第56回 東海ファジィ研究会In 蒲郡（蒲研2024）
予稿集

主催：日本知能情報ファジィ学会・東海支部
協賛：IEEE名古屋支部
日本経営システム学会中部支部
日時：2024年8月5日(月)～6日(火)
会場：生命の海科学館　メディアホール

第56回東海ファジィ研究会（2024年8月5日～6日）プログラム

8月5日（月）

13:50-13:55 【開会挨拶】研究会幹事 野崎佑典（名城大学）

13:55-15:15 セッション1　座長: 高瀬治彦 （三重大学）

S1-01 SegNetによる頸動脈エコー画像のIMT領域分割手法の提案
土居 瑞生　宇佐美 裕康　中山 奈津紀　荒川 尚子

S1-02 かみこみ検査装置（三友工業）の紹介
中垣　雄太

S1-03 ジョジョの奇妙な冒険第二部におけるオノマトペの音象徴
中村剛士　元浪裕　吉兼利浩

S1-04 多属性意思決定における決定方略のクラスター分析
竹村　和久　　玉利　祐樹　　井出野　尚

15:15-15:30 休憩

15:30-16:30 特別講演 座長: 中村剛士（中部大学）
言語的配慮に基づく対話システムによる人間－システム間の新たな関係性構築
片上 大輔　（東京工芸大学）

16:30-18:00 休憩

18:00-23:30 ナイトセッション　座長: 吉川大弘 （鈴鹿医療科学大学）
討論テーマ1「ChatGPT、生成AIとどうつきあい、どう活用するか」
討論テーマ2「理工系分野にて女性活躍社会を実現するには?」

8月6日（火）

9:20-10:20 セッション2　座長: 森田賢太 （鈴鹿医療科学大学）

S2-01 パルス列の処理における Attention 機構と SNN の 学習コスト比較
大須賀 翼　高瀬 治彦　北 英彦

S2-02 ブロックチェーンを用いた塾講師評価システムの提案
岡田蘭丸　竹本修　野崎佑典　吉川雅弥

S2-03 低遅延軽量暗号LTLBCのFPGAへの実装評価
野崎佑典　吉川雅弥

10:20-10:25 【閉会挨拶】東海ファジィ研究会・支部長　中村剛士（中部大学）

会場：生命の海科学館　メディアホール
〒443-0034　愛知県蒲郡市港町17-17
TEL 0533-66-1717

SegNet による頸動脈エコー画像の IMT 領域分割手法の提案

土居瑞生 [1] 宇佐美裕康 [1] 中山奈津紀 [2] 荒川尚子 [3]
[1] 中部大学工学部情報工学科 [2] 名古屋大学医学系研究科 [3] 中部大学生命健康科学部

１．はじめに

頸動脈エコー検査[1]は，頸動脈硬化等の診断に活用され，その診断には総頸動脈における内膜中膜複合体の厚みを測定する Intima Media Thickness（IMT）が用いられる．動脈硬化の早期診断は脳や心臓疾患の予防に重要であり，IMT の正確な測定が求められる．しかし，現行の測定は検査技師によって手動で行われるため，微細な変化の把握が難しく，技師の技量により測定結果にばらつきが生じる．

３．提案手法

本研究では，画像分類を前処理とした SegNet[2] による頸動脈エコー画像の IMT 領域分割手法を提案する．本研究では，モバイルエコーへの実装を見据え，画像分類タスクでは少ないメモリで実装可能な CNN を用いてモデルを構築し，セグメンテーションのタスクに関しては SegNet を用いてモデルを構築している．以下に，画像分類タスク並びにセグメンテーションタスクの詳細について述べる．

画像分類タスク: 画像分類では，3 つのモデルを構築する．分類 1 では長軸断面画像とその他の画像を分類し，分類 2 では IMT 領域が確認できる長軸断面画像とその他の画像を分類する．分類 3 では，まず長軸断面画像とその他の画像を分類（分類 1）し，長軸断面画像に分類されたものを対象に，IMT 領域が確認できるかどうかを分類（分類 2）する．

セグメンテーションタスク: セグメンテーションでは，2 つの SegNet モデルを構築する．セグメンテーション 1 では IMT 領域のみをセグメンテーションし，セグメンテーション 2 では血管のセグメンテーションを行った後，血管領域を拡大し，その画像に対して IMT のセグメンテーションを行う．セグメンテーションは，分類前のデータセットと，分類 1，分類 2，分類 3 で長軸または IMT 領域が確認できると分類された画像を対象に実行する．

３．実験

190 枚の頸動脈エコー画像を用いて実験を行った．分類は K-分割交差検証（5 分割）で行い，分類 1 と分類 2 の学習には 152 枚，テストには 38 枚を用い，この処理を 5 回繰り返す．分類 3 では，1 回目の分類に 152 枚の学習データと 38 枚のテストデータを用い，2 回目の分類では，1 回目の分類で長軸に分類された画像を対象に行う．セグメンテーションの学習データは長軸画像 85 枚，テストデータは分類で長軸または IMT 領域を有する長軸と分類された画像を使用した．分類結果を表 1 に示す．

表 1　分類結果（Accuracy）

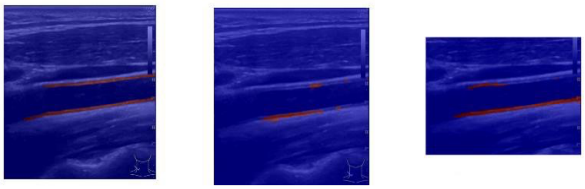
Model	長軸とその他	IMT 領域ありとその他	精度
分類 1	92.63	-	92.63
分類 2	-	90.53	90.53
分類 3	(92.63)	(83.03)	91.57

分類結果から，分類 2 と分類 3 を比較すると，2 回の分類を行う分類 3 ではより精度が向上したことが確認できる．セグメンテーション結果を表 2 に示す．

表 2　セグメンテーション結果（IoU）

Model	セグメンテーション 1	セグメンテーション 2
分類なし	14.147	15.534
分類 1	23.368	36.680
分類 2	29.107	32.066
分類 3	31.318	43.903

IMT 領域の抽出結果を図 1 に示す．



(a)真値　(b)セグメンテーション 1　(c)セグメンテーション 2

図 1　IMT 領域抽出結果

分類 3 と分類 2 の結果から，分類精度が高いとセグメンテーション結果の精度も向上することが確認できる．また，表 1 と表 2 の結果より，分類 3 と分類 1 では分類のタスクでは分類 1 の精度が高いが，長軸の分類に加え，IMT 領域の分類を行うことで，最終的な領域分割のタスクではセグメンテーション結果が向上することが確認できる．セグメンテーション 1 とセグメンテーション 2 の結果から後者の方がより精度が高いことから，血管セグメンテーションを前処理として行うことで精度が向上することが確認できる．また，図 2 からも血管セグメンテーションを前処理として行うことで精度が向上していることが確認できる．

３．おわりに

本研究では，画像分類を前処理とした SegNet による頸動脈エコー画像の IMT 領域分割手法を提案した．実験結果より，IMT 領域を観察するために適したシーンを抽出する画像分類を前処理とすることで，最終的な IMT 領域の抽出結果を向上させることができている．今後は実装を見据えより軽量なセグメンテーションモデルの構築ならびにさらなる精度向上を目指す．

参考文献

[1] 日本超音波医学会用語・診断基準委員会，頸動脈超音波診断ガイドライン小委員会．超音波による頸動脈病変の標準的評価法 2017. jsum0515, GUIDELINE.

[2] Vijay Badrinarayanan, Alex Kendall, and Roberto Cipolla. Segnet: A deep convolutional encoder-decoder architecture for image segmentation. IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 39, No. 12, pp. 2481–2495, 2017.

かみこみ検査装置（三友工業）の紹介

中垣雄太[1]
[1]三友工業株式会社

１．はじめに

かみこみとは、食品・日用品のパッケージフィルムなどのシール部分に内容物がはさまっている状態をさす．（図１参照）

食品や日用品のパッケージフィルムは、中の商品が出てこないように閉じることを目的としているが、商品を投入し閉じる際にかみこみが発生する可能性がある．

かみこみがあると、パッケージが完全に閉じられずに中のものがでてきてしまう恐れがある．
また、密封されない為、商品の品質低下に繋がる恐れもあり、食品・日用品メーカー様にて重要な検査項目となる．

図１　かみこみサンプル

２．自動化に向けての課題

２点の課題を下記する．

(i) パッケージフィルムには透明なものも存在し、折込部分とかみこみ部分で殆ど特徴の差が無い為、ハンドラクラフトによる検査は難しい．（図２参照）

(ii) また、材質が柔らかく撮像した際の輝度ムラが発生する為、一般的なカメラと同方向からの光の照射では検査は難しい．

図２　折込部分

３．対策

２点の対策を下記する．

(i) YOLO V8 による物体検出 AI を採用．
定量的なハンドクラフトのソフトを使用するのではなく、物体検出 AI を使用し、人の感覚に近い検査を行うことでかみこみ部分のみを判別し検査することが可能．

(ii) カメラと逆方向より照明を透過させる透過照明配置を採用．
透過照明配置により、パッケージフィルム及び商品の透過情報のみの画像とすることで、パッケージフィルムの変形による輝度ムラの影響なく、検査することが可能．

４．まとめと今後

本稿では、食品・日用品メーカーが抱える問題点かみこみの自動検査装置である、かみこみ検査装置を紹介した．今後も世の中のメーカーの抱える問題点を調査し新たな検査装置を開発していく．

ジョジョの奇妙な冒険第二部の音象徴

中村　剛士[1]　元浪 裕[1]　吉兼 利浩[1]
[1] 中部大学

1　はじめに

オノマトペは，ある特定の動作や心情等を表現する言葉として活用される．篠原ら [1] は，オノマトペに焦点を当てて音象徴に関する報告を行っている．音象徴とは，特定の音が特定のイメージを喚起する事象として認知されている [2, 3]．しかしながら，音象徴の全容解明は未だされていない．本研究では，“ジョジョの奇妙な冒険”(以後，JOJO) の第二部に登場するオノマトペを事例として調査を行い，音象徴の一端を明らかにする．

我々の研究の最終目的は音象徴の全容解明であり，多様な音象徴事例を収集し，それらの音象徴を解明してボトムアップに全容を明らかにしたいと考えている．そこで本研究では，他の漫画作品とは異なる特異なオノマトペを活用する JOJO について，他の漫画作品との音響的な差異に注目するものとした．本研究では，JOJO らしい音響的な特徴を発見し，“JOJO らしさ” の音象徴仮説を立てることを試みる．今回，JOJO と Manga109[4] のオノマトペを対象にクラス分類を行い，両者を識別する音響的な特徴を調査・分析し，音象徴仮説を立てるものとした．なお，Manga109 とは，学術利用を目的として構築された漫画のデータセットである．

2　音象徴の分析方法

本研究では，中村ら [5] が提案する AI 技術を用いた音象徴分析を採用する．中村らの提案手法の分析の流れは以下のとおりである．

1. 音象徴によってクラス分類可能と思われる事例の収集とデータセット構築
2. データセットの各テキストデータを音響データに変換
3. 機械学習技術を用いた分類器によるクラス分類を実施し，分類精度 (正解率，F 値) を評価
4. 分類精度が一定以上の場合，分類に寄与した音響的な特徴有りと判断し，XAI 技術を用いて分類根拠を分析
5. 音象徴仮説を設定し，主観評価実験によって検証

3　分類実験と分類結果

分類実験は，図 1 に示すとおり，JOJO と Manga109 のクラス間で分類を行った．JOJO のオノマトペデータセットは，JOJO 第二部の漫画作品から抽出した 1,187 個から構成される．一方，Manga109 のオノマトペデータセットは，Manga109 で提供されている日本のプロ漫画家によって描かれた 109 冊の漫画作品から抽出した 237 個のオノマトペから構成される．分類実験では，JOJO のオノマトペデータセットから 237 個のオノマトペを無作為抽出し，それらと Manga109 のオノマトペの間でクラス分類を行った．分類器には図 2 に示す CNN を用いた．無作為抽出と分類実験は合計 5 回行い，5 回の平均正解率と F1 値を求めたところ，平均正解率は.602，平均 F1 値は.603 であった．チャンスレベル.500 に比べ高い値であることから，一定以上の分類精度であると判断した．

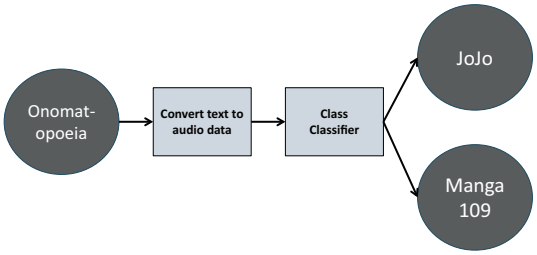


図 1: JOJO と Manga109 のオノマトペの分類

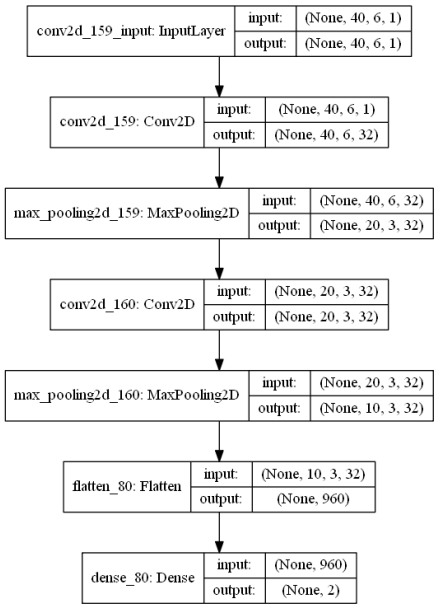


図 2: 本研究で用いた CNN の構造

分類精度が一定以上であることから，XAI 技術の一つである Grad-CAM による分析を行った．Grad-CAM によって獲得されたヒートマップを観察したところ，表

表 1: Grad-CAM のヒートマップ上に現れたモーラの度数

重要モーラ	JOJO	Manga109
/o/ (オ)	52	29
/ba/ (バ)	54	27
/bu/ (ブ)	16	8
/bo/ (ボ)	23	15
/ra/ (ラ)	20	8
/ri/ (リ)	18	5
/ru/ (ル)	26	2
/zju/ (ジュ)	9	0
/gja/ (ギャ)	15	8

1 のような結果が得られた．重要モーラとは，正分類されたオノマトペについてその分類に寄与したと思われるモーラである．表 1 に示す重要モーラについては，JOJO と Manga109 のクラス間で度数の差が大きかったものを示している．ここでは，表 1 に示す重要モーラが “JOJO らしさ” を示す音響的な特徴と考え，これらが JOJO らしさの音象徴の一部であるという仮説を設定した．

4 主観評価実験と評価結果

表 1 に示す重要モーラが，JOJO らしさの音象徴の一部であるという仮説に対して，主観評価実験による検証を行った．主観評価実験については，表 1 に示す重要モーラを含むオノマトペと含まないオノマトペの対を被験者に提示し，どちらが “JOJO らしいか” を回答させる強制選択問題とした．被験者は 32 名で，全員が JOJO の漫画の読書経験またはアニメの視聴経験がある．

表 2 に，主観評価実験において各重要モーラを含むオノマトペを選択回答した被験者数と含まないオノマトペを選択回答した被験者数を示す．表 2 を見て分かるとおり，/ra/，/zju/以外は重要モーラを含む方を選択した被験者が多いことが分かる．とくに，/bu/，/bo/，/gja/ については大きな差があり，破裂音を含む有声阻害音が “JOJO らしさ” の印象を与えている可能性がある．

5 まとめ

本研究では，JOJO に登場するオノマトペには特異なオノマトペが多く，これらのオノマトペに “ジョジョらしさ” の印象を与える音象徴があるのではないかと考え実験を行った．その結果，音象徴に関係すると思われる音響的な特徴として，/bu/，/bo/，/gja/のような破裂音を含む有声阻害音が “JOJO らしさ” の印象を与えている可能性があることを示した．しかしながら，“JOJO らしさ” が音象徴として何を示すものなのか議論は進んでいない．今後は，“JOJO らしさ” という印象が具体的に何を示すものなのか文献調査を進めつつ，明らかにしていきたいと考えている．

表 2: 各重要モーラに対する回答者数の分布

重要モーラ	含む	含まない
/o/ (オ)	**18**	14
/ba/ (バ)	**18**	14
/bu/ (ブ)	**22**	10
/bo/ (ボ)	**20**	12
/ra/ (ラ)	15	**17**
/ri/ (リ)	**19**	13
/ru/ (ル)	**18**	14
/zju/ (ジュ)	16	16
/gja/ (ギャ)	**26**	6

謝辞

本研究は科研費 (22K12232) の助成を受けたものである．

参考文献

[1] 篠原和子, 宇野良子．オノマトペ研究の射程—近づく音と意味, 2013.

[2] John J Ohala. The frequency code underlies the sound-symbolic use of voice pitch. *Sound symbolism*, pp. 325–347, 1995.

[3] Edward Sapir. A study in phonetic symbolism. *Journal of experimental psychology*, Vol. 12, No. 3, p. 225, 1929.

[4] Kiyoharu Aizawa, Azuma Fujimoto, Atsushi Otsubo, Toru Ogawa, Yusuke Matsui, Koki Tsubota, and Hikaru Ikuta. Building a manga dataset “manga109” with annotations for multimedia applications. *IEEE multimedia*, Vol. 27, No. 2, pp. 8–18, 2020.

[5] Tsuyoshi. Nakamura and Takuyu. Miura. Analysis of the acoustic characteristics of takarazuka revue member names. In *Proceedings of FUZZ-IEEE2024*. IEEE, July 2024.

多属性意思決定における決定方略のクラスター分析

竹村和久 [1]　玉利祐樹 [2]　井出野尚 [3]
早稲田大学 [1] 静岡県立大学 [2] 東京理科大学 [3]

１．はじめに

人間は意思決定において、最善の結果を望むが [1), 2), 3), 4)]、しばしば望ましくない結果をもたらす決定をすることがある [5)]。例えば、危険な行動や、健康や生命にリスクがある医療判断を行うことがあり、また集団が全体として望まない選択肢を採用し、集団の利益に反する危険な決定をすることもある [6), 7), 8)]。近年の行動経済学や意思決定理論の多くは、不合理な意思決定に焦点を当てているが [3),9), 10), 11), 12)]、多くの研究は期待効用理論やその変種 [3),4),13),14)]からの逸脱に限られている。本発表では Takemura, et al. (2023)[15)]の方法を基礎として計算機シミュレーション結果をクラスター分析した知見を論じる。

２. 方法

Takemura et. al (2023)[15)]の方法に基づいて、9 つの多様な意思決定方略のすべての可能な組み合わせについて、メルセンヌ・ツイスター法を用いてシミュレーションを行った。その結果、複数の属性からなる選択肢の集合が作成された。各属性の値は 1 から 1000 までの整数をとり、その値は一様乱数発生器を用いて生成した。また、各属性の重要度は 0 から 1 までの実数で、一様乱数を用いて生成した。 多属性意思決定課題を定式化するために、第 1 段階から第 2 段階までの選択肢の数を 3 つ以上になることも考慮して、意思決定開始時の選択肢の数を 5、8、10 の 3 水準とした。同様に、各決定課題における優位な選択肢の有無を考慮しながら、属性数も 3、5、8 の 3 水準に設定した。属性の重要度は、高分散と低分散の設定により分岐する 2 種類の作成方法を用いて、ランダムに生成し適用した。選択肢数（3 水準）×属性数（3 水準）×重要度の分散（2 水準）×優位選択肢の有無（2 水準）の計 36 条件毎に 1 万個の多属性意思決定課題を作成した。第一段階では、連結型（CON）、分離型（DIS）、EBA 型（Elimination-by-aspect）、辞書編纂型（LEX）、半順序的辞書編纂型（LEX-S）の 5 種類の方略を使用した。また、単一方略の決定は、選択肢を絞らずに一つの方略を用いて行った。第 2 段階では、9 つの方略を使用した。CON、DIS、EBA、LEX、LEX-S、WAD、EQW（等加重加算型）、加算差型（ADF）、勝率最大化型（MCD）である。そのため、45 通りの方略の組み合わせをシミュレーションした。これらのシミュレーションから、各方略で定義された平均的な基本情報処理量（EIP）と相対的正確さ（Relative accuracy; RA）、期待値指標における最良選択率と最悪選択率を算出した。決定方略間の特徴を検討するための指標を作成した。作成した指標は、Reference とする決定方略と Target の決定方略に関して、RA の比、EIP の比、選択の一致率、トレードオフ率であった。基本的に Reference を加重加算型とした。なお、EIP に関しては、シミュレーションの条件（選択肢数、属性数、ドミナンスの有無、重要度の分散の高低）毎に、最大の EIP で基準化した。また、RA の比、選択の一致率、トレードオフ率に関して、Target 方略の基準化 EIP で除した指標も作成した。各指標の定義を下記に示した。

RA の比

$$r_{RA}(Target, Reference) = \frac{EV_{Target} - EV_{Random}}{EV_{Reference} - EV_{Random}} \quad (1)$$

ただし、EV は決定方略が採択した選択肢の期待値である。また、$Random$ は、ランダムに選択をする決定方略である。

EIP の比

$$r_{EIP}(Target, Reference) = \frac{EIP_{Target}}{EIP_{Reference}} \quad (2)$$

選択の一致率

$$r_{match}(Target, Reference) = \frac{1}{N}\sum_{i=1}^{N} I\left(X_i^{Target} = X_i^{Referece}\right) \quad (3)$$

ただし、Nはシミュレーションの試行数、$I()$は指示関数、X_i^kは決定方略kが試行iで採択した選択肢である。

トレードオフ率

$$r_{tradeoff}(Target, Reference) = \frac{1}{N}\sum_{i=1}^{N} I\left(\left|\sum_{j=1}^{M} sgn\left(x_{ij}^{Target} - x_{ij}^{Referece}\right)\right| \neq M\right) \quad (4)$$

ただし、$sgn(\cdot)$は符号関数、Mは属性数、x_{ij}^kは決定方略kが試行iで採択した選択肢の属性jの属性値である。決定方略間の関係を探索的に検討するために、階層的クラスター分析を行った。変数は、Reference の決定方略と Target の決定方略に関して、相対的正確さの比、EIP の比、選択の一致率、トレードオフ率の四つを用いた。距離はユークリッド距離を仮定し、変数の標準化を行ってから距離行列を求めた。クラスターの形成法にはウォード法を用いた。

３. 結果と考察

Reference の決定方略が、CON、WAD、BAD の時の、デンドログラムを以下に示した。基本的な傾向として、1 段階目の決定方略か 2 段階目の決定方略でクラスターを形成がされた。Reference が CON の時に関して、Target 方略は CON + DIS、DIS + CON とクラスターを形成していた。Reference が WAD の時に関して、Target 方略は CON が DIS + WAD、DIS + ADF とクラスターを形成していた。Reference が BAD の時に関しては、DIS、BAD、RAN を含むクラスターと、それ以外のクラスターが形成された。

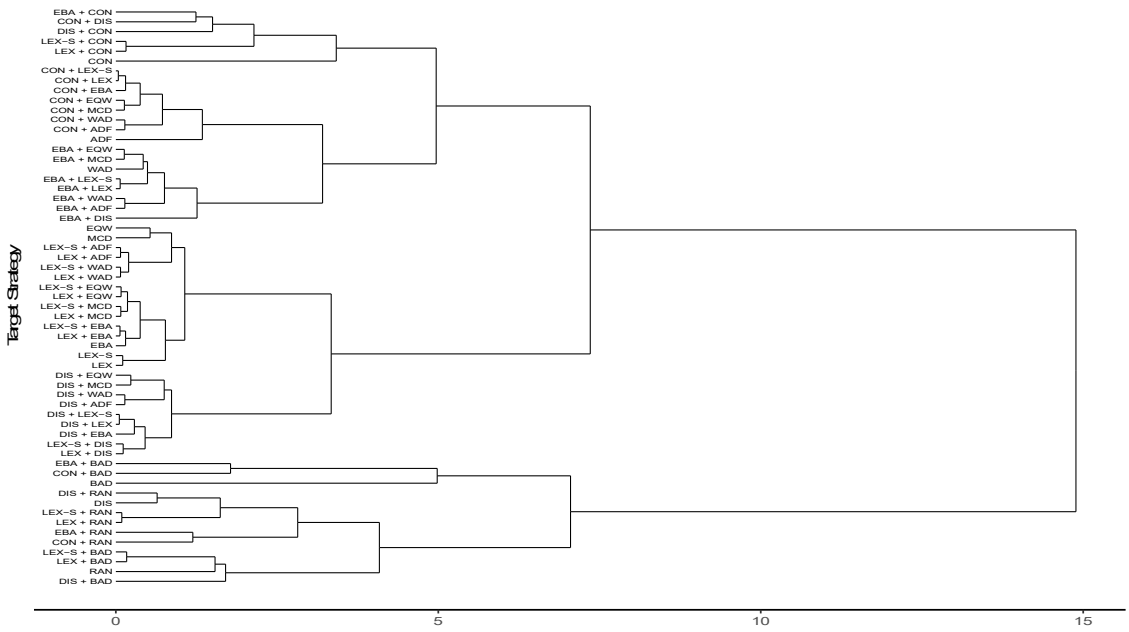
４． 結論

本発表では Takemura, et al. (2023)[15]の方法を基礎として計算機シミュレーション結果をクラスター分析した知見を示した。本研究結果から、何を基準にするかによってクラスターが分かれることがわかった。ただし、加重加算型を基準におくと、第一段階目の決定方略によってクラスターが形成されること、DIS のような分離型は、LEX のような辞書編型方略とパターンが分かれることが示された。DIS は最良選択が少なく最悪選択が比較的多く [16]、LEX はその逆であり、その意味でもパターンが異なっている。

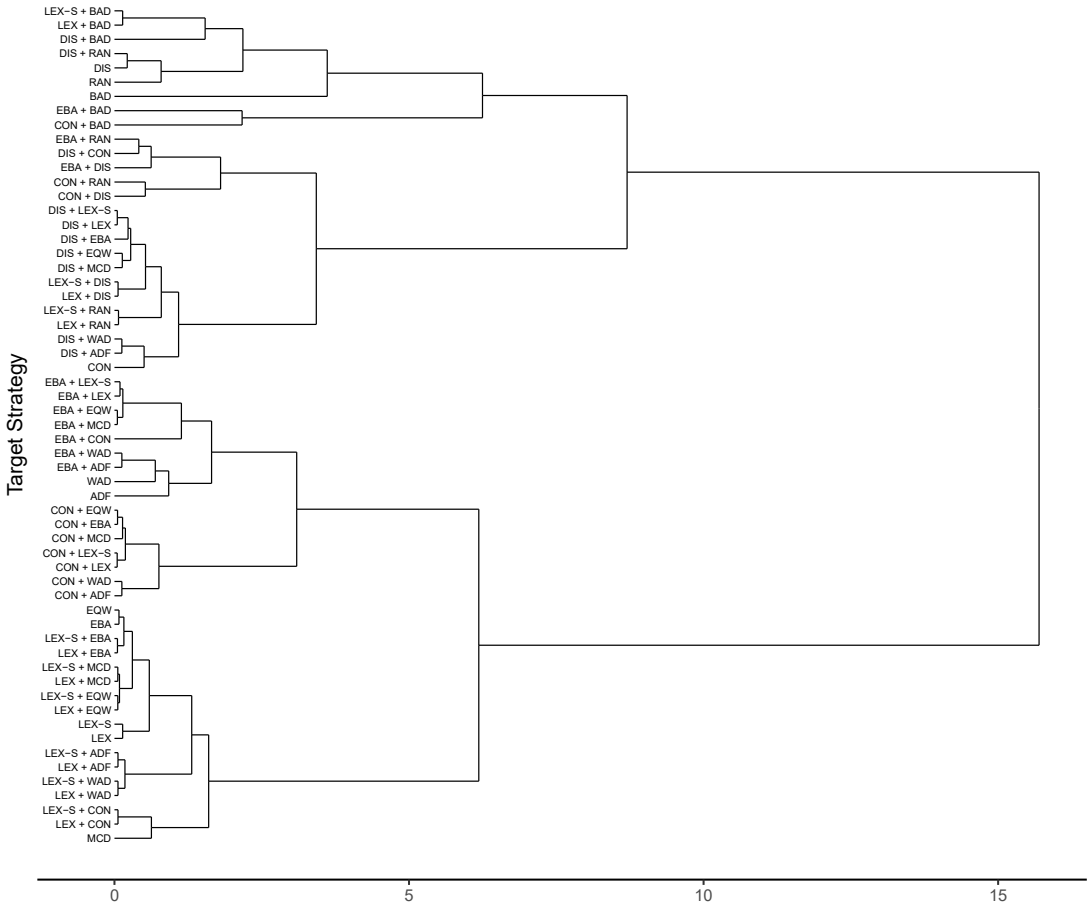
参考文献

1) Hertwig, R., & Grüne-Yanoff, T. (2017). Nudging and boosting: Steering or empowering good decisions. *Perspectives on Psychological Science*, *12*(6), 973/986.
2) Summerfield, C., & Tsetsos, K. (2015). Do humans make good decisions? *Trends in cognitive sciences*, *19*(1), 27–34.
3) Summerfield, C., & Tsetsos, K, (2020). Rationality and efficiency in human decision-making. *The Cognitive Neurosciences VII*, M. Gazzaniga, Ed. MIT Press, 427/438
4) Takemura, K., (2021a). *Behavioral decision theory: Psycho logical and mathematical descriptions of human choice behavior* (2nd ed.). Tokyo: Springer Japan.
5) Takemura, K. (2021b). *Escaping from bad decisions: A behavioral decision-theoretic perspective*. Academic Press.
6) Gigerenzer, G., Todd, P.M., & ABC Research Group (1999). *Simple heuristics that make us smart*, Oxford University Press, USA.
7) Janis, I.L. (1972). *Victims of groupthink*, Houghton Mifflin.
8) Janis, I.L. (1982). *Groupthink: Psychological studies of policy decisions and fiascoes* (2nd ed.), Houghton Mifflins.
9) Bault, N., & Rusconi, E. (2020). The art of influencing consumer choices: a reflection on recent advances in decision neuroscience. *Frontiers in Psychology*, 3009.
10) Trueblood, J.S., Brown, S.D., & Heathcote, A. (2014). The multiattribute linear ballistic accumulator model of context effects in multialternative choice. *Psychological review*, *121*(2), 179.
11) Tsetsos, K., & Chater, N. (2012). Usher, M, Salience driven value integration explains decision biases and preference reversal. *Proceedings of the National Academy of Sciences*, *109*(24), 9659-9664.
12) Tsetsos, K., Moran, R., Moreland, J., Chater, N., Usher, M., & Summerfield, C. (2016). Economic irrationality is optimal during noisy decision making. *Proceedings of the National Academy of Sciences*, *113*(11), 3102-3107.
13) Brandstätter, E., Gigerenzer, G., & Hertwig, R. (2006). The priority heuristic: making choices without trade-offs, *Psychological review*, *113*(2), 409-432.
14) Gigerenzer, G., Reb, J., & Luan, S. (2022). Smart heuristics for individuals, teams, and organizations. *Annual Review of Organizational Psychology and Organizational Behavior*, *9*, 171-198.
15) Takemura, K., Tamari, Y., and Ideno, T. (2023). Avoiding the Worst Decisions: A Simulation and Experiment. *Mathematics*, *11*(5), 1165; https://doi.org/10.3390/math11051165.
16) 竹村和久・玉利祐樹・井出野尚　（2024）多属性意思決定における決定方略の数理的性質と計算機シミュレーション：パレート最適の観点から　日本行動計量学会第 52 回大会発表論文抄録集.

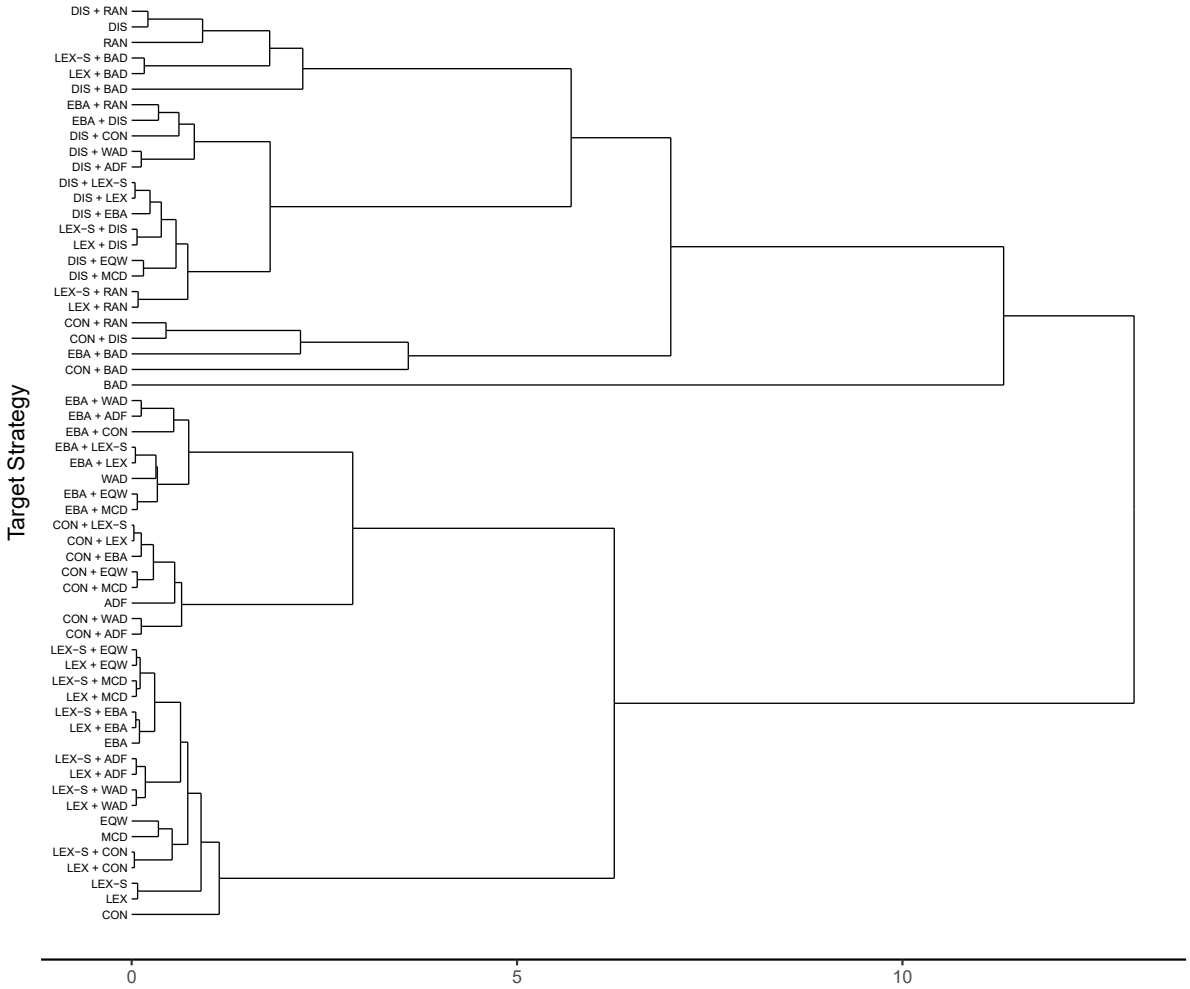
Reference strategy: CON



Reference strategy: WAD



Reference strategy: BAD



パルス列の処理における Attention 機構と SNN の学習コスト比較

大須賀 翼　高瀬 治彦　北 英彦
三重大学

1　はじめに

近年，さまざまな情報処理を行うモデルとして，深層学習が注目を集めている。深層学習の適用範囲は画像から始まり，言語，時系列情報へと広がり続けている。時系列情報は，時々刻々と変化する情報であり，自然言語処理・音声情報処理などの分野で必要とされる。

一般的な深層学習のモデルでは，時系列情報を扱うために，RNN (Recurrent Neural Network) など特殊な構成を導入している [1]。RNN は，階層型 NN (Neural Network) に再帰結合を導入したものである。これは，再帰処理の時間間隔内で生じる時間変化は扱うことができないが，言語のような記号列の取り扱いを可能にした。さらに，再帰結合部に LSTM (Long-Short Term Memory) が導入され性能が向上した。加えて，Attention 機構 (以下 Attention と略す) が導入され，Transformer 機構と組み合わせることで，近年の自然言語処理技術などの革新的な性能向上をもたらした [2]。

それとは別に，脳細胞の動的特性に着想を得たスパイキングニューロンを用いた SNN (Spiking Neural Network) も古くから，時系列信号を処理できる NN として注目されてきた [3]。SNN はその入出力としてパルス列を用いる。これは，時間変化するアナログ値という意味の時系列信号ではないが，PDM (Pulse-Density Modulation) 等の手法により，このような情報の取り扱いも可能である。

本研究では，時系列 (パルス列) の情報を処理するシステムとして，Attention と SNN に着目し，その比較を行う。特に，学習コストを比較し，それぞれの長所と短所を明らかにすることを目標とする。これは，Attention と SNN の使い分けの指針を定めることに貢献するだろう。

2　時系列を処理するニューラルネットワーク

この章では，Attention と SNN についてそれぞれ簡単に説明する。

2.1　Attention 付き RNN

Bahdanau らは，機械翻訳のための拡張した RNN のモデルを提案した [4]。このモデルは，式 (1) に示す長さ T_x の入力系列 $\boldsymbol{x}$ をコンテクストベクトル $\boldsymbol{c}$ へと変換し，それをもとに出力系列を生成する。

$$\boldsymbol{x} = (x_1, x_2, \cdots, x_{T_x}) \tag{1}$$

$\boldsymbol{c}$ は，式 (2)∼(5) に従い求める。なお，文献 [4] では，機械翻訳を想定して，過去の出力系列も用いて $\boldsymbol{c}$ を求めているが，過去の出力系列を参照しない形式 (self-attention) を示す。

$$h_t = f\left(x_t, h_{t-1}\right) \tag{2}$$

$$c_i = \sum_{j=1}^{T_x} \alpha_{ij} h_j \tag{3}$$

$$\alpha_{ij} = \frac{\exp e_{ij}}{\sum_{k=1}^{T_x} \exp e_{ik}} \tag{4}$$

$$\boldsymbol{e} = \boldsymbol{W}\boldsymbol{h} \tag{5}$$

ここで，h_t は時刻 t までの入力による RNN の隠れ状態を，f は LSTM を，$\boldsymbol{W}$ は Attention のパラメータ行列を意味する。このようにして得られた $\boldsymbol{c}$ を，変換器 g に渡すことで，最終的な出力を得る。一般には，この部分に Transformer 機構に渡すことで，出力系列を生成し，系列変換器として機能するようにする。また，パターン分類等に用いる場合は，この部分に階層型 NN を適用する。

これらの概略を図 1 に示す。LSTM の部分は，入力 $\boldsymbol{x_t}$ と前時刻の状態 $\boldsymbol{h_{t-1}}$ を受け取り現時刻の状態 $\boldsymbol{h_t}$ を出力するユニットを，時間方向に展開して表記している。なお文献 [4] では，LSTM 部に双方向 LSTM を用いるモデルも示されているが，概略は変わらない。

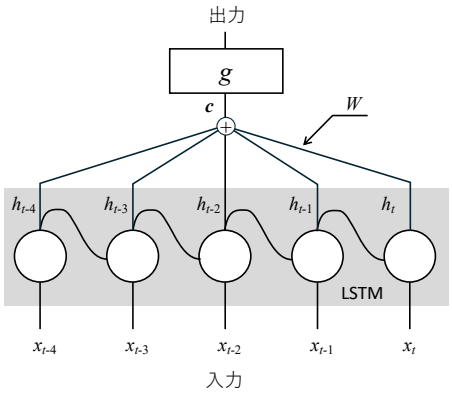


図 1: Attention の概略

この学習は，実際の出力と教師信号により求められた損失を最小化するように，誤差逆伝搬法に基づき f, $\boldsymbol{W}$ および g を繰り返し調整する。

2.2 スパイキングニューラルネットワーク

SNN にはさまざまなモデルがあるが，本稿では Shrestha らによる SLAYER[5] を取り上げる。このモデルは，パルス列からパルス列への変換を学習できる階層型のモデルおよびその学習法である (図 2)。

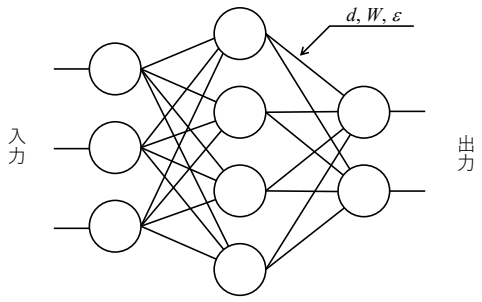


図 2: SNN の概略

パルス列 $s(t)$ は，ディラックのデルタ関数を用いて，式 (6) のように表現する。

$$s(t) = \sum_f \delta\left(t - t^{(f)}\right) \tag{6}$$

ここで $t^{(f)}$ は，系列の f 番目のパルスの時刻を意味する。このモデルの動作を式 (7)∼(9) に示す。

$$\boldsymbol{a}^{(l)}(t) = \left(\epsilon_d * \boldsymbol{s}^{(l)}\right)(t) \tag{7}$$

$$\boldsymbol{u}^{(l+1)}(t) = \boldsymbol{W}^{(l)}\boldsymbol{a}^{(l)}(t) + \left(\nu * \boldsymbol{s}^{(l+1)}\right)(t) \tag{8}$$

$$\boldsymbol{s}^{(l+1)}(t) = f_s\left(\boldsymbol{u}^{(l+1)}(t)\right) \tag{9}$$

ここで，$\boldsymbol{s}^{(l)}$ は第 l 層への入力スパイク列を，$\boldsymbol{a}^{(l)}(t)$ は第 l 層の時刻 t における内部状態を，$\boldsymbol{W}^{(l)}$ は第 l 層の入力側の結合荷重を，ϵ_d は d の遅延およびスパイク応答関数 ϵ を適用する操作を，ν は不応関数を適用する操作を，f_s はしきい値判定による内部状態からパルス列への変換操作を意味する。ネットワークへの入力は $\boldsymbol{s}^{(0)}$ に与え，最終層の出力 $\boldsymbol{s}^{(n_l)}$ をネットワークの出力とする。

この学習は，出力スパイク列と教師スパイク列により求められた損失を最小化するように，誤差逆伝搬法に基づき $\boldsymbol{W}$ および $\boldsymbol{d}$ を繰り返し調整する。

3 実験

前の章に示したように，Attention，SNN のいずれも損失の勾配に基づいて多数のパラメータを繰り返し調整することで学習する。そのため，多量の学習データ・多数の学習回数が必要となる。しかし，Attention，SNN では，モデルの構成が大きく異なるため，必要な学習データ・学習回数の傾向が異なる可能性がある。

この章では，同一のデータセットを用いて学習データ量を変えながら Attention および SNN を学習し，その学習回数・精度を比較する。

3.1 実験条件

学習データは，UCR の時系列分類問題のアーカイブ [6] から，1 次元の系列の 2 ∼ 3 分類のデータセットとして，Power Cons (以下 PC と略す)，UMD および Large Kitchen Appliances (以下 LKA と略す) を用いた。1 次元のデータセットを用いたのは，時系列情報処理の能力に着目して議論するために，入力の空間的な広がりを排除するためである。系列の例を図 3， 4 および 5 に示す。

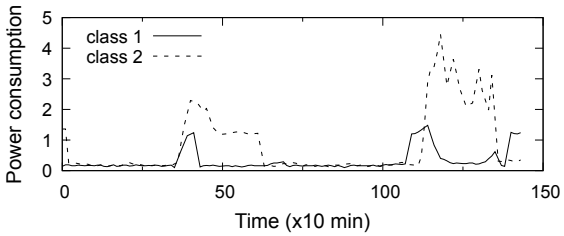


図 3: PC データセットの系列例

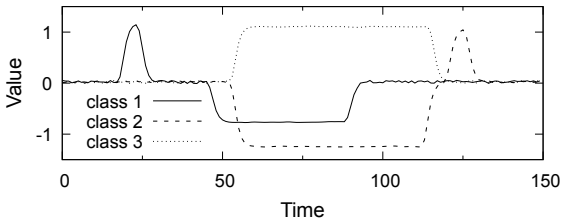


図 4: UMD データセットの系列例

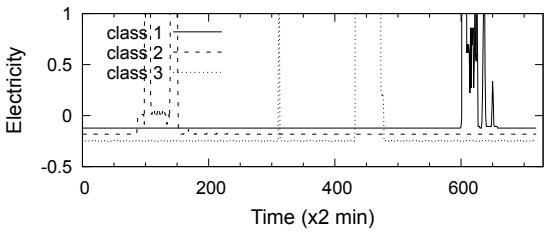


図 5: LKA データセットの系列例

なお，入力信号は PDM(最小パルス間隔は 1) によりパルス列に変換して使用した。また各データセットに

おいて，各クラスの系列数が同数となるように系列を間引いて使用した。いずれのデータセットも，ほぼ学習用とテスト用が提供されていたので，それぞれ学習用・評価用 (学習終了判定および精度を求めるために使用) として使用した。ただし，UMD データセットについては，テスト用の方が学習用より多かったので，テスト用と学習用を入れ替えて用いた。実験では，学習対象の系列数が多いときと少ない時を比較するため，元のデータセット毎に系列数が異なる 2 種の学習用データセット (多および少) を用意した。各データセットの概略を表 1 に示す。

表 1: データセット概要

名前	クラス数	系列長	系列数 多	系列数 少
PC	2	144	180	10
UMD	3	150	144	15
LKA	3	720	375	15

モデルの大きさに関わるパラメータは，両モデルの学習対象のパラメータ数がおおむね同じになるように定めた。Attention では，f は隠れ状態 4 次元の双方向 LSTM ネットワーク、g の部分は，線形 2 層全結合のネットワークを用いた。SNN では、2 分類の場合は 164 個，3 分類の場合は 145 個の隠れ層ユニットをもつ 3 層構造のネットワークを用いた。SNN の出力計算は，入力系列と同じ時間間隔で行った。また、SNN の出力はパルス列であるため、パルス数エンコードを出力・教師に対して行った。具体的には、学習時はクラス数分の出力を用意し、正解クラスに対して出力パルス数が 100 個、そうでないものの出力パルス数が 10 個となるように学習した。また分類時は、最も出力パルス数が多い出力に対応するクラスを結果とした。その他のハイパーパラメータは，予備実験により安定して学習に成功する値を探し用いた。学習は，予備実験で学習に成功した回数の 5 倍を打ち切り回数として，評価用のパターンに対する損失が下げ止まったときに終了した。

学習は，モデル (Attention，SNN)・パターンセット (3 種)・学習系列数 (多，少) の各組み合わせについて，乱数系列を変化させ 10 回行った。

3.2 精度の比較

学習終了後のネットワークについて，評価用データに対する認識精度を図 6，7，8 に示す。いずれの図も，モデル・学習系列数の各組み合わせに対して得られた精度を，それぞれの列にプロットした。図 6，7，8 は，それぞれ PC，UMD，LKA に対する結果である。

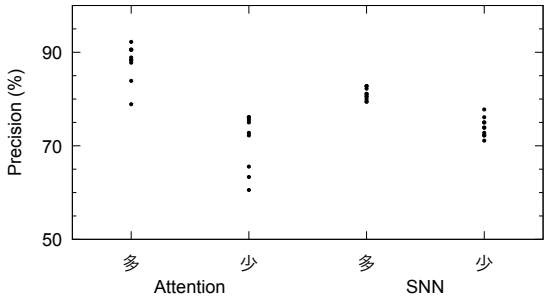


図 6: PC に対する精度

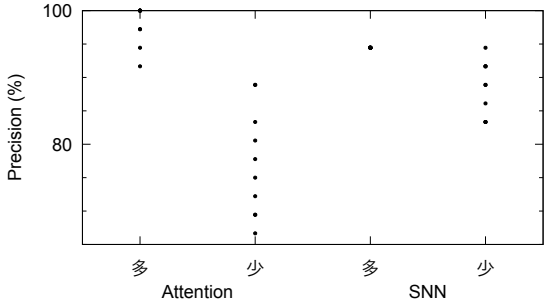


図 7: UMD に対する精度

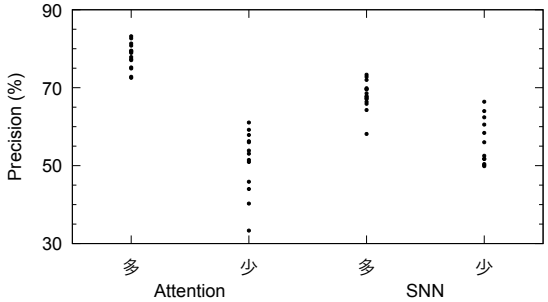


図 8: LKA に対する精度

まず，データ量が多いときのモデルの違いによる精度の違いに着目する。いずれのデータセットでも，データ量が多いときには，Attention の方が精度が高い傾向にあった。これは，データ量が多いときの認識性能は Attention の方が高いことを示唆している。

次に，データ量が減ったときの，各モデルの精度低下に着目する。いずれのデータセットにおいても，Attention ではデータ量が少ないときの精度は，データ量が多いときの最小値を下回った。それに対し，SNN においては，データ量が多いときと少ないときの精度の差は，Attention の場合と比べ小さかった。これは，データ量が限定されている状況下では，Attention の認識性能は SNN にくらべ悪化しやすいことを意味する。

3.3 学習回数の比較

ニューラルネットワークの実際の学習時間は，実装方法，使用ハードウェア，学習モデル (種類・規模) および学習パターン数に主に依存する。これらのうち，実装方法，使用ハードウェアについては，その進歩により学習時間が短縮される。しかし，これらの進歩だけでは，学習回数は減少しない。また，学習パターン数は，計算時間に対して，おおむね比例した影響を及ぼす。これらは，学習回数がモデルに固有な学習速度を示すことを示唆している。そのため，本稿でのモデルの比較では，学習時間ではなく学習回数で主に議論する。

学習回数 (epoch 数) を図 9，10，11 に示す。いずれの図も，モデル・学習系列数の各組み合わせに対して得られた精度を，それぞれの列にプロットした。図 9，10，11 は，それぞれ PC，UMD，LKA に対する結果である。

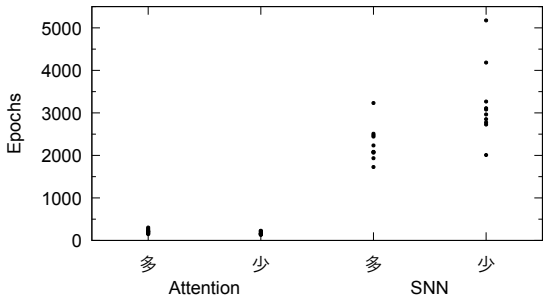


図 9: PC の学習回数

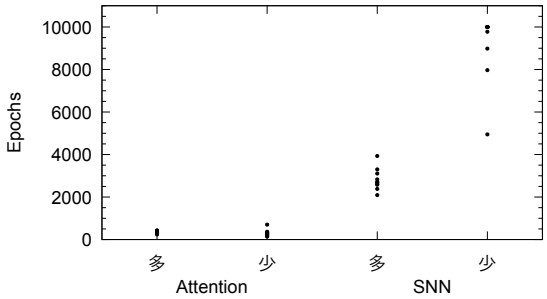


図 10: UMD の学習回数

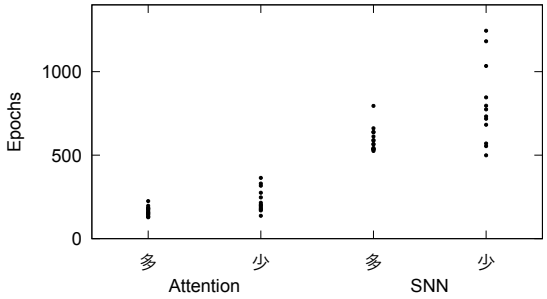


図 11: LKA の学習回数

なお参考のため，今回の実験での実行時間を見積もれるように，各条件での 1 エポックあたりの平均学習時間を求めた (表 2)。表中,「倍率」は Attention の計算時間を 1.0 としたときの，SNN の計算時間を表したものである。データセットが PC や UMD の場合は Attention の方が SNN と比べ，計算時間がやや短い。その反面,LKA では SNN が半分近くの時間で計算できており，単純には比較できない。ただし，学習回数と併せて考えると Attention の方が計算時間は短くなるため，現在の実装・ハードウェアにおいて実行時間では Attention が有利である。

表 2: 1 エポックあたりの平均学習時間

データセット		Attention	SNN	倍率
PC	多	690	718	1.04
	少	387	425	1.10
UMD	多	476	494	1.04
	少	248	268	1.08
LKA	多	3,313	1,435	0.433
	少	1,270	737	0.580

(ms)

まず，モデルの違いによる学習回数の違いに着目する。いずれのデータセットでも，Attention の方が学習回数が少なかった。これより，Attention では，LSTM, Attention など，異なるシステムが混在しているが，これにより学習回数が増加することはなく，効率よく学習できるといえる。

次に，データ量の違いによる学習回数の変化について着目する。いずれのモデルでも，データ量が少なくなることで，学習回数が増加する傾向にあった。なお，データ量が減った場合は，1 エポックあたりの平均学習時間は減少しているため，学習時間としては増加しなかった。あくまでも，学習終了までの繰返し回数が多くなるという意味である。各モデルでの傾向は，以下のとおりであった。Attention では，その増加量は少なかった。これは，データ量は学習回数に必ずしも影響しないことを意味する。それに対し，SNN では，学習回数が倍以上に増加する場合があった。これは，データ量が少ないときには，学習が困難になることを意味する。

3.4 考察

以上の結果より，Attention，SNN においてデータ量の観点から，異なる性質が得られた。Attention では，データ量が多いときには分類性能が高かったが，デー

タ量が減った時の性能劣化はSNNと比べ大きい。しかし，データ量の変化は，学習回数に対して大きな影響を与えない。SNNでは，データ量が多くても必ずしも分類性能は高くないが，データ量が減った時，学習回数が増大する代わりに性能劣化はAttentionと比べ小さい。これらより，一方的にAttention，SNNのどちらかが良いと言うことはなく，状況に応じた使い分けが必要であることが分かった。

本稿では，3種の簡単な波形の分類を題材に，データ量の違いがAttention，SNN各モデルに与える影響について簡単に調査した。しかし，事例が十分でないことと，定性的な分析がされていないため，今後のさらなる検討が必要である。

4 まとめ

本研究では，時系列(パルス列)の情報を処理するシステムとして，AttentionとSNNに着目し，学習コストの観点から比較を行った。簡単な時系列信号の分類を行った結果，データ量が多いときには，AttentionがSNNより高い性能を示した。また，データ量が減ることで，Attentionでは認識性能について，SNNでは学習回数について悪化した。この結果は，一方的にAttention，SNNのどちらかが良いと言うことはなく，状況に応じた使い分けが必要であることを示している。

今後は，広範な事例について検討するとともに，定性的な分析を行う。

参考文献

[1] Ian Goodfellow et al., “深層学習”, KADOKAWA, 2018.

[2] Ashish Vaswani et al., “Attention is All You Need”, Advances in Neural Information Processing Systems, Vol. 30, pp. 6000–6010, 2017.

[3] Wolfgang Maass and Christopher M. Bishop, “Pulsed Neural Networks”, The MIT Press, 2001.

[4] Dzmitry Bahdanau et al., “Neural Machine Translation by Jointly Learning to Align and Translate”, arXiv preprint arXiv:1409.0473, 2014.

[5] Sumit Bam Shrestha and Garrick Orchard, “SLAYER: Spike Layer Error Reassignment in Time”, Proceedings of the 32nd International Conference on Neural Information Processing Systems , pp. 1419–1428, 2018.

[6] Hoang Anh Dau et al., “The UCR Time Series Classification Archive”, https://www.cs.ucr.edu/~eamonn/time_series_data_2018/ (2019)

ブロックチェーンを用いた塾講師評価システムの提案と実装

岡田 蘭丸[1]　竹本 修[2]　野崎 佑典[2] 吉川 雅弥[2]
[1] 名城大学

1　はじめに

近年，教育の質を向上させるために，塾や家庭教師の選択が重要な課題となっている．特に，塾に通いたい生徒やその保護者は，事前に講師の評価を知ることでより適切な選択ができるようになる．しかし，従来の評価システムにはいくつかの問題が存在する．評価の信頼性や透明性の欠如，また，プライバシーの観点から個人情報が適切に保護されていないことが挙げられる [1][2].

そこで本研究では，これらの課題を解決するためにブロックチェーン技術を活用した新たな塾講師評価システムを提案する．このシステムは，講師の評価を透明かつ改ざん不可能な形で記録し，利用者が安心して評価情報を参照できる環境を提供する．これにより，生徒は信頼性の高い情報に基づいて講師を選択できるようになり，教育の質向上に寄与することが期待される．

2　関連技術

2.1　ブロックチェーン

ブロックチェーンとは，サトシ・ナカモトにより考案された分散型台帳技術 [3] であり，暗号資産の一種である Bitcoin を実装する目的で考案された分散型ネットワーク技術の一つである．ブロックと呼ばれる 1 単位のデータを鎖のように連結していくことからブロックチェーンと呼ばれる．ブロックのハッシュ値を次のブロックに格納することで，あるブロックを改ざんした場合，以降のブロックすべてのハッシュ値が変わってしまうため改ざんの検知が容易な構造を持つ．コンセンサスアルゴリズムと組み合わせることで，現実的に改ざんが不可能なデータベースを構築することができる．この連結されたデータを，P2P 技術を用いて多数の参加者が通信し合い同期することで，中央サーバやその管理者なしに，データ内容の正当性と一貫性を確保することが可能になる．

2.2　スマートコントラクト

スマートコントラクトとは，ブロックチェーン技術を活用した自動化プログラムで，条件が満たされた際に自動実行される．信頼性が高く，改ざん耐性を持つ．そのプログラムが実行されるとその記録もブロックチェーンに格納されるため，一連の動作の透明性を確保することができる．また，P2P ネットワーク上で実行されるため，単一障害点となるものは基本的に存在しない．この特性により，第三者機関を介さずに，任意の契約を自動で実行できると言われている．

2.3　Ethereum

Ethereum とは，分散型アプリケーション (DApps) やスマートコントラクトを構築するためのオープンソースのブロックチェーンプラットフォームであり，Vitalik Buterin によって考案され，2013 年に正式発表された [4]．また，Ethereum のスマートコントラクトを開発するための統合開発環境（IDE）の一つに Remix IDE がある．これは，ブラウザベースで動作し，主に Solidity というプログラミング言語を使用してスマートコントラクトを作成，コンパイル，デプロイすることができる．

3　提案手法

提案手法では，Remix IDE を用いて塾講師評価システムを Solidity で構築し，Sepolia テストネットワークへのデプロイを行う．評価システムには以下の機能を持つ関数を各々記述した．提案手法の概要を図 1 に示す．

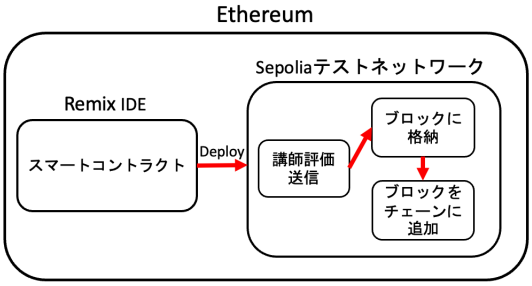


図 1: 提案手法概要

(i) 評価送信 (講師のアドレス・評価値を入力)
(ii) 評価をした人 (生徒) の直近一件の評価値参照
(iii) 評価を受けた人 (講師) の直近一件の評価値参照
(iv) 評価を受けた人 (講師) の情報照会 (合計スコア・評価を受けた合計回数・合計評価平均値)

また，塾講師評価の平均値更新アルゴリズムに，オンラインアルゴリズムを用いた．オンラインアルゴリズムは，入力データ全体を最初から利用可能にすることなく，逐次的にデータを処理するアルゴリズムである．データを逐次的に処理するため，計算資源の使用が分散でき，ピーク時の負荷を軽減できる．これにより，計算資源の効率的利用が可能になり，学期開始時や夏季・

冬季講習時の申し込みが集中する時のシステムトラブルを回避できる．

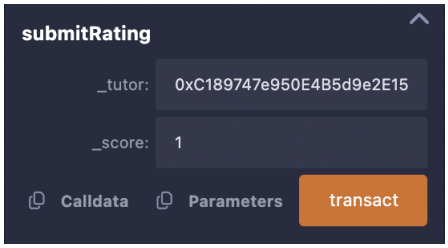


図 2: 評価値送信の様子

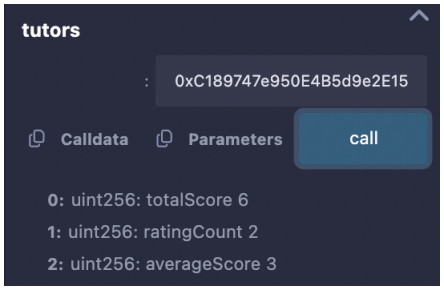


図 3: 講師情報照会の様子

今回，評価値は便宜上 1〜5 までの 5 段階評価とした．また，講師のアドレスと生徒のアドレスは MetaMask アカウントのアドレスをそれぞれ利用した．図 2 に評価値送信の様子を，図 3 に講師情報照会の様子を示す．今回評価値送信は 2 回行った．1 回目の評価値は 1 であり，2 回目の評価値は 5 とした．そのため，図 3 より合計スコアが 1+5=6 であり，合計評価回数は 2，合計評価平均値は 6 ÷ 2=3 となっている．

評価方法として，評価値を変動させた時のガス代とレイテンシ，トランザクション手数料を比較する．

4 評価実験

提案システムの有効性を示すために Chrome Devtools の Performance 機能を用いて，作成した塾講師評価システムの評価値変動処理におけるレイテンシを評価する．またブロックチェーンエクスプローラーである Etherscan を用いて送金処理におけるガス代・トランザクション手数料も測定・比較する．

表 1 に，セキュリティの定性的な評価を示す．従来手法では機密性・完全性，そしてデータの透明性について，データ管理に暗号化が用いられていなかったが，提案手法ではブロックチェーンを用いることでその課題を解決した．これにより，評価の信頼性の担保と，データの透明性の確保を可能にした．

表 1: セキュリティ評価

	機密性・完全性	データの透明性
提案手法	○	○
従来手法 [1][2]	×	×

測定結果を表 2 に示す．評価値とトランザクション手数料，ガス代には僅かであるが比例関係があることが計測できた．しかし， レイテンシに関しては相関関係が見られなかった．これは，レイテンシは評価値の変動ではなく評価値送信時における送金手数料の設定によるものであり，本実験では送金手数料を均一にしたため，変化がなかった．

表 2: 実験結果

評価値	トランザクション手数料	レイテンシ (ms)	ガス代 (wei)
5	0.001265	10.6	6.363
4	0.001238	39.2	6.325
3	0.001238	36.8	6.139
2	0.001170	34.3	5.927
1	0.001129	27.1	5.127

5 まとめ

本研究では，Remix IDE を用いて塾講師評価システムを Solidity で構築し，Sepolia テストネットワークへのデプロイを行い，評価値を変動させた時のガス代とレイテンシ，トランザクション手数料を比較した．今後はプライバシー保護対策として，評価者が実際に講師から指導を受けたことを証明するゼロ知識証明を組み込む予定である．また，今回レイヤー 1 テストネットワークでのデプロイであったが，低コスト・高スケーラビリティを実現するレイヤー 2 テストネットワークでのデプロイも行う予定である．

参考文献

[1] S. Nam, J. Choi: Development of a user evaluation system in virtual reality based on eye-tracking technology. Multimed. Tools Appl. 2023, 82, 21117–21130.

[2] 小森和子: 自動評価システムによる作文評価は教師評価の代用になるのか (2024).

[3] S. Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System (2008).

[4] V. Buterin: A next-generation smart contract and decentralized application platform, Vol. 3, No. 37 (2014).

低遅延軽量暗号 LTLBC の FPGA への実装評価

○野崎　佑典 [1]，吉川　雅弥 [2]
○Yusuke Nozaki[1], Masaya Yoshikawa[2]
[1, 2] 名城大学
[1, 2]Meijo University

Abstract:　リアルタイム処理が要求されるアプリケーションにおけるセキュリティ技術（暗号化技術）として，低遅延軽量暗号が注目されている．これまでにいくつかの低遅延軽量暗号が提案されており，本研究で対象とする LTLBC は 2024 年に提案された最新の低遅延軽量暗号である．一方で，先行研究では Open Cell Library を用いた設計による評価は行われているが，エッジ端末での利用が期待されている FPGA での実装評価は行われていない．そこで本研究では，LTLBC を FPGA に実装しその性能について評価する．

１．はじめに

軽量暗号技術の需要が高まっており，様々な暗号アルゴリズムが提案されている [1]–[6]．また，米国立標準技術研究所 National Institute of Standards and Technology （NIST）では軽量暗号に関する標準化プロジェクト Lightweight Cryptography（LWC [5]）が実施されており，次世代標準暗号として Ascon [6]が選出されている．一方で，LWC では回路規模や安全性などの様々な観点で評価されているが，リアルタイム処理を考慮したレイテンシについては十分に評価されていない．近年，レイテンシに着目した低遅延軽量暗号が注目されており，PRINCE [2]や MANTIS [3]，QARMA [4]をはじめとして様々な暗号技術が提案されている．本研究で対象とする LTLBC [1]は 2024 年に提案された新しい低遅延軽量暗号アルゴリズムである．先行研究では，NanGate 社が公開している 45nm プロセスの Open Cell Library を用いた設計を行い，代表的な低遅延暗号である PRINCE よりも回路規模やレイテンシの観点で優位性を持つことが示されている [1]．しかし，エッジ端末等での利用が期待される Field Programmable Gate Array（FPGA）での実装評価は行われていない．今後の幅広いアプリケーションでの低遅延軽量暗号の利用を検討する上で FPGA 実装における性能評価は重要である．そこで本研究では，LTLBC を FPGA に実装しその性能について定量的に評価する．

２．LTLBC

LTLBC [1]は，ブロック長が 64bit，鍵長が 128bit の SPN 構造を持つブロック暗号である．LTLBC の概要を図 1 に示す．最初に平文と鍵 K_0 との XOR 演算を行い，その後はラウンド関数を繰り返し適用する．このラウンド関数は，主に PermuteBits, MixWord, SubCell で構成し，これらの処理後にはラウンド鍵 RK とラウンド定数 RC との XOR 演算を行う．この処理を 14 回繰り返すことで，暗号文を生成する．ただし，最終ラウンドである 14 ラウンド目では，MixWord を除いた処理を行う．

ラウンド関数の各処理に関して，PermuteBits と MixWord は線形処理を，SubCell は非線形処理を行う．まず，PermuteBits はビット単位での転置処理を行う．次に，MixWord はワード単位での線形処理を行う．また，SubCell は 4bit 単位の S-BOX 表を用いた置換処理を適用する．PermuteBits や MixWord, SubCell の詳細については文献 [1]を参照されたい．

鍵スケジュール部に関して，128bit の秘密鍵 K を 64bit の部分鍵 K_0 と K_1 に分割し，K_1 を Whitening Key として用いている．ラウンド鍵については，K をベースに左ローテーション処理と S-BOX による置換処理，4bit のラウンド定数値（カウンタ値）との XOR 演算を各ラウンドで繰り返すことで生成している．

全体のアルゴリズムの設計に関して，線形層や S-BOX において，論理ゲートの数を削減しつつ遅延を抑え，暗号解析に対する安全性を確保するための様々な工夫が加えられている．そして，NanGate 社の 45nm プロセスの Open Cell Library を用いた評価では，回路規模やレイテンシの観点で，従来の PRINCE [2]や MANTIS [3]，QARMA [4]よりも高い性能を持つことを示している [1]．

３．評価実験

本研究では，実装対象の FPGA として SASEBO-GII 評価ボードを使用し，SASEBO-GII に搭載されている Xilinx Virtex-5 XC5VLX30 に LTLBC を実装した．設計では，ハードウェア記述言語として Verilog HDL を用いて記述し，Xilinx ISE Design Suite 14.7 を使用した．実装に関して，S-BOX は全てテーブル実装し，アーキテクチャに関してはループ実装とアンロールド実装を採用した．実装したループ型アーキ

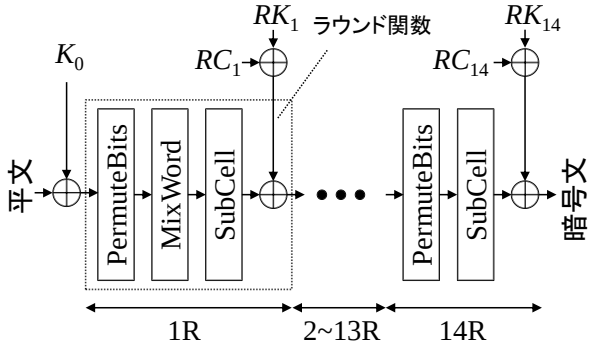


図 1　LTLBC の概要

テクチャを図 2 に示す．また，アンロールド実装は全ての処理を組み合わせ回路で実装した．さらに，評価の比較対象として代表的な低遅延暗号である PRINCE を同様に実装した．

まず，回路規模について比較した結果を表 1 に示す．表 1 の括弧内の roll はループ実装を，unroll はアンロールド実装をそれぞれ示している．表 1 から，ループ実装においては，LTLBC は PRINCE よりも Lookup Table（LUT）数や SLICE 数が少なく小型実装が可能であることが確認できる．一方で，アンロールド実装では PRINCE と比較して LUT 数と SLICE 数がともに増加していることが分かる．

また，低遅延処理を指向するアンロールド実装を対象にレイテンシについても評価した．この評価では ISim の遅延付きシミュレーションを実行し，一回の暗号化に必要な時間を算出した．比較結果を表 2 に示す．表 2 に示す通り，PRINCE の方が遅延が短く，レイテンシの性能が高いことが分かる．先行研究の評価 [1]では，LTLBC の方が遅延が小さいと報告されているが，表 2 の結果から FPGA 実装では PRINCE の方がレイテンシがよいことが確認できる．これは，LTLBC の設計が論理ゲートレベルで最適化されているのに対して，FPGA では LUT や SLICE 単位で実装が行われるため，論理ゲートレベルの最適化が十分に機能しなかったためだと考えられる．

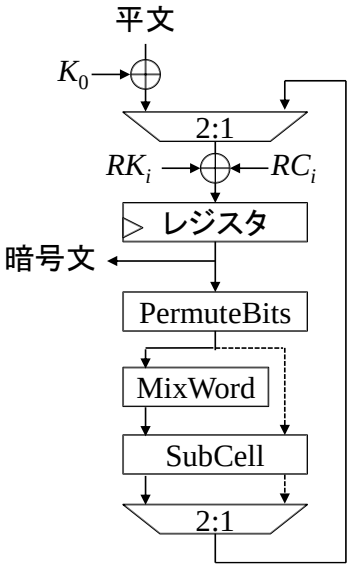


図 2　実装した LTLBC のループアーキテクチャ

表 1　回路規模の比較

	LUT 数	SLICE 数
LTLBC (roll)	361	178
LTLBC (unroll)	2426	1473
PRINCE (roll)	776	455
PRINCE (unroll)	1575	1223

表 2　レイテンシの評価

	遅延 [ns]
LTLBC (unroll)	1.821
PRINCE (unroll)	1.247

４．まとめ

本研究では，低遅延軽量暗号 LTLBC を FPGA に実装し，その性能について定量的に評価した．その結果，LTLBC はループ実装では PRINCE よりも小型に実装できることを明らかにした．一方で，アンロールド実装では PRINCE よりも回路規模が大きくなることを示した．また，レイテンシにおいても FPGA 実装では PRINCE の方がレイテンシの性能が高いことを明らかにした．

今後は，FPGA 実装においてもレイテンシを向上できるような実装方法について検討を進める予定である．また，安全性に関してサイドチャネル攻撃に対する耐タンパ性についての評価も行う予定である．

謝辞

本研究の一部は，JSPS 科研費 22K17891 の助成を受けたものです．

参考文献

[1] W. Sun, L. Li, and X. Huang, “LTLBC: a low-latency lightweight block cipher for internet of things,” Cluster Computing, pp. 1–12, Springer, 2024.

[2] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavum, M. Knežević, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and T. Yalçin, “PRINCE – A low-latency block cipher for pervasive computing applications,” Proc. of ASIACRYPT 2012, LNCS vol. 7658, pp. 208–225, Springer, Dec. 2012.

[3] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, “The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS,” Proc. CRYPTO 2016, LNCS vol. 9815, pp. 123–153, Springer, Aug. 2016.

[4] R. Avanzi, “The QARMA Block Cipher Family. Almost MDS Matrices Over Rings With Zero Divisors, Nearly Symmetric Even-Mansour Constructions With Non-Involutory Central Rounds, and Search Heuristics for Low-Latency S-Boxes,” IACR Trans. on Symmetric Cryptology, vol. 2017, no. 1, pp. 4–44, 2017.

[5] https://csrc.nist.gov/projects/lightweight-cryptography

[6] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, “Ascon v1.2: Lightweight Authenticated Encryption and Hashing,” Journal of Cryptology, vol. 34, no. 33, pp. 1–42, 2021.

連絡先

野崎佑典
E-mail: 143430019@ccalumni.meijo-u.ac.jp