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　 １ 日現在

機関番号：１２６０５
研究種目：若手研究(A)
研究期間：2016～2019
課題番号：１６Ｈ０６０９１

研究課題名（和文）双方向通信を伴う分散計算のための情報理論の展開

研究課題名（英文）Distributed computation via interactive communication

研究代表者
渡辺　峻（Watanabe, Shun）

東京農工大学・工学（系）研究科（研究院）・准教授

研究者番号：７０５４６９１０

交付決定額（研究期間全体）：（直接経費）　　12,600,000円

研究成果の概要（和文）：情報理論は従来のように通信システムの漸近的な性能指針を与えるに留まらず，近年は有限長における性能指針を与える手法が発展してきている．本研究では，ネットワークセキュリティにおいて重要な秘密鍵共有や，センサーネットワークのモデルである分散仮説検定の問題などに対して，有限のブロック長における性能指針を与える方法論を発展させることに成功した．

研究成果の学術的意義や社会的意義
情報理論は現在の情報通信技術を背後で支える基盤理論である．特に，1970年代から1980年代に発展したマルチユーザ情報理論は近年の無線通信網の発展などに大きく貢献している．一方，情報理論は実用的なシステムを構築する際の指針は与えているものの，理論と実践の間に多少のギャップがあることは否定できない．近年，そのようなギャップを埋めるために，遅延が有限である際の性能指針を与える有限長解析理論が発展してきている．本研究は，そのような有限長解析理論をセキュリティなどを含むいくつかのマルチユーザの問題に展開してものであり，今後の情報通信技術の発展を促進するものであると考えられる．

研究成果の概要（英文）：Recently, information theory has developed so that it can provide a performance criterion for communication systems with finite block length.. In this research, for the problem of secret key agreement, which is an important problem in the network security, and the problem of distributed hypothesis testing, which is a model for sensor network, we have developed an analysis method for evaluating finite block length performance.

研究分野：情報理論

キーワード：情報理論　暗号理論　秘密鍵共有　秘密計算　双方向通信

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

パーティ間で双方向の通信を伴う分散計算は，所望のタスクを効率的に実現できることから注目を集めている．また，情報理論は従来のように通信システムの漸近的な性能指針を与えるに留まらず，近年は有限長における性能指針を与える手法が発展してきていた．しかしながら，双方向の通信を伴うプロトコルに対しては十分な研究がされておらず，漸近的な解析手法はいくつか知られていたものの，実用的なシステムの解析に使えるような手法が開発されておらず，多くの基礎的な問題が未解決であった．

２．研究の目的

本研究では，双方向の通信を伴う分散計算プロトコルに対する非漸近的な性能解析手法を確立することを目的としていた．特に，申請者のこれまでの研究成果をもとに，セキュリティを伴うタスクの解析手法を発展させることを目指していた．

３．研究の方法

本研究では，複数のユーザが参加するマルチユーザネットワークにおける有限長解析を発展させるためのテクニックの開発に注力した．マルチユーザの問題では特殊な符号化法を使うことに起因する補助確率変数が現れることと，分散符号化に起因するマルコフ連鎖の条件が現れることが解析を著しく困難にしている．本研究ではこれらの困難を乗り越えるためのツールの開発に注力した．

また，複数のユーザが所有するデータを処理した結果を計算する分散関数計算の問題では，通常のデータ圧縮と異なりデータの関数値だけを復元することを目的とするため，符号の最適性を示すのが著しく困難である．そのため，最適な符号化レートを評価するための新しい解析手法が必要になり，本研究では新しい解析手法の開発に注力した．

複数の地点で観測したデータに基づき統計的検定を行う分散仮説検定分散データ圧縮と統計学の複合問題として 1990 年頃から研究が始まった．しかしながら，従来の研究では前金的な性能解析が主に行われており，有限長性能の評価は十分に行われていなかった．そこで，本研究では有限長において優れた性能を有する分散検定法の模索に注力した．

マルチユーザネットワークにおいて安全な通信を行うためには，ユーザ間で秘密鍵を共有する必要がある．秘密鍵共有の問題は多くの先行研究で研究されていたものの，それらの研究では鍵を生成するためのシード乱数の分布が既知である場合を考えていた．より現実的には分布が未知の場合を考える必要があるため，本研究では分布を適応的に推定しながら鍵共有が行えるプロトコルの開発に注力した．

４．研究成果

前述の方法に基づき，本研究では大きく分けると以下の４つの成果をあげることができた．

＜マルチユーザネットワークにおける有限長解析の方法＞

前述のように，マルチユーザの問題では特殊な符号化法を使うことに起因する補助確率変数が現れる．本研究では補助確率変数が現れる最もシンプルなネットワークである，Gray-Wyner ネットワークを考察し，最適な二次オーダレートを導出することに成功した．さらに，この解析手法を発展させ，様々なマルチユーザネットワークに対して，強逆符号化定理を示すためのテクニックを開発することに成功している．さらに，このテクニックを暗号理論において重要な Parallel Repetition 定理の証明にも応用している．

＜分散関数計算における性能解析手法＞

前述のように，分散関数計算の問題において，受信側では観測データには興味がなく，それらを処理した関数値のみに興味があるため，通常のデータ通信における解析手法はあまり使えず，従来の研究では非常に複雑な解析手法によって分散計算プロトコルの性能解析を実施していた．本研究では，分散計算の特徴と関数の構造に基づく新たな性能解析手法を提案した．提案手法は従来の手法で扱えなかったより広いクラスの関数に対して適用可能である．さらに，この提案手法を３人以上のユーザが参加するマルチユーザネットワークに拡張した．マルチユーザの場合，復号器が情報源を直接観測することができないため，提案法を直接適用することができない．そこで，関数構造から誘導される条件付き独立性を利用し復号器で情報源のシミュレーションを行うというアイディアに基づき，性能解析を行う手法を提案した．この方法により，従来は性能解析が困難であった関数に対しても性能解析が可能になった．

＜分散仮説検定における Neyman-Pearson 型の検定法の提案＞

通常の仮説検定における重要な検定法として，Neyman-Pearson の検定法と Hoeffding の検定法がある．分散仮説検定において，従来の研究で Hoeffding 型の検定法が提案されており，漸近的に最適な性能を有することが明らかにされていた．本研究では，Neyman-Pearson 型の検定法を提案し，漸近的には Hoeffding 型の検定法と同等な性能を有し，有限長においては従来より優れた性能を有することを明らかにした．

＜双方向通信を用いたマルチユーザユニバーサルプロトコルの提案＞

マルチユーザの秘密鍵共有ならびにデータ交換の問題において，従来の研究ではデータが生成される分布が既知であることを仮定して研究がされていた．しかしながら，現実的には分布を正確に知ることは困難であり，データが生成される分布に依存しないユニバーサルなプロトコルの提案が望まれていた．本研究では，分布が未知である場合にも，最適なデータ交換レートならびに最適な秘密鍵生成レートを有するユニバーサルなプロトコルを提案した．提案したプロトコルは双方向の通信を利用した可変長符号化によるプロトコルであり，未知の分布に対して適応的に最適なレートを達成することが可能である．

５．主な発表論文等

〔雑誌論文〕　計10件（うち査読付論文　10件／うち国際共著　5件／うちオープンアクセス　0件）

１．著者名 Watanabe Shun	４．巻 64
２．論文標題 Neyman-Pearson Test for Zero-Rate Multiterminal Hypothesis Testing	５．発行年 2018年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 4923～4939
掲載論文のDOI（デジタルオブジェクト識別子） https://doi.org/10.1109/TIT.2017.2778252	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Himanshu Tyagi and Shun Watanabe	４．巻 63
２．論文標題 Universal Multiparty Data Exchange and Secret Key Agreement	５．発行年 2017年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 4057-4074
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2694850	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Himanshu Tyagi, Shaileshh Bojja Venkatakrishnan, Pramod Viswanath, and Shun Watanabe	４．巻 63
２．論文標題 Information Complexity Density and Simulation of Protocols	５．発行年 2017年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 6979-7002
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2746859	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

１．著者名 Shigeaki Kuzuoka and Shun Watanabe	４．巻 63
２．論文標題 On Distributed Computing for Functions with Certain Structures	５．発行年 2017年
３．雑誌名 IEEE Transactions on Information Theory	６．最初と最後の頁 7003-7017
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2749234	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Himanshu Tyagi, Pramod Viswanath, and Shun Watanabe	4．巻 64
2．論文標題 Interactive Communication for Data Exchange	5．発行年 2018年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 26-37
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2017.2769124	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 S. Watanabe	4．巻 63
2．論文標題 Second-Order Region for Gray-Wyner Network	5．発行年 2017年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 1006-1018
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2016.2642985	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 M. -H. Hsieh and S. Watanabe	4．巻 62
2．論文標題 Channel Simulation and Coded Source Compression	5．発行年 2016年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 6609-6619
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2016.2597853	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 M. Hayashi, H. Tyagi, and S. Watanabe	4．巻 62
2．論文標題 Secret Key Agreement: General Capacity and Second-Order Asymptotics	5．発行年 2016年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 3796-3810
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2016.2567440	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

1．著者名 M. Hayashi and S. Watanabe	4．巻 62
2．論文標題 Uniform Random Number Generation from Markov Chains: Non-Asymptotic and Asymptotic Analyses	5．発行年 2016年
3．雑誌名 IEEE Transactions on Information Theory	6．最初と最後の頁 1795-1822
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/TIT.2016.2530084	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 M. Hayashi and S. Watanabe	4．巻 44
2．論文標題 Information Geometry Approach to Parameter Estimation in Markov Chains	5．発行年 2016年
3．雑誌名 Annals of Statistics	6．最初と最後の頁 1495-1535
掲載論文のDOI（デジタルオブジェクト識別子） 10.1214/15-AOS1420	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計9件（うち招待講演　3件／うち国際学会　7件）

1．発表者名 Himanshu Tyagi and Shun Watanabe
2．発表標題 Strong Converse using Change of Measure Arguments
3．学会等名 2018 IEEE International Symposium on Information Theory（国際学会）
4．発表年 2018年

1．発表者名 Shun Watanabe
2．発表標題 Proving Strong Converse is Difficult?
3．学会等名 International Conference on Signal Processing and Communications（招待講演）
4．発表年 2018年

１．発表者名
Shun Watanabe

２．発表標題
Second-Order Optimal Test in Composite Hypothesis Testing

３．学会等名
2018 International Symposium on Information Theory and Its Applications (ISITA)（国際学会）

４．発表年
2018年

１．発表者名
Himanshu Tyagi and Shun Watanabe

２．発表標題
Optimality of Recursive Data Exchange Protocol

３．学会等名
2017 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2017年

１．発表者名
Shun Watanabe

２．発表標題
A Converse Bound on Wyner-Ahlswede-Korner Network via Gray-Wyner Network

３．学会等名
2017 IEEE Information Theory Workshop（国際学会）

４．発表年
2017年

１．発表者名
Shun Watanabe

２．発表標題
Neyman-Pearson Test and Hoeffding Test

３．学会等名
Beyond IID Workshop 2017（招待講演）

４．発表年
2017年

１．発表者名
S. Kuzuoka and S. Watanabe

２．発表標題
On Distributed Computing for Functions with Certain Structures

３．学会等名
2016 IEEE Information Theory Workshop（国際学会）

４．発表年
2016年

１．発表者名
H. Tyagi and S. Watanabe

２．発表標題
Universal Multiparty Data Exchange

３．学会等名
2016 IEEE International Symposium on Information Theory（国際学会）

４．発表年
2016年

１．発表者名
S. Watanabe

２．発表標題
Neyman-Pearson Test for Zero-Rate Multiterminal Hypothesis Testing

３．学会等名
2017 Information Theory and Application Workshop（招待講演）（国際学会）

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
https://sites.google.com/site/shunwatanabeshomepage/

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