
Boost SAT Solver with Hybrid Branching Heuristic

３．学会等名
SOCS2017（国際学会）

４．発表年
2017年

１．発表者名
Reiji Hatsugai, Mary Inaba

２．発表標題
Robust Reinforcement Learning with a Stochastic Value Function.

３．学会等名
MOD 2017（国際学会）

４．発表年
2017年

１．発表者名
Seongsoo　Moon、稲葉真理

２．発表標題
Boost SAT solver with hybrid branching heuristic

３．学会等名
IJCAI 2017（国際学会）

４．発表年
2017年

１．発表者名
小泉賢一、平木敬、稲葉真理、他6名

２．発表標題
Single stream TCP data transfer over trans pacific 100Gigabit network

３．学会等名
43rd Asia-Pacific Advanced Network (APAN43) Meeting（国際学会）

４．発表年
2017年

１．発表者名
西野兼治、稲葉真理

２．発表標題
The filling-in Function of the Bayesian AutoEncoder Network

３．学会等名
2017 the Second International Workshop on Pattern Recognition (IWPR 2017)（国際学会）

４．発表年
2017年

１．発表者名
小泉賢一、平木敬、稲葉真理、下見淳一郎、他5名

２．発表標題
Single stream TCP data transfer over trans pacific 100Gigabit network

３．学会等名
43rd Asia-Pacific Advanced Network (APAN43) Meeting（国際学会）

４．発表年
2017年

１．発表者名
小泉賢一、平木敬、稲葉真理、他1名

２．発表標題
Complexity Analysis and Balancing Extension of JR-tree for Continuous Skyline Computation

３．学会等名
EDBT 2017 : 20th International Conference on Extending Database Technology（国際学会）

４．発表年
2017年

１．発表者名
小泉賢一、平木敬、稲葉真理

２．発表標題
All You Need is Deep Buffer: Observations of Multiple TCP Streams on Long Fat-pipe Networks

３．学会等名
SC16 (Supercomputing 2016): The International Conference for High Performance Computing, Networking, Storage and Analysis（国際学会）

４．発表年
2016年

１．発表者名
小泉賢一、平木敬、稲葉真理、下見淳一郎、他3名

２．発表標題
Extensions for 100 Gbps Single TCP Stream on High Bandwidth-Delay Product Networks

３．学会等名
TNC16 : The Networking Conference 2016（国際学会）

４．発表年
2016年

１．発表者名
小泉賢一、平木敬、稲葉真理

２．発表標題
JR-tree: Effective Tree Structure for Continuous Skyline Computation

３．学会等名
VLDB2016 : 42nd International Conference on Very Large Data Bases（国際学会）

４．発表年
2016年

１．発表者名
森　清貴、稲葉真理、他2名

２．発表標題
Algorithm for Detecting Overlapped Community Structures in Complex Networks

３．学会等名
1st Workshop on Scholarly Web Mining (in conjunction with WSDM2017)（国際学会）

４．発表年
2017年

１．発表者名
福永 武志、平木敬、稲葉真理、下見淳一郎、他4名

２．発表標題
Fully secure 6Gbps le transfer for personal genome data application

３．学会等名
The TNC16 Networking Conference（国際学会）

４．発表年
2016年

１．発表者名
文　性琇、稲葉真理

２．発表標題
Dynamic strategy to diversify search using history map in parallel solving

３．学会等名
Learning and Intelligent OptimizatioN (LION 10)（国際学会）

４．発表年
2016年

１．発表者名
平木敬、稲葉真理、下見淳一郎、他4名

２．発表標題
Distance scalability in real-time sensor fusion systems

３．学会等名
TNC16 : The Networking Conference 2016（国際学会）

４．発表年
2016年

１．発表者名
小泉賢一、平木敬、稲葉真理

２．発表標題
Fast Recovery for SACK-disabled TCP on Long-distance Fat-pipe Networks

３．学会等名
NSDI '17: 14th USENIX Symposium on Networked Systems Design and Implementation（国際学会）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
本研究により、電気情報通信学会の2019年度IA研究賞（最優秀賞）を受賞した。

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
研究分担者	下見　淳一郎 (Shitami Junichiro) (40417225)	東京大学・大学院理学系研究科（理学部）・助教 (12601)	
研究分担者	宮野　悟 (Miyano Satoru) (50128104)	東京大学・医科学研究所・教授 (12601)	
研究分担者	稲葉　真理 (Inaba Mary) (60282711)	東京大学・大学院情報理工学系研究科・准教授 (12601)	