早稲田大学大学院　基幹理工学研究科

博　士　論　文　概　要

論　文　題　目

計算時間，信頼性，情報秘匿性を考慮した分散符号化計算方式に関する研究

A Study on Distributed Coded Computation Methods Considering Computation Times, Error-Correcting Capabilities and Information Securities

申　請　者

風間　皐希
Koki KAZAMA

数学応用数理専攻　情報理論研究

2021年12月

大規模データを扱う機会が増えた現代社会において，高速にデータを処理する方式の研究の一つである分散計算方式の必要性が，いっそう高まっている．分散計算方式は，主要な計算機（マスター）が複数の計算機（ワーカー）にデータの一部を分散し，並列計算を行う方式である．この方式には，(a)という利点があるが，(b)(c)といった欠点がある．

(a) システムの総計算時間を少なくする．

(b) ワーカーの故障等により，マスターが一部のワーカーの計算結果を受信できない，あるいはマスターが誤った値を受信する可能性が高まる．マスターが一部のワーカーの計算結果を受信しなかったとき，その計算結果に消失が発生したとみなす．また，マスターが誤った値を受信したとき，その計算結果に誤りが発生したとみなす．

(c) データに個人情報などユーザの秘密情報を含む場合，データを分散することで秘密情報が多くのワーカーに漏洩する可能性が高まる．

本研究では，利点(a)を有しつつ，欠点(b)や(c)を解消する分散計算方式の数学的基礎理論を論じる．本研究では，(b)に対する耐性を信頼性，(c)に対する耐性を情報秘匿性と呼ぶ．(a)と(b)を考慮した方式は，従来から分散符号化計算方式という方式が提案されているが，本研究では耐性のある誤り消失の範囲を拡張する．これについては，本論文の第 3,4 章で論じる． 一方，(a)(b)(c)をすべて同時に考慮した方式は従来提案されておらず，本研究で新たに提案する．これについては，第 5 章で論じる．本研究では，特に，有限体 F_q 上の巨大な $k_A \times l$ 行列 A と $l \times k_B$ 行列 B の積行列 AB の計算方式を論じる．

第 3 章で論じられている従来の分散符号化計算方式の一般的手順は次の通りである．ここでは，マスターと n 台のワーカーを用いる．ただし $n \geqq k_A$.

(1) 行列 A が入力されると，マスターは，前処理として，行列 A を k_A 個の行ベクトルに分割し，F_q 上 $n \times k_A$ 行列 G を用いて冗長性を付加する変換（符号化）を行い $n \times l$ 行列 GA に変換する．その後，GA を n 個の行ベクトルに分割し，n 台のワーカーに行ベクトルを 1 個ずつ送信する． i 番目のワーカーは GA の i 番目の行ベクトルを受信して保存する．

(2) 行列 B が入力されると，マスターは全ワーカーに行列 B を送信する．I 番目のワーカーは保存していた GA の i 番目の行ベクトルと行列 B の積計算を行い，マスターに計算結果を送信する．この分散計算において，マスターは，一部のワーカーの計算結果を受信しない，あるいは誤った出力を受信する場合を想定する．

(3) マスターは，各ワーカーから受信した計算結果を集約し，誤りや消失の訂正（復号）を行う．誤り，あるいは消失が発生した箇所の個数がある条件を満たせば，積行列 AB の正しい値を得る．

全ワーカーにベクトルを分散させて並列計算する計算時間と，単独のワーカーで計算する計算時間の比は 1/n 程度になるため，この方式におけるシステム全体

の総計算時間は削減される．また，この方式は，デジタルデータ通信において発生した誤り，消失を訂正する方式である誤り訂正符号の原理を利用しているため，計算途中で生じた誤り，消失を条件によっては訂正可能である．

第3章では，最初に，上記で説明した従来方式の数理的に厳密な再定式化により，分散符号化計算方式において誤り訂正符号の原理が機能する部分を明確化する．これを明確化にすることもまた本研究の新規性の一部に含まれる．この再定式化により，従来の分散符号化計算方式は，積行列ABを列ごとに符号化しGABを得る方式であることを明確し，したがって，一部のワーカーの故障による誤り，消失を訂正可能な方式であることを再確認する．

上記をもとに，第4章では，ワーカーの試みる分散計算の結果が積行列AB自体をまとめて符号化した行列となるように各ワーカーの計算する関数を変更した方式を，本研究の方式として提案する．特に，一例として，行列ABをGabidulin符号化する方式の構成法を提案し，従来では訂正できなかったワーカー全体に及ぶ誤りも条件により訂正可能であることを示す．さらに，誤り訂正能力と計算時間の評価や従来法との比較も行う．

第5章では，本研究の新たな方式として，(a)(b)(c)を同時に考慮した分散符号化計算方式である「グループ型秘匿分散符号化計算方式」を提案する．ここでは，一部のワーカーは結託して自身の有する情報を持ち寄ることで行列Aの値を得ようとするが，マスターは行列Aの値を秘匿したいとする．なお，マスターは行列Bの値を各ワーカーに公開してもよいとする．従来，(b)と(c)に着目する研究として秘匿分散符号化計算方式が論じられてきたが，(a)に着目しない点で本研究と異なる．

第5章で新たに提案するグループ型秘匿分散符号化計算方式（基本方式）の手順は，次の通りである．ここでは，ワーカーをn_A個のグループに分ける．各グループはn_B個のワーカーで構成される．

(1) 行列Aが入力されると，マスターは，前処理として，行列Aとそれとは独立な確率変数行列Rを並べた行列$(A^T,R^T)^T$を符号化して行列$\tilde{A}$を生成する．その後，$\tilde{A}$をn_A個の部分行列に分割し，n_A個のグループに部分行列を1個ずつ送信する．i番目のグループはi番目の部分行ベクトルを受信して，グループ内の各ワーカーは同じi番目の部分行列を保存する．

(2) 行列Bが入力されると，マスターは行列Bをn_B個の部分行列に分割し各ワーカーに送信する．i番目のグループのj番目のワーカーは，$\tilde{A}$のi番目の部分行列とBのj番目の部分行列の積を計算し，その出力結果をマスターに送信する．この分散計算において，マスターは，一部のグループ，あるいは一部のワーカーの計算結果を受信しない，あるいは誤った結果を受信することを想定する．

(3) マスターは，各ワーカーから受信した計算結果を集約し，復号を行う．誤り，あるいは消失が発生した箇所の個数がある条件を満たせば，積行列ABの正

しい値を得る．

(1)において，行列 A と確率変数行列 R を用いて生成した行列 $\tilde{A}$ を部分行列へ分割することによって，行列 A の値が各ワーカーへ秘匿される．具体的には，グループ間で結託するワーカーの個数が一定以下の時に，行列 A の情報が一切漏洩しないことが保証される．さらには，(1)における符号化によって，マスターはグループ間で発生した誤り，消失を訂正できる．また，(2)において，行列 B が分割されることにより，各ワーカーの計算時間が少なくなる．

さらに，本研究では，グループ内で発生した誤りや消失も訂正可能な方式など，情報秘匿性や信頼性を一般化した方式の構成法もまた提案する．そして，信頼性，情報秘匿性，計算時間の性能評価を行うことで，これらの方式が良い性質を持つことを示す．

本論文は，以下のように構成される．まず，第 1 章では，本論文の研究背景と研究目的，研究成果の概要を述べる．第 2 章では，符号理論，秘密分散等，本研究に必要な基礎事項を説明する．第 3 章では，最初に，上記で説明した従来方式の数理的に厳密な再定式化により，分散符号化計算方式において誤り訂正符号の原理が機能する部分を明確化する．さらに，秘匿性を有する分散方式の従来研究についても説明する．第 4 章，第 5 章が，本研究の提案の内容の説明である．第 4 章では，ワーカーの試みる分散計算の結果が積行列 AB 自体をまとめて符号化した行列となるように各ワーカーの計算する関数を変更した方式を，本研究の方式として提案する．第 5 章では，本研究の新たな方式として，(a)(b)(c)を同時に考慮した分散符号化計算方式である「グループ型秘匿分散符号化計算方式」を提案する．最後に第 6 章では，本論文のまとめと今後の課題を説明する．

早稲田大学　博士（工学）　学位申請　研究業績書

氏名：風間　皐希　印

（2022年　1月　現在）

種類別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
論文○	Gabidulin符号に基づく符号化分散計算方式とその誤り訂正能力の評価 電子情報通信学会論文誌A, Vol.J104-A, No.6, pp.156-159, 2021年6月 風間皐希, 鎌塚明, 吉田隆弘, 松嶋敏泰
論文	拡張直交配列を用いた混合水準の実験計画法に関する一考察 電子情報通信学会論文誌A, Vol.J103-A, No.1, pp.17-24, 2020年1月 山口純輝, 風間皐希, 鎌塚明, 齋藤翔太, 松嶋敏泰
講演	一般的なアクセス構造を実現する秘密分散方式を用いた行列の積計算のための秘匿符号化分散計算方式に関する一考察 第44回情報理論とその応用シンポジウム(SITA2021), 兵庫県, 2021年12月 風間皐希, 松嶋敏泰
講演	高効率なプライバシー保護情報検索システムの構成アルゴリズムの提案 日本経営工学会 2021年 春季大会, オンライン開催, 2021年5月 今津潮, 風間皐希, 松嶋敏泰
講演	クラスタごとに状態遷移確率が異なる複数の対象を同時制御するためのマルコフ決定過程 電子情報通信学会情報論的学習理論と機械学習研究会（IBISML）, オンライン開催, 2021年3月 本村勇人, 鎌塚明, 風間皐希, 松嶋敏泰
講演○	A Note on a Relationship between Smooth Locally Decodable Codes and Private Information Retrieval 2020 International Symposium on Information Theory and Its Application (ISITA), online, Oct. 2020 Koki KAZAMA, Akira KAMATSUKA, Takahiro YOSHIDA, Toshiyasu MATSUSHIMA
講演	Private Information Retrieval と Smooth Locally Decodable Codes の対応関係に関する一考察 電子情報通信学会情報理論研究会（IT）, 発表中止, 2020年3月 風間皐希, 鎌塚明, 吉田隆弘, 松嶋敏泰
講演	セキュアな再生成符号に基づく分散ストレージシステムにおける秘匿情報検索 第42回情報理論とその応用シンポジウム(SITA2019), 鹿児島県, 2019年11月 鎌塚明, 風間皐希, 吉田隆弘, 松嶋敏泰
講演	拡張直交配列を用いた混合水準の実験計画法に関する一考察 みずほ銀行・早稲田大学 学術交流協定締結1周年記念シンポジウム, 東京都, 2019年7月 山口純輝, 風間皐希, 鎌塚明, 齋藤翔太, 松嶋敏泰
講演	$(n,k,d,r,t,x,y)_{q}$ LRC符号の最小距離および次元の限界式に関する一考察 第41回情報理論とその応用シンポジウム予稿集（SITA2018）, 福島県, 2018年12月 風間皐希, 鎌塚明, 松嶋敏泰
講演	拡張直交配列を利用した多水準の実験計画法に関する一考察 第41回情報理論とその応用シンポジウム予稿集（SITA2018）, 福島県, 2018年12月 山口純輝, 風間皐希, 鎌塚明, 齋藤翔太, 松嶋敏泰
講演○	A Note on a Bound on the Rate of a Locally Recoverable Code with Multiple Recovering Sets 2018 International Symposium on Information Theory and Its Application (ISITA), Singapore, Oct. 2018 Koki KAZAMA, Akira KAMATSUKA, Takahiro YOSHIDA, Toshiyasu MATSUSHIMA
講演	On Distance Properties of (r, t, x)-LRC Codes（最新論文紹介セッション） 第7回 誤り訂正符号のワークショップ, 岩手県, 2018年9月 風間皐希, 松嶋敏泰
講演	ランク誤りを考慮したcoded computationに関する一考察 データ科学総合研究教育センター第3回シンポジウム, 東京都, 2018年7月 風間皐希, 鎌塚明, 松嶋敏泰

早稲田大学　博士（工学）　学位申請　研究業績書

氏名：風間　皐希　　印

（2022年　　1月　現在）

種類別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
講演	ランク誤りを考慮したcoded computationに関する一考察 第40回情報理論とその応用シンポジウム(SITA2017), 新潟県, 2017年11月−12月 風間皐希, 鎌塚明, 松嶋敏泰
講演	シンボルペア通信路における符号のリスト復号に関する一考察 第39回情報理論とその応用シンポジウム(SITA2016), 岐阜県, 2016年12月 風間皐希, 鎌塚明, 松嶋敏泰
講演○	A Maximum Likelihood Decoding Algorithm of Gabidulin Codes in Deterministic Network Coding 2016 International Symposium on Information Theory and Its Applications (ISITA), Monterey, California, USA, Oct.-Nov. 2016 Koki KAZAMA, Akira KAMATSUKA, Toshiyasu MATSUSHIMA
講演	A Note on Unequal Error Protection in Random Network Coding 2016 International Symposium on Information Theory and Its Applications (ISITA2016), Monterey, California, USA, Oct.-Nov. 2016 Tomohiko SAITO, Koki KAZAMA, Toshihiro NIINOMI, Toshiyasu MATSUSHIMA
講演	Subspace Unequal Error Protection Codes for Random Linear Network Coding 2016 International Symposium on Multimedia and Communication Technology, Tokyo, Japan, Aug.-Sep. 2016 Tomohiko SAITO, Koki KAZAMA, Toshihiro NIINOMI, Toshiyasu MATSUSHIMA
講演	Array-Errorモデルにおける軟判定復号に関する一考察 電子情報通信学会情報理論研究会（IT）, 大阪府, 2016年1月 風間皐希, 鎌塚明, 吉田隆弘, 松嶋敏泰