研究課題名　知能コンピューティングを加速する自己学習型・革新的アーキテクチャ基盤技術の創出

北海道大学・大学院情報科学研究科・教授　本村（もとむら）　真人（まさと）

研究課題番号：18H05288　研究者番号：90574286
キーワード：深層ニューラルネット、ニューロモルフィック、アナログ・インメモリ回路方式

【研究の背景・目的】

深層ニューラルネット(DNN)の勃興により、AI(人工知能)技術とその社会応用が大きく進展しています。AI 技術をより賢く進化させ、より低エネルギーで実現し、将来の超スマート社会を支える「知能コンピューティング」へと発展させていくためには、ソフトウェア技術だけではなく、その基盤となるハードウェア(HW)技術やアーキテクチャ技術の大きな進化が欠かせません。本研究は、DNN 処理を加速する HW エンジンのアーキテクチャ技術を中核として、DNN の隣接領域であり、より脳に近い情報処理を目指したニューロモルフィック HW 分野の最新の知見や研究進展を積極的に結集して、将来の知能コンピューティングを支える革新的アーキテクチャ基盤技術の創出を目指すものです。

【研究の方法】

本研究は、北海道大学・大学院情報科学研究科の集積アーキテクチャ研究室及び集積ナノシステム研究室を中心として行うものです。前者の研究室(研究代表者らのチーム)では、近年、図 1 に示す二値化 DNN と対数量子化 DNN のハードウェアやその学習技術を発表し、大きな注目を集めています。

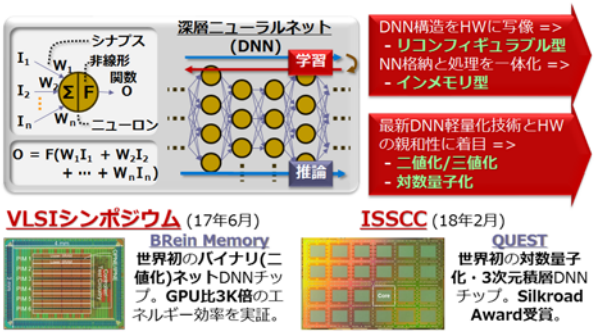

図 1. DNN アクセラレータ技術

一方、後者の研究室(研究分担者・浅井哲也教授らのチーム)では、アナログ回路技術を用いたニューロモルフィック HW や(図 2)、その延長線上で近年注目を集め始めたリザーバコンピューティングの研究を積極的に進めています。この二つの研究室が密に交流し、隣接領域の知見を持ち寄った大きな枠組みで研究活動を進めている点が、北海道大学の本研究体制の大きな特徴です。

これらの既存の研究活動を背景に、基盤(S)の本課題では、特に、1) DNN 向けリコンフィギュラブル

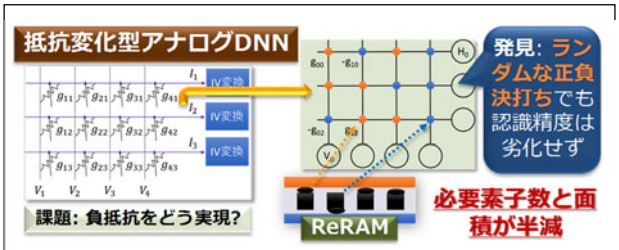

図 2. ニューロモルフィック HW 技術

HW の新たな回路方式、2) DNN-ニューロモルフィック分野融合で生まれる新たな学習方式とその情報処理アーキテクチャ、3) アルゴリズム-回路の協創による高エネルギー効率 HW 方式(アナログ回路技術、インメモリ回路技術など)、の三つの技術構築を中核に据えて研究を進めます。

【期待される成果と意義】

シミュレーション等の机上評価だけで終わらせることなく、アルゴリズム研究から実証 HW の試作・評価まで、トータルな研究を遂行します。最終的には、DNN とニューロモルフィック HW に立脚し、将来の知能コンピューティングを支える自己学習型・機能獲得型リコンフィギュラブル HW プラットフォームの提案に結実させることを狙います。

【当該研究課題と関連の深い論文・著書】

- Ando K., et.al., "BRein memory: a 13-layer 4.2 K neuron/0.8M synapse binary/ternary reconfigurable in-memory deep neural network accelerator in 65 nm CMOS," 2017 Symposium on VLSI Circuits [VLSI]. (Jun. 5-8, 2017).
- Ueyoshi K., et.al., "QUEST: a 7.49-TOPS multi-purpose log-quantized DNN inference engine stacked on 96MB 3D SRAM using inductive-coupling technology in 40nm CMOS," IEEE International Solid-State Circuits Conference [ISSCC] (Feb. 12-14, 2018).

【研究期間と研究経費】

平成 30 年度－34 年度
148,300 千円

【ホームページ等】

http://lalsie.ist.hokudai.ac.jp/jp/

研究課題名　暗号技術による IoT エコシステムのレジリエンス向上

電気通信大学・大学院理工学研究科・教授　崎山（さきやま）　一男（かずお）

研究課題番号：18H05289　研究者番号：80508838
キーワード：情報セキュリティ、暗号理論、情報理論、ハードウェアセキュリティ、集積回路工学

【研究の背景・目的】【研究の背景・目的】

本研究の目的は、IoT (Internet of Things) デバイスへの物理攻撃によって遷移する安全性状態の循環を、IoT のエコシステムの機能とみなし、システム全体のレジリエンスを向上させることにある。IoT 時代の暗号デバイスは、次々と登場する新たな物理攻撃の脅威に直面している。レーザーフォールト攻撃は、暗号回路に対する最も深刻な物理攻撃として知られているが、攻撃者の能力がさらに高くなった場合には、回路内部のデータを直接読み出すプロービング攻撃を想定しなければならない。そこで本研究では、暗号デバイスの鍵の安全性状態を測るために、リーケージセンサを新たに開発し、暗号プリミティブ、暗号アルゴリズム及び暗号プロトコルの各レイヤーにおいて、たとえ、鍵の一部がリークした場合でも、しなやかに IoT システムを正常状態に回復させるレジリエンスの向上を狙う。

【研究の方法】

取り組むべき具体的課題として、二つの課題を設定する。一つ目の課題は、物理攻撃対策を念頭に置いた IoT システムへの暗号技術の適切な導入である。暗号鍵が正常な状態であるかを見張るリーク検知技術と、物理攻撃による鍵のリークに耐えるリーク耐性暗号技術を構築する。

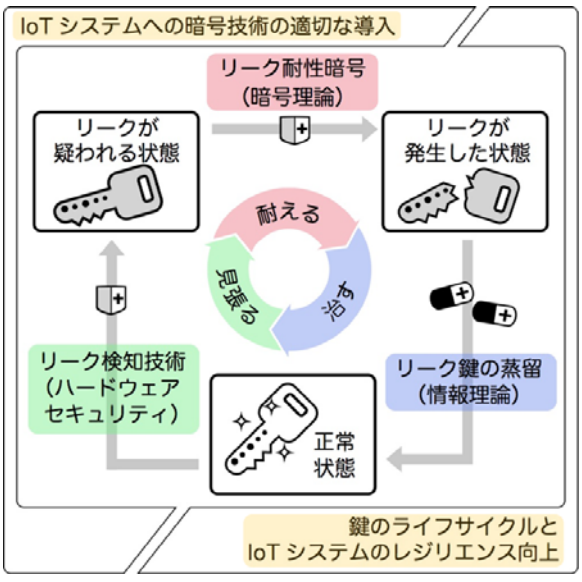

図１　暗号デバイスの安全性状態の循環と対策技術

二つ目は、鍵のライフサイクルと IoT エコシステムのレジリエンス向上である。鍵のリークは不可避との立場を取り、リークが疑われる状態でも、物理攻撃に耐えるリーク耐性暗号の拡張を検討し、情報の一部がリークした鍵からセキュアな鍵を抽出する鍵の蒸留技術の構築に向けた研究との連携を図る。

本研究におけるコア技術は、暗号とリーケージセンサである。H31 年度に、光センサと電磁波センサを応用した最初のリーケージセンサを設計し、動作検証と安全性評価を行う。H33 年度には、リーケージセンサを搭載した暗号デバイスを開発し、リーク耐性暗号、リーク鍵の蒸留及びリーク検知技術に関する研究と協働を進める。

【期待される成果と意義】

センサと暗号技術の融合による新たな物理攻撃対策つき IoT デバイスの創生が期待できる。理論的研究では、物理パラメータを取り入れた安全性証明技法の確立や、漏れた鍵情報を排除できる情報蒸留といった発展課題につながる。実践研究と理論研究の成果を合わせることで、IoT エコシステムの一面として、鍵の安全性状態の循環が実現できると考える。

本研究で開発するリーケージセンサは、プロービング攻撃の検知を軸に、物理（もの）と数理（こと）を橋渡しする技術であり、異なる研究分野間の協働を可能にする新しい概念ともいえる。つまり、本研究課題は、物理攻撃対策に関連する学術的知識創生の源泉として機能することが期待できる。

【当該研究課題と関連の深い論文・著書】

・K. Matsuda, T. Fujii, N. Shoji, T. Sugawara, K. Sakiyama, Y. Hayashi, M. Nagata, N. Miura, “A 286F²/cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” ISSCC 2018: 352-354 (2018).
・K. Sakiyama, Y. Li, M. Iwamoto, and K. Ohta, “Information-Theoretic Approach to Optimal Differential Fault Analysis,” IEEE Trans. Inf. Forensic Secur., 7(1): 109-120, (2012).

【研究期間と研究経費】

平成 30 年度－34 年度
149,500 千円

【ホームページ等】

http://sakiyama-lab.jp/study

研究課題名　広汎な観測に対する因果性の導入とその最適統計推測論の革新

早稲田大学・理工学術院・教授　谷口（たにぐち）　正信（まさのぶ）

研究課題番号：18H05290　研究者番号：00116625
キーワード：因果性、統計的最適推測、時空間観測、トポロジカルデータ、医用画像

【研究の背景・目的】

本研究では、ノーベル経済学賞受賞者 Granger が提案した因果性などを含む高度な指標を一般的な乖離度から導入して、データ科学における今まで捉えられなかった潜在要因の統一的指標を提案する。観測対象も従来の統計データだけでなく、高次元時空間過程、グラフ・ネットワーク、遺伝子、トポロジカルデータ等にも適用する。この統一的指標を以下、一般化因果性指標と呼ぶことにする。本研究の主題は、一般化観測データからの一般因果性指標の統計的推測理論の構築とその広汎な分野への新しい潜在要因抽出法の提案である。推測法としては、従来の手法だけでなく多様な手法提案、検証を行い、高次元データ、生体・遺伝子データ、グラフィカル・トポロジカル（図形的）データ等の観測に対して我々の構築する最適統計推測法を適用し、広汎な分野の現象に対する新たな潜在指標を洗い出し、それにより予知、要因分析、コントロール、リスク管理に貢献する。

【研究の方法】

研究推進は谷口正信（早稲田大学）が中心になって、早稲田大学で、セミナー、ワークショップを開催して意見交換、共同研究および、そのマッチング

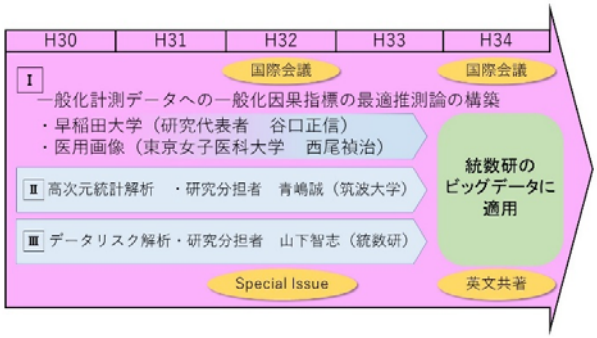

図１　ロードマップ

を行う。研究は主に一般化因果性の導入とその最適推測論と医用画像への応用を推進する。青嶋誠（筑波大学）は、特に高次元統計解析の理論構築を推進し、高次元解析の流れのセミナー、ワークショップを筑波大学で開催する。山下智志（統計数理研究所）は金融リスク解析を潜在因子を使って推進し、金融リスク分野のセミナー、ワークショップを統計数理研究所で開催する。

【期待される成果と意義】

統計数理において、本研究の一般化因果性指標の提案は、従来の因果性が定義出来なかった場合への成果も含み、それ自体新しいもので、それを時空間観測、高次元観測、トポロジカル観測、医用画像まで含む膨大かつ広汎な一般化データから、高度な推測の基礎概念 LAN 性に基づいての統計的最適推測理論の構築は、統計数理理論への貢献として大変革新的である。図 2 は東京女医大西尾教授による。

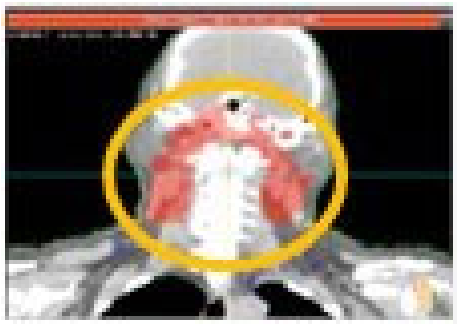

図２　医用画像解析

【当該研究課題と関連の深い論文・著書】

・Granger,C.W.J., Investigating causal relations by econometric models and cross-spectral methods. Econometrica 37 424-439, (1969).
・Taniguchi,M. and Kakizawa,Y. *Asymptotic Theory of Statistical Inference for Time Series Analysis*, Springer-Verlag, 661pages, (2000).

【研究期間と研究経費】

平成 30 年度－平成 34 年度
140,600 千円

【ホームページ等】

http://www.taniguchi.sci.waseda.ac.jp/kakenhoukoku2018.html

研究課題名　巨大グラフとビッグデータ解析の基礎基盤：理論研究と高速アルゴリズム開発

情報・システム研究機構・国立情報学研究所・
情報学プリンシプル研究系・教授
かわらばやし　けんいち
河原林　健一

研究課題番号：　18H05291　研究者番号：40361159
キーワード：　グラフ、アルゴリズム、理論計算機科学、組合せ最適化

【研究の背景・目的】

現代の情報化社会が抱える大部分の問題は、センサー、画像、音声などによって収集された多種類の大量のデータの解析、そして情報処理技術によって解決されることが期待されている。しかしながら、データ量が膨大であるため、超大型コンピュータを使用しても解決が容易でないものばかりである。このような問題を解決するためには、アルゴリズムの革新が必要不可欠であり、計算モデルと数理の探求に基盤をおく革新的アルゴリズム設計技法の構築や体系化は、科学の共通基盤として最優先の意義を持つ。

本研究では、以上の背景のもと、数学的理論を駆使することにより、アルゴリズムの理論分野（おもにグラフアルゴリズム）の強化および、理論分野の道具を利用によるアルゴリズムの高速化・スケール化に挑む。

【研究の方法】

以下の 3 点の研究課題を中心にする予定である。

１．劣モジュラ関数とその応用

劣モジュラ性は普遍的な概念であり、これまでに扱われてきた機械学習、人工知能分野だけではなく、自然言語、コンピュータビジョンにも応用されている。本提案では、近似アルゴリズム設計手法や代数的手法などさまざまな組合せ最適化手法を取り入れることでロバスト最適化（最悪時の解の質を担保する）などの、実社会に出現する最適化問題の解決に取り組む。

２．基礎数理理論の探求：有向グラフマイナー理論

グラフ理論における最も重要な理論体系「グラフマイナー理論」を用いた効率的なアルゴリズムの設計は、従来のアルゴリズム理論をはるかに深化させることが過去 20 年で明らかになってきた。しかしながら従来のグラフマイナー理論およびそれに基づくアルゴリズムは、すべて無向グラフにおけるものであり、有向グラフで同様の議論を展開することは困難であると考えられてきた。本研究では、有向グラフ版グラフマイナー理論の構築をめざす。

３．グラフ彩色問題

離散数学の中心的課題「4 色定理、そして曲面上に埋め込まれたグラフに対するグラフ彩色問題」に対する本質的貢献を目指す。

【期待される成果と意義】

本研究を通して、将来的に次のような学術、技術寄与が期待される。

１．数学、情報学の個別分野で開発されたアルゴリズム手法を整備、標準化し、各分野に提供できる体制が確立される。

２．離散数学、理論計算機科学、確率論、組合せ最適化研究者によるアルゴリズム科学と実問題の数理モデル化の解決のための共同研究拠点が構築される。

【当該研究課題と関連の深い論文・著書】

K. Kawarabayashi, M. Thorup: Coloring 3-colorable graphs with o(n^{1/5}) colors, Journal of the ACM, 64 Issue 1, Article No 4

K. Kawarabayashi, S. Kreutzer: The Directed Grid Theorem. STOC 2015, 655-664.

【研究期間と研究経費】

平成 30 年度－34 年度
148,500 千円

【ホームページ等】

https://bigdata.nii.ac.jp/wp/
k_keniti@nii.ac.jp