Case I: A biologically inspired neuromorphic processor:
This research program will engage students in studying learning algorithms for biological neural network as well as designing innovative high-performance, low-area and power-efficient and biologically plausible embedded neuromorphic processors.

Background: Neuromorphic systems include a large number of neurons, synapses and their interconnecting structure on hardware. Such systems are highly parallel, fast, fault tolerant, intelligent and compact. This research focus is on neuromorphic systems implementing Spiking Neural Networks (SNNs). Spiking neural networks are the third generation of neural networks where neurons communicate through sparse sequences of spikes. Comparing to previous generations, SNNs are faster, smaller in size, more energy efficient and biologically realistic [1,2].

Implementation of SNNs is computationally expensive because of nonlinear expressions in neuron models, size of the networks and various communication pathways. This research objective is to address this challenges by designing efficient and high speed hardware implementation platform for SNN.

Methods: Current neuromorphic research has led to the development of a plethora of models to mimic real neurons with different levels of abstraction in biological details [3,4]. The choice of models depends on the application of the device to be designed. In this research we intend to focus on biologically plausible and detailed models and optimize them without comprising their correctness.

First objective at the lowest level is designing practical circuits realizing brain cells using hardware implementation techniques (e.g. pipelining and power optimization techniques). It is very important to implement the cell models as efficient and fast as possible since they are basic building block of the neuromorphic systems. Biologically plausible models are relatively complex in nature comparing to high-level models due to their large array of differential equations and accompanying parameters. As a result, they have seen limited proposed hardware implementations. Currently, there is no neuromorphic processor available for large scale simulation of the biologically detailed models. However these models are gaining more attention by researchers.

At the architectural and software levels, brain cells are connected together through different interaction mechanisms and their systematic behavior is analyzed. This research has two objectives in architectural level; First is applying brain inspired learning and information processing algorithms in the software level and second is designing a configurable hardware for large scale implementation of biological neural network.

Previous Research: My M.Sc. dissertation titled "Digital Implementation of a Concise Model for Astrocyte Calcium Oscillations" was beginning of my research in the field of neuromorphic engineering where I optimized a biological astrocyte for hardware implementation using Piece Wise Linear (PWL) approximation technique. Since, I continued to research in spiking neural network and neuromorphic engineering. As a PhD student, I started using COordinate Rotation DIgital Computer (CORDIC) method to implement Izhikevch neuron and on-hardware online spike time dependent plasticity. The advantage of CORDIC algorithm over previous methods including PWL, is its very high precision to calculate nonlinear terms and yet it is well suited for hardware implementation. The primary goal of those researches was to find an appropriate hardware for neurons, astrocytes and other biological cells as buildings blocks of a biological detailed neuromorphic processor.

Future Research
My future research plan involves both studying algorithms underlying learning and information processing in biological neural network as well designing neuromorphic processor for large scale implementation of such networks. Design prototypes would be implemented and tested on Field Programmable Gate Arrays (FPGAs) at first phase. FPGAs provide relatively cheap, fast, reconfigurable, and easy to work with plat-

form for testing functionality and performance of the digital hardwares and are a popular implementation platform Second phase is designing an Application Specified Integrated Circuit (ASIC) to implement the neuromorphic processor which require softwares such Cadence that currently are accessible through CMC Microelectronics for universities. Finally, the design need to be fabricated that is also is supported by CMC Microelectronics. The primary goal of those researches was to find an appropriate hardware for neurons, astrocytes and other biological cells as buildings blocks of a biological detailed neuromorphic processor.

Future Research

My future research plan involves both studying algorithms underlying learning and information processing in biological neural network as well designing neuromorphic processor for large scale implementation of such networks. Towards these objectives, I defined 4 projects.

Project 1: This project aims to study the different models presented by researchers . The objective is to adapt and modify differential equation describing these models to maximize performance and minimize power consumption and area. Students will run computer simulation of these models. Project 2: Designing digital circuits for ODEs describing cells. Students will use hardware implementation and optimization techniques to increase performance and reduce power consumption and area of designs. Project 3: Students will run computer simulations to observe changing of biological parameters and ions concentrations inside and around the cells that are active in learning and information processing. Project 4: Large scale implementation of the biological cells and communication pathways in the biology. Students will design a new architecture capable of online on-chip learning with biological neural networks. Project 5: software design and optimization for the hardware.

References

[1] K. E. Friedl, A. R. Voelker, A. Peer, and C. Eliasmith, "Human-inspired neurorobotic system for classifying surface textures by touch," IEEE Robotics and Automation Letters, vol. 1, no. 1, pp. 516–523, 2016.

[2] F. Ponulak and A. Kasinski, "Introduction to spiking neural networks: Information processing, learning and applications.," Acta neurobiologiae experimentalis, vol. 71, no. 4, pp. 409-433, 2011.

[3] M. Samie, G. Dragffy, A. M. Tyrrell, T. Pipe, and P. Bremner, "Novel bio-inspired approach for fault-tolerant vlsi systems," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 21, no. 10, pp. 1878–1891, 2013.

[4] A. L. Hodgkin and A. F. Huxley, "A quantitative description of membrane current and its application to conduction and excitation in nerve," The Journal of physiology, vol. 117, no. 4, p. 500, 1952.

[5] E. M. Izhikevich, "Simple model of spiking neurons," IEEE Transactions on neural networks, vol. 14, no. 6, pp. 1569–1572, 2003.

Case II: Post Quantum Hardware Cryptography and Homomorphic Encryption

This research program involves reducing complexity and efficient hardware implementation of the post quantum cryptography, homomorphic encryption, and homomorphic data processing embedded systems.

Background: Cryptography systems have become inseparable parts of almost every communication device. Cryptography is used to provide confidentiality, data security, and authentication in many applications such as communication devices, autonomous vehicles, Internet of Things (IoT), healthcare [1,2,3,4] etc.

However, with rise of the quantum computers capable of executing Shor algorithm [5], many popular public key cryptography systems including RSA and elliptic curve cryptography will be no longer secure. This would greatly endanger the security of digital communications and expose user's data. National Institute of Standards and Technology (NIST) has already started a competition for developing cryptographic systems that are resistant to quantum computers attacks. At present, NIST has called for submissions for round 3 of this completion [6].

Another issue with expansion of the Internet and cloud systems is privacy concern. Currently, with the most secure communication between user computer and cloud system, still the data is decrypted in the cloud for processing. Therefore, the third parties owning the cloud and those with authorized access

can read the data and use it for their own advantages. Homomorphic Encryption (HE), first introduced by Gentry is a privacy preserving algorithm that allows valid computing over encrypted data without the need to decrypting it.

Since these algorithms are expected to be the future cryptography systems, it is important to design an efficient embedded systems for these systems. In next section, I further explain my methods to address this challenge.

Method: Since post quantum cryptography is a rather new field and because of complexity of its algorithms, there exists only a limited number of the hardware implementations for these algorithms. In this research proposal, Field Programmable Gate Arrays is selected as the initial implementation target since they provide a reconfigurable, cheap and yet fast hardware platform. In homomorphic encryption, plaintext is transformed into ciphertext, allowing computation on the encrypted data resulting in another ciphertext. Decryption of this ciphertext yields the same computation result as if it had been performed on plaintext. However, such operations are computationally expensive and increases the complexity of the homomorphic computations circuit. Compared to software implementations, hardware cryptography results in a higher speed and a lower cost, while satisfying efficiency and low-power requirements of electronic devices. Implementation of homomorphic encryption and evaluation circuit is a extremely challenging because of the very large word length of ciphertexts and computational unit, specifically multipliers. Homomorphic encryption is a rather new research topic and its hardware implementation is less explored. In the following, I discuss my approach towards this problem to achieve a better hardware for practical homomorphic encryption and data processing.

Previous Research: As postdoctoral fellow, I was working on the efficient FPGA implementation of finite field multipliers for Elliptic Curve Cryptography (ECC) where we proposed a new binary polynomial multiplication algorithm with low complexity and high speed. The work was then extended to to hardware implementation of lattice based cryptography algorithms and other post-quantum encryption algorithms.

Future Research (Research Plan): My future research plan engages both studying and optimizing post quantum and homomorphic encryption and computation algorithms as well as designing an efficient embedded processor and processor for these algorithms.

Research Program Feasibility: For the first phase which is optimizing algorithms for hardware implementation, I will use Python programming language to run simulations and check the validity of modified algorithms. Further, I will use FPGAs as implementation platform to measure efficiency of design. FPGAs are substantially cheaper than designing and fabricating a VLSI ASIC and have advantage of flexibility. Eventually, after testing design could be fabricated for final evaluations. Towards this objectives, I defined 3 projects: Project 1: This project aims to study the different algorithms presented by researchers for post quantum cryptography including finalists of the NIST completion to standardize quantum resistant public key cryptographic algorithms. The objective of this study is to reduce complexity and optimize these algorithms for FPGA implementation. Project 2: Investigating homomorphic encryption and ciphertext computation algorithms. Students will perform mathematical analysis to enhance these algorithm in the terms of area and delay complexity. Further, they will run computer simulations to check validity of the algorithms. Project 3: Students will design an architecture and circuit to efficiently implement these algorithms on hardware, either as accelerator for computer software or possibly as an standalone hardware cryptography system.

Funding for research In terms of funding , I would be able to use my background and familiarity with problems and concerns of industry to secure funding for the research. I have also experience of writing successful research proposal with industry partner to obtain MITACS grant.

References

[1] J. Yoo and J. H. Yi, "Code-based authentication scheme for lightweight integrity checking of smart vehicles," IEEE Access, vol. 6, pp. 46731–46741, 2018.

[2] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith, "Obstacles to the adoption of secure communication tools," in 2017 IEEE Symposium on Security and Privacy (SP), pp. 137–153, 2017.

[3] P. Aparna and P. V. V. Kishore, "Biometric-based efficient medical image watermarking in e-healthcare application," IET Image Processing, vol. 13, no. 3, pp. 421–428, 2019.

[4] T. D. P. Bai, K. M. Raj, and S. A. Rabara, "Elliptic curve cryptography based security framework for internet of things (iot) enabled smart card," in 2017 World Congress on Computing and Communication Technologies (WCCCT), pp. 43–46, 2017.

[5] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124-134, doi: 10.1109/SFCS.1994.365700

[6] "Post-Quantum Cryptography-Round 3 Submissions," 2020.