April 27, 2025
Chair, Faculty Search Committee
in Department of Electrical and Computer Engineering,
Concordia University,
2160 Bishop St suite 301
Montreal, Quebec H3G 2E9

Dear Search Committee Members,

I am writing to express my interest in the Assistant Professors in the Area of Computer Engineering position in Department of Electrical and Computer Engineering at Concordia University. Currently employed as a Digital Logic Design Engineer at NXP Semiconductors, I am also a part-time research assistant in the Department of Electrical and Computer Engineering at the University of Windsor.

My research contributions have been in the area of neuromorphic engineering, Post-Quantum Cryptography (PQC) and Homomorphic Encryption (HE) circuit and systems. Throughout my MSc and PhD, I have developed various novel techniques aimed at enhancing performance and reducing the area of systems implementing Spiking Neural Networks (SNNs), the third generation of neural networks. SNNs have numerous advantages over previous generations with wide range of applications in classification and medical purposes.

Subsequently, as a postdoctoral fellow, my focus shifted to reducing complexity and designing hardware for low-latency, low-area finite field multipliers widely used in cryptosystems. In my role as a part-time research assistant at the University of Windsor, I am currently engaged in designing efficient hardware architectures for implementing PQC and HE systems. These areas have gained prominence due to the imminent threat of quantum computers and escalating concerns about data privacy and security. My research contributions include several journal and conference papers, and two US patents.

In my industry experience, I have actively participated in designing various System On Chips (SOCs), contributing to a team that designed an SOC utilizing artificial neural networks in cybersecurity. Presently, I am involved in the design of Ethernet controllers for integration into cars and other systems. These experiences have provided me with valuable insights into the requirements, development, and applications of embedded systems in the industry, and I am eager to bring this expertise into the research lab and classroom.

Beyond my research activities, I have been fortunate enough to obtain wide range of teaching experiences. Since beginning of my PhD, I have been involved in teaching and preparation of course materials in several courses including: Digital Logic Design, Embedded Systems and Electronics. As a postdoctoral fellow and part-time researcher at the University of Windsor, I provided guidance to PhD, MSc, and bachelor students. In my capacity as a seasonal instructor for continuing education, I conducted online courses in Cybersecurity.

Having been inspired by exceptional teachers and advisers, I recognize the profound impact a dedicated educator can have on a student. I am committed to following in their footsteps, continually improving my teaching and research skills.

Sincerely,

Mason (Moslem) Heidarpur
217 Big Dipper St., Ottawa, ON, Canada, K4M 0J8
Email: heidarpur.m@gmail.com
Immigration status: Permanent resident of Canada

Moslem Heidarpur

Webpages:

- ORCID
- Google Scholar
- Linkedin
- Researchgate

Immigration status:

- Permanent resident of Canada

Address:

- 217 Big Dipper, Ottawa, ON, Canada

Email:

- heidarpur.m@gmail.com (preferred)
- heidarp@uwindsor.ca
- moslem.heidarpur@nxp.com

Phone:

- 6137976194

Education

- **PhD in Electrical Engineering**
  - University: University of Windsor, ON, Canada. *2020*
  - Dissertation Title: Digital Implementation and Modification: Spiking Neural Network
  - Dissertation Advisors: Majid Ahmadi, Distinguished Professor, Arash Ahmadi, Assistant Professor.

- **M.Sc. in Electrical Engineering**
  - University: Razi University of Kermanshah, Kermanshah, Iran. *2014*
  - Dissertation Title: Digital Implementation of a concise model for astrocyte calcium oscillations.
  - Dissertation Advisors: Arash Ahmadi, Assistant Professor

- **B.Sc. in Electrical Engineering**
  - University: Razi University of Kermanshah, Kermanshah, Iran *2009*
  - Project Title: Digital Implementation of a PC Oscilloscope
  - Project Advisors: Mohsen Hayati, Professor

Industry Training and Courses

- **Functional Safety**
  - Introduction to functional safety, why it is required, and its implications
  - Meeting requirements of ISO26262 and IEC 61508

- **Design Excellence and Quality Management System (QMS)**
  - Documenting policies, procedures and controls necessary to create high-quality products
  - Meeting requirements of ISO 9001 and IATF 16946

- **Root Cause Analysis (RCA)**
  - 8-D (8-Discipline) problem solving process
  - 3x5 why analysis and Corrective Action (CA)

- **Cross Domain Clocking (CDC)**
  - Historical issues related to CDC mishandling leading to Mean Time between Failures (MTBF)
  - Best approaches to asynchronous communication between modulus running on different clock frequencies

- **Right Review Training**
  - Right Reviews (Review of code, documentation, specification etc.) and characteristics

- Roles and Responsibilities recommended to conduct review and validation process

- **Practical development of risk management for process**
  - Introduction to risk management, process steps, and roles and responsibilities
  - Change management system and risk register

- **Business Creation and Management (BCaM)**
  - R&D policies at the corporation
  - Design Failure Modes and Effects Analysis (DFMEA)

Research Experience

- **Part-time Research Assistant, University of Windsor**
  - Location: Windsor, ON, Canada. *2021-Present*
  - Description:
    - Continue research on efficient and fast digital hardware for cryptography and cybersecurity algorithms
    - Assembled a team of researchers to divide the work toward building a quantum computer attack resistant digital cryptogrpahy hardware which is capable of performing homomorphic operations on cyphertext.
    - Research on hardware accelerator which is capable of performing homomorphic operations on cyphertext.
    - Research on neuromorphic engineering, a power efficient sparsely connected neural network hardware were developed for FPGA implementation based on Time To First Spike (TTFS) algorithm.
    - Proposed hardware capable of recognizing MNIST patterns with a lower power consumption and higher speed comparing to rate coding algorithms.

- **Postdoctoral Researcher, University of Windsor**
  - Location: Windsor, ON, Canada. *2020-2021*
  - Description:
    - Performed research in the field of digital hardware cryptography, focusing on post-quantum cryptography algorithms and homomorphic encryption.
    - Designed a highly optimized re-configurable hardware for accelerating binary polynomial multiplication on FPGA.
    - Proposed design achieved superior performance in terms of both speed and area-delay product comparing to previously presented works in the field.

- **Graduate Research Assistant, University of Windsor**
  - Location: Windsor, ON, Canada. *218-2020*
  - Description:
    - Conducted dissertation research at the Research Centre for Integrated Microsystems (RCIM) with a focus on the efficient FPGA implementation of spiking neural networks.
    - Used different techniques including Piece Wise Linear (PWL) approximation and COrdinate Rotation DIgital Computer (CORDIC) methodologies to architect high-performance, cost-effective digital hardware for large scale spiking neural network implementation.

- **Adjunct Researcher, St. Clair College**
  - Location: Windsor, ON, Canada. *2019-2020*
  - Description:
    - Supervised two college students to perform research on a project with collaboration of a local industry (Standard Tool & Mold Inc)
    - Project aimed to design a novel device for possible commercial production. First prototype was successfully developed.

- I applied and successfully received MITACS funding to continue the project in its second phase.

Research Interests

- **Cryptographic Circuits and Systems**
  - Post Quantum Cryptography
  - Homomorphic Encryption
  - Hardware Security

- **Learning and Intelligent Circuits and Systems**
  - Spiking Neural Networks
  - Neuromorphic Engineering
  - Biomedical Circuits and Systems

Teaching Experience

- **Instructor, University of Windsor**
  - Location: Continuing Education, Windsor, ON, Canada. *2023-Present*
  - Description:
    - Courses are offered remotely, where students learn about different types of cyber attacks and how to secure computers, networks, and servers
    - Course materials, attendance, quizzes, and grading were online in Brightspace.
  - Courses:
    - Cybersecurity I : Introduction to Systems Security
    - Cybersecurity II: System Implementation

- **Mentor, University of Windsor**
  - Location: Windsor, ON, Canada *2020-Present*
  - Description:
    - Closely supervising and mentoring four PhD and seven master students on weekly meeting basis.
    - Helping them to gain fundamental knowledge, identifying problems, literature survey for solutions, and critical analysis of published works.
    - PhD students have successfully published papers in IEEE transactions within their second year, with additional papers currently under review and in preparation
    - Offered guidance and evaluate the progress of an undergraduate student as they completed their project.

- **Graduate Teaching Assistant, University of Windsor**
  - Location: Windsor, ON, Canada. *2019-2020*
  - Description:
    - Prepared materials, tutorials and answered student questions as a teaching assistant
    - During labs, I helped students to formulate their ideas to flowcharts and further to codes to implement on FPGA, Arduino or Raspberry Pi evaluation boards and eventually debugging it.
  - Courses:
    - Digital Logic Design II
    - Embedded Systems
    - Electronics I

- **Lecturer, Islamic Azad University**
  - Eslamabad-Gharb, Kermanshah, Iran *2018-2020*
  - Description:
    - Delivered lectures, designed, prepared, and developed teaching materials, and assessed students.
    - Supervised final year undergraduate projects.

- Courses:
  - Digital Logic Design
  - Computer Architecture
  - Analog CMOS Integrated Circuits
  - Electronics

- **High School Teacher, Chamran Vocational High School**
  - Eslamabad-Gharb, Kermanshah, Iran *2010-2012*
  - Description:
    - Taught Courses in school and evaluated students
    - Worked with weaker students in individual
    - Graded exams and communicated with parents about students progress.
  - Courses:
    - Electronics Measurements
    - Electronics

Work Experience

- **ASIC Design Engineer, NXP Semiconductors**
  - Location: Ottawa, ON, Canada. *2024-Present*
  - Job Description:
    - Conducting research and development to improve DDR PHY performance and reliability.
    - Assisting customers with questions related to PHY design and integration
    - Developed an AI-based IP setting inspection and optimization tool (ISIO) to detect incorrect settings and optimize PHY eye quality.
    - Added new features and extended the RDS tool to enhance debugging capabilities for customer issues.

- **Digital Logic Designer, NXP Semiconductors**
  - Location: Ottawa, ON, Canada. *2021-2024*
  - Job Description:
    - Responsible for designing high performance network controllers for Ethernet switches.
    - The designed unit decoded the frame descriptor, extracted pointers and performed memory reads.
    - ECC check block was coded to ensure the integrity of received data
    - block was designed to decode and perform frame modification instructions received with frame context
    - Parity check and fault injection and detection mechanism was coded for safety enabled SOCs.

- **System On Chip Engineer, Axiado Canada**
  - Location: Ottawa, ON, Canada. *2020-2021*
  - Job Description:
    - Designed system on chip using ARM CPUs including Cortex A53, Cortex M55, Cortex M0, Ethos U65, AXI interconnect etc.
    - HDL Programming (System Verilog, Verilog), architecture, simulation and performance monitoring.
    - Writing basic tests and programs using Bare Metal C.
    - The objective was to design an SOC that could inspect the Ethernet packets and detect cyber threats using A

- **Postdoctoral Researcher, University of Windsor**
  - Location: Windsor, ON, Canada. *2019-2020*
  - Job Description:
    - Closely supervising and mentoring two PhD students and coordinating their research.
    - Identification of funding opportunities and writing of funding applications.

- **Android Developer, Freelance**

- Freelance. *2018-present*
- Job Description:
  - Google play developer with more than 12000 active app installations
  - apps include dictionaries, nomenclatures and classic poems which were developed in Eclipse and Android studio IDEs (Based on Java)

Technical Skills

- **HDL**
  - System Verilog
  - Verilog
  - VHDL
- **Programming**
  - Python
  - C++
  - Bare Metal C
  - Java
  - Assembly
  - Latex
  - Linux Shell Scripting
- **AI**
  - Neural Network
  - Deep Learning
  - Spike Time Dependent Plasticity (STDP)
- **CPUs and microcontrollers**
  - Cortex M55
  - Cortex A53
  - Cortex M0
  - Ethos U65
  - Zilog Z80
  - Arduino
  - Raspberry Pi.
  - 8051 Microcontroller
  - AXI Interconnect
- **Optimization**
  - Single and multi objective Particle Swarm Optimization (PSO)
  - Genetic Algorithm
- **Software and Tools**
  - Synopsys VCS
  - Synopsys Lint
  - Synopsys SpyGlass
  - Siemens PowerPro
  - Siemens Questa
  - Cadence Genus Synthesis
  - Verplex's BlackTie
  - Xilinx ISE

- Xilinx Vivado
- Quartus prime
- Modelsim
- Matlab
- Hspice
- Agilent Advanced Design System
- Microsoft Visual Studio
- Eclipse
- Android Studio
- DesignSync
- Git
- Jira

Academic Services

- **Guest Reviewer To Journals and Conferences.**

- Description:
  - Conducted peer review of papers for possible publication in the journals and conferences
  - Journals and Conferences:
    - IEEE Transactions on Circuits and Systems I (TCAS I)
    - IEEE Transactions on Very Large Scale Integration (VLSI) Systems (TVLSI)
    - IEEE Transactions on Biomedical Circuits and Systems (TBIOCAS)
    - Neural Computing and Applications
    - IEEE Access
    - Microelectronics Journal
    - IEEE Transactions on Emerging Topics in Computational Intelligence (TETCI)
    - IEEE International Symposium on Circuits and Systems (ISCAS)

- **Review Committee Members (RCM)**
  - Description:
    - Assigned reviewers to papers and follow up regarding reviews
    - Preliminary decision on papers based on reviewer comments
  - Journals and Conferences:
    - IEEE International Symposium on Circuits and Systems (ISCAS) 2024
    - IEEE International Symposium on Circuits and Systems (ISCAS) 2023

- **Vice Chair of IEEE Signal Processing Societies**
  - Location: Windsor, ON, Canada.
  - Description:
    - Organized events, workshops and tutorials as well as running face-to-face meeting and performing chair duties in his absence.
    - Presented a workshop on spiking neural networks and their application in signal processing.

Grants

- Mitacs Accelerate grant in partnership with Standard Tool & Mold Inc., CAD$ 45k, 1 year project.
- Competitive post doctoral fellowship, University of Windsor, CAD$ 60k, 1 year project.

Honours and Awards

- Certificate of appreciation in recognition of leadership and service as vice-chair of IEEE signal processing and communication societies.
- Top 15% in the program, University of Windsor, May. 2020.
- Top 10% in class, Razi University of Kermanshah, Sep. 2014.
- Top 1% in national university entrance exam (Konkur)

Membership

- Academic assessment has been completed to determine eligibility for PENG membership. Currently enrolled for the NPPE exam as part of the membership process.

Presentations

- "CORDIC-SNN: On-FPGA STDP Learning and Izhikevich Neuron Model."
  Paper presented at 2020 International Symposium on Circuits and Systems, Online Presentation.
- "Time step impact on performance and accuracy of izhikevich neuron: Software simulation and hardware implementation"
  Paper presented at 2020 International Symposium on Circuits and Systems, Online Presentation.
- FPGA Implementation of Spiking Neural Networks and its application to signal processing
  Presented at a IEEE research presentation event, University of Windsor, Canada.
- An Integrated Astrocyte-Adaptive Exponential (AAdEx) Neuron And Circuit Implementation.
  Paper presented at the 2016 24th Iranian Conference on Electrical Engineering (ICEE), University of Shiraz, Iran

Publications

- **Journals**
  - Heidarpur, Moslem, Mitra Mirhassani, and Norman Chang. "A Fully Pipelined FIFO Based Polynomial Multiplication Hardware Architecture Based On Number Theoretic Transform." arXiv preprint arXiv:2501.11867 (2025).
  - Thirumoorthi, Madhan, et al. "A High Speed and Area Efficient Processor for Elliptic Curve Scalar Point Multiplication for GF (2^m)." in IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2024).
  - Alammari, Khalid, et al. "LIF neuron—a memristive realization." in Frontiers in Electronics 5 (2024): 1366299.
  - M. Heidarpur, A. Ahmadi, M. Ahmadi, "The Silence of the Neurons: An Application To Enhance Performance and Energy Efficiency ," in Frontiers in Neuroscience, vol. 17, doi: 10.3389/fnins.2023.1333238, Dec. 2023
  - M. Thirumoorthi, A. J. Leigh, M. Heidarpur, M. Khalid and M. Mirhassani, "Novel Formulations of M-Term Overlap-Free Karatsuba Binary Polynomial Multipliers and Their Hardware Implementations," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 31, no. 10, pp. 1509-1522, Oct. 2023
  - A. J. Leigh, M. Heidarpur and M. Mirhassani, "A Resource-Efficient and High-Accuracy CORDIC-Based Digital Implementation of the Hodgkin–Huxley Neuron," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 31, no. 9, pp. 1377-1388, Sept. 2023
  - Leigh, A.J., Heidarpur, M. and Mirhassani, M. The input-dependent variable sampling (I-DEVS) energy-efficient digital neuron implementation method. Nonlinear Dyn 111, 10559–10571 (2023).
  - A. J. Leigh, M. Heidarpur and M. Mirhassani, "Digital Hardware Implementations of Spiking Neural Networks With Selective Input Sparsity for Edge Inferences in Controlled Image Acquisition Environments," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 5, pp. 1724-1728, May 2023
  - A. J. Leigh, M. Heidarpur and M. Mirhassani, "A High-Accuracy Digital Implementation of the Morris-Lecar Neuron with Variable Physiological Parameters," in IEEE Transactions on Circuits and Systems II: Express Briefs, 2022
  - M. Thirumoorthi, M. Heidarpur, M. Mirhassani and M. Khalid, "An Optimized M-Term Karatsuba-Like Binary Polynomial Multiplier for Finite Field Arithmetic," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 30, no. 5, pp. 603-614, May 2022
  - M. Heidarpur and M. Mirhassani, "An Efficient and High-Speed Overlap-Free Karatsuba-Based Finite-Field Multiplier for FGPA Implementation," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 29, no. 4, pp. 667-676, April 2021

- M. Heidarpur, P. Khosravifar, A. Ahmadi and M. Ahmadi, “CORDIC-Astrocyte: A Tripartite Glutamate-IP3-Ca^{2+} Interaction Dynamics on FPGA,” IEEE Transactions on Biomedical Circuits and Systems, vol. 14, no. 1, pp. 36-47, Feb. 2020

- M. Heidarpur, A. Ahmadi, M. Azghadi and M. Ahmadi, “CORDIC-SNN: On-FPGA STDP Learning and Izhikevich Neuron Model,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 7, pp. 2651-2661, Jul. 2019

- M. Heidarpur, A. Ahmadi, R. Rashidzadeh,“ A CORDIC Based Digital Hardware For Adaptive Exponential Integrate and Fire Neuron,” IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 63, no. 11, pp. 1986-1996, Nov. 2016.

- M. Heidarpur, A. Ahmadi, N. Kandalaft,“An Efficient Digital Implementation of 2D Hindmarsh-Rose Neuron”, Nonlinear Dynamics, vol. 89, no. 3, pp. 1–14, Aug

- **Conference Papers**

  - E. Z. Farsa, M. Heidarpur, A. Ahmadi and M. Mirhassani, ”High-Performance FPGA Implementation of Fully Connected Networks of SAM Neurons,” 2023 IEEE International Symposium on Circuits and Systems (ISCAS), Monterey, CA, USA, 2023, pp. 1-5

  - A. J. Leigh, M. Heidarpur and M. Mirhassani, ”A Low-Resource Digital Implementation of the Fitzhugh-Nagumo Neuron,” 2022 17th Conference on Ph.D Research in Microelectronics and Electronics (PRIME), Villasimius, SU, Italy, 2022, pp. 369-372

  - A. J. Leigh, M. Heidarpur and M. Mirhassani, ”Selective Input Sparsity in Spiking Neural Networksfor Pattern Classification,” 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, 2022

  - A. Leigh, M. Heidarpur, M. Mirhassani, “Selective Input Sparsity in Spiking Neural Networks for Pattern Classification,” 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Austin, 2022 (accepted-not online yet)

  - M. Heidarpur, A. Ahmadi and M. Ahmadi, “Time Step Impact on Performance and Accuracy of Izhikevich Neuron: Software Simulation and Hardware Implementation,” 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Sevilla, 2020, pp. 1-5

  - M. Heidarpur, A. Ahmadi, N. Kandalaft, “Concurrent Dual-Band 1.8/2.4 GHz LNA Using Miller Effect of the Gate-Drain Capacitor,” 2016 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, 2016, pp. 1-4.

  - M. Heidarpur, A. Ahmadi,“ An Integrated Astrocyte-Adaptive Exponential (AAdEx) Neuron And Circuit Implementation,” 2016 24th Iranian Conference on Electrical Engineering (ICEE), Shiraz, 2016, pp. 1545-1550

  - S. Haghiri, A. Ahmadi, M. Nouri and M. Heidarpur,“ An investigation on neuroglial interaction effect on Izhikevich neuron behaviour,” 2014 22nd Iranian Conference on Electrical Engineering (ICEE), Tehran, 2014, pp. 88-92

- **Book Chapters**
  - M. Heidarpur, A. Ahmadi and M. Ahmadi, “An efficient digital implementation of a detailed biological model of astrocyte , in Advances in Computational Intelligence, Springer International Publishing, Switzerland, Cham, 2019, pp. 857-868.

Patents

M. Heidarpur, A. Leigh and Mitra Mirhassani, A Dual State Circuit for Energy Efficient Hardware Implementation of Spiking Neural Networks, US20230153585A1, May. 2023

M. Heidarpur, M. Mirhassani, A fully pipelined fast FIFO based polynomial multiplication digital circuit based on number theoretic transform, US Patent application 63/378 537 , 6 Oct, 2022 [Provisional]

References

- Prof. Majid Ahmadi (PhD Dissertation Advisor)

  Electrical and Computer Engineering (ECE), University of Windsor
  Tel.: 519-972-5813
  Email: ahmadi@uwindsor.ca
- Dr. Mitra Mirhassani (Postdoc Supervisor)
  - Electrical and Computer Engineering (ECE), University of Windsor
  - Tel.: 5197354838
    mitramir@uwindsor.ca
- Dr. Arash Ahmadi (PhD Dissertation Advisor)
  - Department of Electronics, Carleton University
  - Tel.: 2262466025
    ArashAhmadi3@cunet.carleton.ca

Research Proposal: Post Quantum Hardware Cryptography and Homomorphic Encryption

- **Summary:**

This research program focuses on simplifying the complexity and ensuring efficient hardware implementation of post-quantum cryptography, homomorphic encryption, and homomorphic data processing embedded systems.

- **Introduction:**

This research proposal aims to address two aspects of concern related to modern communication devices and systems. The first aspect is security, and the second aspect is privacy.

- Security:
  Cryptographic systems have become integral components of nearly every communication device, providing confidentiality, data security, and authentication in various applications such as communication devices, autonomous vehicles, the Internet of Things (IoT), and healthcare [1,2,3,4]. However, the advent of quantum computers capable of executing the Shor algorithm [5] poses a threat to popular public key cryptography systems like RSA and elliptic curve cryptography. This jeopardizes the security of digital communications and exposes user data. The National Institute of Standards and Technology (NIST) has initiated a competition for developing cryptographic systems resistant to quantum computer attacks, with round 3 submissions currently underway [6].
- Privacy:
  Another issue arising from the expansion of the Internet and cloud systems is privacy concern. Despite secure communication between user computers and cloud systems, data is still decrypted in the cloud for processing. Consequently, third parties with access can read and exploit the data. Homomorphic Encryption (HE), introduced by Gentry, is a privacy-preserving algorithm enabling computation over encrypted data without decryption.

As these algorithms are expected to shape future cryptographic systems, designing efficient embedded systems for their implementation is crucial. In the next section, I elaborate on my methods to address this challenge.

- **Challenges:**

In this section, the challenges ahead of Post-Quantum Cryptography (PQC) and Homomorphic Encryption (HE) is briefly explained and how this research proposal tries to address these challenges.

Post-quantum cryptography are believed to be secure against attacks by quantum computers. While post-quantum cryptography aims to provide alternatives that resist quantum attacks, it also faces several challenges:

- Standardization: There is not yet a widely accepted standard for post-quantum cryptographic algorithms.

- Migration: Transitioning from existing cryptographic systems to post-quantum cryptography poses challenges. It requires updating protocols, systems, and infrastructure across various applications and services, which can be a time-consuming and complex process.
- Performance: Many post-quantum cryptographic algorithms are computationally more intensive than current algorithms, potentially leading to performance challenges, especially in resource-constrained environments. Researchers are working to optimize these algorithms to improve efficiency.
- Implementation Issues: Implementing cryptographic algorithms correctly is crucial for security. However, there's a risk that poorly implemented post-quantum algorithms may introduce vulnerabilities. Ensuring secure and correct implementations is a challenge, especially given the complexity of some post-quantum cryptographic schemes.
- Lack of Real-World Testing: Post-quantum cryptographic algorithms are relatively new, and their real-world performance and security need to be validated through extensive testing and deployment. Until these algorithms are widely deployed and tested, their effectiveness and resilience against both quantum and classical attacks remain theoretical.
- Quantum-Safe Key Management: Post-quantum cryptographic systems rely on key exchange mechanisms, and secure key management is crucial. Quantum-safe key exchange protocols need to be developed and integrated into existing systems to ensure that keys remain secure even in a post-quantum world.
- Evolving Threat Landscape: The threat landscape is dynamic, and adversaries may adapt their strategies and techniques. Post-quantum cryptographic algorithms need to be resilient not only to known quantum attacks but also to potential new attack vectors that may emerge.
- Global Adoption: Achieving global adoption of post-quantum cryptographic standards is a challenge. Different countries and organizations may have varying levels of readiness and priorities, and achieving a coordinated transition is essential for overall security.

Homomorphic encryption provides a significant advantage for privacy and security in scenarios where sensitive data needs to be processed in a secure manner. However, homomorphic decryption, or more accurately, the challenge associated with homomorphic encryption, involves several factors:

- Computational Overhead: Homomorphic encryption typically introduces a significant computational overhead. Performing operations on encrypted data is computationally more intensive than on the equivalent unencrypted data. This can lead to slower processing times, making it less practical for certain applications.
- Key Management: Managing the keys used in homomorphic encryption is crucial. If keys are compromised, it can potentially lead to the compromise of the entire encrypted data. Key management becomes even more challenging as the complexity of the homomorphic encryption scheme increases.
- Limited Functionality: While homomorphic encryption allows for certain types of computations on encrypted data, it may not support all types of operations. Some computations, particularly those involving complex data structures or iterative algorithms, can be challenging to perform efficiently in a homomorphically encrypted domain.
- Size Expansion: Homomorphic encryption can cause significant expansion in the size of the encrypted data compared to the original unencrypted data. This can be a concern, especially when dealing with large datasets.

- Adaptation of Applications: Existing applications and algorithms may need to be adapted or restructured to work with homomorphic encryption. This can be a barrier to the widespread adoption of this technology.

- **Proposed Research:**

  This research objective is to develop a novel hardware-based solution aimed at addressing challenge such as Performance, Implementation Issues, Lack of Real-World Testing, Quantum-Safe Key management. The key characteristics of the proposed encryption hardware is listed below:

  - Design and implement a hardware accelerator for post-quantum cryptographic algorithms to enhance performance.
  - Address implementation challenges, ensuring robustness against side-channel attacks, fault-injection attacks, Differential Power Analysis (DPA), and Tempest Attacks.
  - Conduct extensive real-world testing to validate the effectiveness and practicality of the proposed hardware solution.
  - Develop quantum-safe key management protocols suitable for integration into existing cryptographic systems.

  Regarding the HE, the main objective of this research would be to design a hardware capable of the performing neural network inference on the encrypted data. The hardware focus would be on efficient addition and subtraction. Leverage parallel processing capabilities and optimized memory management to enhance overall performance.The objectives of this research are:

  - Break down neural network inference computations into homomorphic encryption-supported operations, emphasizing addition, subtraction, and minimizing multiplications.
  - Design a specialized hardware accelerator targeting homomorphic encryption operations to significantly improve computational efficiency.
  - Mitigate key management challenges associated with homomorphic encryption, ensuring secure and efficient use.
  - Adapt the proposed hardware accelerator for seamless integration into neural network applications

- **Method:**

  The methodology to carry out the PQC research proposal could be breakdown into following phases:

  - Phase 1, Hardware Design and Verification: Design a specialized hardware architecture optimized for PQC encryption, focusing on enhancing performance while minimizing costs. Considerations will include parallel processing capabilities, efficient memory management, and power consumption optimization.
  - Phase 2, Implementation Robustness: Implement countermeasures against common cryptographic attacks, including side-channel attacks, fault-injection attacks, DPA, and Tempest Attacks. Employ techniques such as secure coding practices, constant-time algorithms, and hardware-based protections to fortify the implementation against potential vulnerabilities.
  - Phase 3, Real-World Testing: Conduct comprehensive real-world testing in various scenarios to evaluate the proposed hardware's performance, scalability, and compatibility with existing systems. Collaborate with industry partners and organizations to simulate diverse deployment environments.

- Phase 4, Quantum-Safe Key Management: Develop and implement quantum-safe key management protocols that ensure the security and integrity of cryptographic keys. Evaluate the resilience of these protocols against both classical and quantum attacks.

The methodology to carry out the HE research proposal could be breakdown into phases:

- Phase 1, Neural Network Optimization: Explore the methods (such as sparsity) to minimize the number of computations required to perform inference. Since, the HE computations are expensive, this phase can significantly improve the overall performance.
- Phase 2, Operation Breakdown: Analyze neural network inference computations to identify opportunities for minimizing multiplicative operations. Propose strategies to restructure computations and replace multiplications with more homomorphic encryption-friendly additions and subtractions.
- Phase 3, Implementation: This phase aims to implement the HE based neural network inference engine on hardware. In this research proposal, Field Programmable Gate Arrays (FPGAs) are chosen as the initial implementation target for their reconfigurability, affordability, and speed.
- Phase 4, Verification and Testing: This phase aims to test the designed hardware and verify the functionality. The patterns are encrypted using He algorithms and would serve as inputs to test the HE based NN inference engine. The obtained accuracy should be closed to the accuracy obtained from the hardware.
- Phase 5, Real-world Application: Explore methods to seamlessly integrate the designed hardware accelerator into existing neural network applications. Address compatibility issues and provide adaptation guidelines to facilitate widespread adoption.

- **Current Research:**

  While working as a postdoctoral researcher at the University of Windsor, I began my research in cryptography by focusing on creating efficient hardware for multiplying binary polynomials. The results of this project were successfully published in a well-known journal.

  Afterwards, I shifted my focus to Post-Quantum Cryptography (PQC) and Homomorphic Encryption (HE) algorithms. I worked on improving the efficiency of hardware for multiplying large integer polynomials, a crucial aspect in PQC and HE cryptography systems. Specifically, I addressed the challenge of slow and resource-intensive polynomial multiplication by using the Number Theoretic Transform (NTT), a widely adopted algorithm.

  This work was completed during my part-time role as a researcher at the University of Windsor, resulting in the filing of a provisional patent. Currently, we are working on obtaining a patent for the developed circuit. Additionally, a circuit was developed based on this concept to perform hardware multiplication of extremely large integers for Fully Homomorphic Encryption (FHE), addressing the challenge of dealing with very large numbers. This research in under review for publication.

  Regarding the Neural Networks, where I strategically utilized sparsity to achieve a significant reduction in the number of parameters by almost 80%, without compromising accuracy. This reduction substantially lowered the computation required for inference tasks. The overarching goal is to apply these techniques to reduce computational requirements when performing inference on the encrypted data using HE.

- **Research Program Feasibility:**

The first phase involves optimizing algorithms for hardware implementation using Python for simulations and FPGAs for efficiency measurement. FPGAs, being cost-effective and flexible, are advantageous over designing and fabricating a VLSI ASIC. After testing, the design can be fabricated for final evaluations. Three defined projects include studying post-quantum cryptographic algorithms, investigating homomorphic encryption and ciphertext computation algorithms, and designing an architecture and circuit for efficient hardware implementation.

- **Funding and Grant Potential:**

  Leveraging my industry background and familiarity with industry problems, I plan to secure funding for the research. I have successfully written research proposals with industry partners to obtain MITACS grants in the past.

  - Natural Sciences and Engineering Research Council of Canada (NSERC): NSERC provides grants to support research in natural sciences and engineering, including computer science and cryptography.
  - Tech Companies:

    IBM Research: Companies like IBM have research divisions that may fund projects related to cryptography and encryption.
    Microsoft Research: Microsoft has an interest in various areas of cryptography and may provide research grants.
  - Canadian Institutes of Health Research (CIHR): CIHR may provide funding for research projects that involve the intersection of health data and encryption technologies.
  - Mitacs: Mitacs offers collaborative research internships and training programs that connect researchers with industry partners. It could be a valuable resource for projects with practical applications.
  - Canada Foundation for Innovation (CFI): CFI supports state-of-the-art infrastructure for research. If your project involves the development of specialized equipment or facilities, CFI might be a relevant funding source.
  - Defence Research and Development Canada (DRDC): DRDC, as the research arm of the Canadian Department of National Defence, may fund projects related to cryptographic solutions with applications in defense and security.
  - Federal Economic Development Agency for Southern Ontario (FedDev): Ontario support academic research in emerging technologies through FedDev.

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," 2024.

Research Proposal: A biologically inspired neuromorphic processor

- **Summary:**

  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.

- **Introduction:**

  A Spiking Neural Network (SNN) is a type of artificial neural network inspired by the way biological neurons communicate in the brain. Unlike conventional neural networks, which are based on the concept of continuous activation values (e.g., in feedforward or recurrent neural networks with sigmoid or rectified linear unit activations), SNNs model the information processing in terms of discrete spikes, or action potentials. The information is encoded in the temporal domain, taking into account the timing and rate of the firing of action potentials. Overall, SNNs are faster and more energy efficient comparing to conventional neural networks [1,2].

  Neuromorphic systems include a large number of spiking neurons, synapses and their interconnecting structure on hardware. Such systems are highly parallel, fast, fault tolerant, intelligent and compact. Further, Neuromorphic systems often operate in an event-driven manner, processing information only when there is a change or event in the input, rather than continuously processing static data. This event-driven approach can lead to increased energy efficiency. This research focus is on neuromorphic systems implementing Spiking Neural Networks (SNNs).

- **Challenges:**

  Implementing Spiking Neural Networks (SNNs) poses several challenges, both in terms of hardware and software aspects. In the following, some of these challenges are outlined.

  - Training Complexity: Training SNNs is more challenging compared to conventional neural networks. The discrete and temporal nature of spikes makes it difficult to apply traditional backpropagation algorithms directly. Developing effective and efficient training algorithms for SNNs, is an active area of research.
  - Sparse Connectivity: In biological neural networks, connectivity between neurons is often sparse. Implementing and optimizing sparse connectivity efficiently in hardware poses challenges.
  - Temporal Precision: The temporal dynamics of SNNs play a crucial role in information processing. Achieving high temporal precision in hardware implementations is challenging, especially in the presence of noise and variability.
  - Energy Efficiency: While SNNs are expected to be more energy-efficient than traditional neural networks, achieving this efficiency in hardware implementation requires specialized architectures. Developing low-power neuromorphic hardware that can efficiently handle spiking dynamics is a significant challenge.

- Real-Time Processing: SNNs are well-suited for real-time processing, but achieving low-latency implementations on hardware platforms is a challenge. This is particularly important for applications such as robotics and sensor networks

The objective of this research is to contribute to advancements in neuromorphic hardware, novel training algorithms, and dedicated hardware frameworks to help overcome some of the limitations associated with the implementation of neuromorphic systems.

- **Proposed Research:**

  This research proposal aims to address these challenges by designing and implementing a neuromorphic hardware platform on FPGA (Field-Programmable Gate Array). The primary objectives include the design of a hardware architecture optimized for SNNs on FPGA, development of hardware-friendly training algorithms, addressing challenges related to temporal precision and real-time processing, and achieving energy-efficient spiking neural processing.

- **Method:**

  The methodology to carry out this the PQC research proposal could be breakdown into following phases:

  - Phase 1, Training Algorithm: This phase focuses on optimizing training algorithms suitable for hardware acceleration, with a focus on the temporal dynamics of SNNs .Spike-timing-dependent plasticity (STDP) is a popular learning rule observed in the synapses of biological neural networks. It refers to the phenomenon where the strength of a synaptic connection between two neurons is modified based on the relative timing of their spikes (action potentials). STDP is a form of Hebbian plasticity, a concept derived from Donald Hebb's hypothesis that states "cells that fire together wire together." The STDP rule can be summarized as follows:

    If a presynaptic neuron fires shortly before a postsynaptic neuron, the synaptic strength is potentiated (increased).

    If a postsynaptic neuron fires shortly before a presynaptic neuron, the synaptic strength is depressed (decreased).

    At end of this phase, an optimized version of STDP is developed and its learning capabilities are validated through simulations and experiments This research aims to use novel methods such as Time To First Spike (TTFS) to ehance the speed and energy efficiency of the neuromprhic hardware. TTFS refers to the time it takes for a neuron to generate its first action potential (spike) in response to a specific input stimulus. TTFS can modulate the learning window of STDP, allowing neurons with shorter TTFS to contribute more to synaptic potentiation. During unsupervised learning, neurons that respond quickly (short TTFS) to specific patterns in the input data can have their connections strengthened, enhancing their sensitivity to those patterns. Regarding the inference, neurons with shorter TTFS may be preferentially assigned to represent specific features or patterns in the input data, leading to a form of spike-based coding. Therefore, applying TTFS could considerably improve the inference time comparing to the rate coding in SNNs. Furthermore, it would also contribute to reducing power consumption.

    Another methods would be utilized in this research is to optimize the neuromorphic system is sparsity. There are two main aspects of sparsity in SNNs:

    Sparse Connectivity: In a sparsely connected network, each neuron typically receives input from only a subset of the neurons in the previous layer. This sparse connectivity is thought

to be more biologically realistic, as not all neurons in the brain are connected to every other neuron.

Sparse Activity: Sparse activity refers to the fact that at any given time, only a small fraction of neurons in the network are active or "spiking." Most neurons remain inactive, and only a few neurons produce spikes in response to specific stimuli.

Using sparsity contribute considerably to improve the neuromorphic hardware performance and efficiency. Some of the advantages of Sparsity in SNNs are listed below:

Energy Efficiency: Sparse connectivity and activity contribute to energy efficiency. In a sparse network, fewer connections need to be updated, reducing the overall energy consumption during information processing. This is particularly important in neuromorphic computing, where mimicking the brain's energy-efficient processing is a goal.

Computation Efficiency: Sparse connectivity reduces the computational load on the network. During information propagation, only a fraction of neurons need to be updated, leading to more efficient computations.

Noise Robustness: Sparse networks tend to be more robust to noise. The presence of sparse activity allows the network to focus on relevant information while ignoring irrelevant or noisy input.

Facilitates Learning: Sparse connectivity and activity can facilitate the Spike-Timing-Dependent Plasticity (STDP) leraning, which relies on the precise timing of spikes between connected neurons.

In summary, sparsity in SNNs is advantageous for achieving more biologically plausible, energy-efficient, and computationally efficient neural network models. Combining sparsity with TTFS could considerably improve the existing neuromorphic platfroms.

- Phase 2, Hardware Design and Optimization: In this research proposal, Field Programmable Gate Arrays (FPGAs) are chosen as the initial implementation target for their reconfigurability, affordability, and speed. This phase will involve the design and optimization of a detailed hardware architecture for SNNs, considering FPGA constraints and capabilitie. The designed hardware would be implemented using hardware description languages (e.g., Verilog or VHDL) on FPGA. using hardware description languages (e.g., Verilog or VHDL) for FPGA implementation. Training algorithms suitable for hardware acceleration will be implemented and optimized.
- Real-Time Processing Optimization: This phase mostly involve investigating methods to optimize the hardware to minimize processing delays and achieve real-time performance. Accuracy of neuromorphic system should also be evaluated and methods to enhance temporal precision in spike communication and processing on the FPGA need to be investigated.
- Energy Efficiency Evaluation: At this phase, experiments are designed to measure and evaluate the energy efficiency of the implemented neuromorphic hardware. Although FPGAs are not optimized for minimum power consumption, at very first step the energy efficiency of the FPGA-based solution could be compared to state-of-the-art FPGA neuromorphic implementation. Some methods such as clock gating could be utilized to improve the power consumption.

- **Current Research:**

  I started my research in neuromorphic engineering during my M.Sc. dissertation titled "Digital Implementation of a Simple Model for Astrocyte Calcium Oscillations." In this project, I made a biological astrocyte work on hardware using a technique called Piecewise Linear (PWL) approximation. After that, I explored spiking neural networks and neuromorphic engineering.

As a Ph.D. student, I used the COordinate Rotation DIgital Computer (CORDIC) method to set up the Izhikevich neuron and online spike time-dependent plasticity on hardware [5]. I chose CORDIC because it's good at calculating tricky stuff precisely and works well in hardware, unlike other methods like PWL.In another project, I made a digital version of a realistic astrocyte and glutamate-release mechanism. The hardware I designed could handle complex calculations precisely and had decent performance. This is important because simulating realistic models with lots of details using high-level models takes a long time and needs a lot of computer power. This hardware is helpful for mimicking the tripartite synapse and its parts.

Throughout my time as part-time research associate at University of Windsor, a method was presenting for reducing power consumption in an artificial neural network, the method comprising: receiving an input signal; modulating a sampling frequency of an artificial neuron based on the input signal; and forwarding the input signal or a further input signal obtained from the input signal to the artificial neuron at the sampling frequency. A US patent was obtained for the proposed method [6].

In another work, Selective Input Sparsity (SIS) method proposed for edge inference applications in image classification where the image acquisition environment is controlled. These sparsely connected networks are well-suited to area-constrained applications as they require fewer neurons and synapses than baseline Fully Connected (FC) networks of analogous structures. The SIS networks require fewer hardware resources and make inferences faster than the baseline FC networks without substantial impact on the classification accuracy [7].

- **Research Program Feasibility:**

  The research project comprises four key phases. The initial phase involves studying algorithms and optimization techniques for neuromorphic hardware. This phase is conducted without the need for specialized equipment and is primarily planned to be simulated using the Python programming language. The next phase focuses on designing and implementing the hardware, with a primary emphasis on verifying functionality. FPGAs are employed during this stage for implementation, allowing for the validation of functionality and the measurement of design efficiency. In the third phase, FPGAs are also used in optimizing performance to meet Real-Time Processing requirements. In the final stage, the emphasis shifts towards ASIC (Application-Specific Integrated Circuit) implementation. While an initial evaluation can be performed on FPGAs, it is noteworthy that FPGAs are not inherently power-efficient devices

- **Funding and Grant Potential:** Leveraging my industry background and familiarity with industry problems, I plan to secure funding for the research. I have successfully written research proposals with industry partners to obtain MITACS grants in the past.
  - Natural Sciences and Engineering Research Council of Canada (NSERC): NSERC is a federal agency that provides funding for research in natural sciences and engineering. Their Discovery Grants program may support projects related to neuromorphic engineering.
  - Tech Companies:

    IBM Research: IBM has a significant interest in neuromorphic computing and artificial intelligence. IBM Research may provide funding for projects aligned with their neuromorphic computing research objectives.

    Intel Labs: Intel is actively involved in research and development in neuromorphic computing. This may provide funding opportunities through Intel Labs, particularly in areas related to hardware and architecture.

    Google Research: Google has a strong focus on artificial intelligence and machine

learning. Google Research may offer funding or collaborative opportunities for projects related to neuromorphic engineering and SNNs.

NVIDIA: NVIDIA is a key player in the graphics processing unit (GPU) market and has been involved in AI research. They may support research projects that leverage GPU technology for neuromorphic applications

- Canadian Institutes of Health Research (CIHR): CIHR focuses on health-related research, and certain programs within CIHR may support studies that involve neural networks and brain-related technologies.
- Canada Foundation for Innovation (CFI): CFI provides funding for research infrastructure.While working on neuromorphic engineering projects, I may be abe to receive support for acquiring or upgrading relevant equipment and facilities.
- Mitacs:
- Mitacs collaborate with academia, industry, and government, and their programs may be applicable to research in neuromorphic engineering.
- National Research Council Canada (NRC): NRC is the Government of Canada's research organization. Collaborative projects related to neuromorphic engineering may find support through various NRC programs.
- Federal Economic Development Agency for Southern Ontario (FedDev): Ontario support academic research in emerging technologies through FedDev.

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] Brzosko, Z., Mierau, S.B. and Paulsen, O., 2019. Neuromodulation of spike-timing-dependent plasticity: past, present, and future. Neuron, 103(4), pp.563-581.

[4] Rueckauer, B. and Liu, S.C., 2018, May. Conversion of analog to spiking neural networks using sparse temporal coding. In 2018 IEEE international symposium on circuits and systems (ISCAS) (pp. 1-5).

[4] M. Heidarpur, A. Ahmadi, M. Ahmadi and M. Rahimi Azghadi, "CORDIC-SNN: On-FPGA STDP Learning With Izhikevich Neurons," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 66, no. 7, pp. 2651-2661, July 2019

[5] Mirhassani, M., Heidarpur, M. and Leigh, A.J., University Of Windsor, 2023. Dual State Circuit for Energy Efficient Hardware Implementation of Spiking Neural Networks. U.S. Patent Application 17/984,612.

[6] A. J. Leigh, M. Heidarpur and M. Mirhassani, "Digital Hardware Implementations of Spiking Neural Networks With Selective Input Sparsity for Edge Inferences in Controlled Image Acquisition Environments," in IEEE Transactions on Circuits and Systems II: Express Briefs, vol. 70, no. 5, pp. 1724-1728, May 2023

Teaching Philosophy

Inspiration: Growing up in the presence of my father, a dedicated teacher, profoundly influenced my educational philosophy. He was a masterful guide who fueled my passion for learning by posing thought-provoking questions, stimulating my curiosity and shaping my approach to critical thinking. Instead of providing direct answers, he encouraged me to explore and discover solutions independently.

This formative experience became the bedrock of my teaching philosophy, emphasizing the important role of critical thinking in education. My aim is to gradually but firmly establish curiosity and foster creativity, ultimately transforming students into innovative and knowledgeable individuals.

Inquiry: I believe the most effective way to engage students is through inquiry-based learning. Students are more likely to embrace a new concept when they perceive it as a solution to a problem in their minds. The approach involves initiating the class with well-chosen questions and allowing students to explore the topic with guidance from the teacher.

In this method, I express the fundamental problem, instill a desire to find the answer, and facilitate class discussions. My role is that of a moderator leading students through a challenging experience designed to promote discussion, critical thinking, and discovery. For instance, when starting Digital Logic Design at the beginning of the semester and discussing number systems, I began with the question, "Why is the decimal system predominant, and not, for instance, octal or hexadecimal?"

After discussing this, I posed the next question, "Now, why do machines use the binary number system?" I noticed more students engaged in answering the second question when the first question was discussed beforehand, compared to classes where I directly presented the second question. This method also fosters a conceptual understanding of problems and solutions in electrical engineering, enabling students to connect different concepts and apply engineering methods creatively.

A Deep Understanding: A successful teaching method involves a combination of various techniques. Another technique I find particularly useful is cognitive learning, where the focus is on understanding the subject at a deeper level rather than memorizing approaches to specific problems. My approach to this process includes three elements: first, students need to understand why they are learning the subject; second, they should gain knowledge about the subject at a deep level; and third, they should contemplate the application of what they learned.

Course contents should be designed to ensure students acquire a deep understanding and develop the skills to apply their knowledge in their field. For example, when presenting logical operations (AND, OR, and NOT) in a Digital Logic Design class, I explained the concept of an idealized switch network, gave simple examples, and asked students to identify different combinations and create separate components. Subsequently, I introduced Boolean algebra and logical operations as tools to analyze and design circuits algebraically in terms of logic gates.

Creativity: Arguably the most crucial aspect of learning, especially at the highest level, is creativity. The scientific approach to creativity involves studying and mastering existing achievements, asking questions, proposing solutions, designing experiments to validate proposed solutions, and communicating research with other scientists to receive feedback.

My plan to involve graduate and last-year undergraduate students in research includes providing them

with sufficient background and knowledge in a specific area I believe has research potential. I will ask them to identify and compile a list of new and noteworthy works published in the subject. Subsequently, they will write briefs on those papers, highlighting their contributions.

The next step involves presenting the papers to deepen their understanding of the works. I firmly believe that explaining something to someone else enhances insight into the topic. Therefore, such conferences will be a fundamental part of my approach, helping students evaluate literature and communicate their findings. The subsequent phase will include a critical analysis of the papers, requiring students to consider the weaknesses, limitations, and drawbacks of proposed approaches. Conducting simulations to replicate and test findings from the papers will help them learn necessary tools and approaches, facilitating problem-spotting.

At each phase, it is my responsibility as a teacher to evaluate their work, provide feedback, and offer suggestions for improvement. This process allows students to enhance their ability to identify problems, review literature for solutions, propose new solutions, and effectively communicate their research.

In summary, I aspire to impart the qualities that meant the most to me during my education: inquiry, deep understanding, and creativity. I aim to instill a love for engineering in my students, as I personally feel an infinite passion for it

Teaching Interests

In my previous teaching roles, I found great joy in breaking down complex ideas and creating an environment where students can comfortably engage with the material. These experiences have solidified my commitment to pursuing a long-term career in teaching.

My love for transferring knowledge aligns with my interest in developing course materials and teaching in areas such as digital logic design, computer architecture, embedded systems, system-on-chip, and microprocessor-based systems. In particular, courses such as Introduction to Digital Systems, Introduction to Computer Organization and Architecture, Computer Organization, Computer Systems Design, Microprocessor Systems. Having taught courses like Computer Architecture and Digital Systems, and with industry experience focusing on embedded systems and logic design, I feel prepared to offer a new perspective based on industry applications.

I would enjoy teaching courses related to cybersecurity and cryptography as well. Currently, I teach Cybersecurity I and Cybersecurity II at the University of Windsor's Department of Continuing Education. These courses cover a range of topics, including social engineering hacking techniques, network attacks, data protection, secure protocols, cryptographic algorithms, authentication methods, and wireless network security. My research in cryptography, particularly in post-quantum algorithms and homomorphic encryption, further enriches my ability to provide relevant and up-to-date instruction.

The other topic that I am interested in teaching is artificial intelligence (AI), with a PhD thesis centered on AI and and published several research papers. I have also mentored MSc and PhD students in AI thesis and am eager to develop course materials for subjects such as Artificial Intelligence and Neural Networks, leveraging both my research and practical experiences.

Moreover, I have experience in networking as I worked as digital logic designer for a L2 switch for the past two years. I am interested in teaching Computer Networks courses that cover topics Networking Fundamentals, Routing and Switching, Basics of Transmission Systems an network architecture. I am also interested in teaching courses related to signal processing and Digital Signal Processing. Furthermore, I have experience and interested in teaching courses relate to electronics such electronics I and II and digital electronics and cover topics transistors, diodes, op Amps, amplifier design, gate design , analysis power dissaption and delay.

In summary, I am eager to contribute to Carleton University through my diverse background and passion for education. My past teaching experiences, coupled with my academic and research foundation as well as industry experience, put me in a good position to become dedicated educator.

Teaching Experience

Instructor, Contniue Eduation, University of Windsor, ON, Canada. *2023-Present*

- Teaching Cybersecurity I : Introduction to Systems Security and Cybersecurity II: System Implementation in the department of continue education in University of Windsor. This courses are offered remotely where students learned about different types of cyber attacks and how to secure computers, networks and servers. Course materials, attendance and quizzes and grading are done int he Brightspcae.

Mentor, University of Windsor, ON, Canada. *2020-Present*

- Closely supervising and mentoring two PhD and three master students on weekly meeting basis. Helping them to gain fundamental knowledge, identifying problems, literature survey for solutions, and critical analysis of published works. Both PhD students managed to publish IEEE transaction papers in their second year of PhD and have more papers in review and preparation. Master students are performing research experiments at the moment. As a mentor, I provided guidance and evaluated progress of an undergraduate student to finish his project.

Graduate Teaching Assistant, University of Windsor, ON, Canada. *2018-2020*

- Prepared materials, tutorials and answered student questions as a teaching assistant. During labs, I helped students to formulate their ideas to flowcharts and further to codes to implement on FPGA, Arduino or Raspberry Pi evaluation boards and eventually debugging it.

  Courses: Digital Logic Design II (DLDII), Embedded Systems and Electronics I

Lecturer, Islamic Azad University, Kermanshah, Iran. *2014-2018*

- Delivered lectures, designed, prepared and developed courses and teaching materials and assessed students. Supervised research activities of students including final year undergraduate projects.

  Courses: Digital Logic Design, Computer Architecture and Analog CMOS Integrated Circuits, Electronics.

High School Teacher, Chamran High School, Eslamabad Gharb, Iran. *2009-2010*

- Designed courses, instructed and evaluated students, worked with weaker students in individual, graded exams and communicated with parents about students progress.

  Courses: Electronics, Electronics Measurements.

Teaching Methodology

As an enthusiastic educator, my teaching methodology centers on creating a dynamic and interactive learning environment that empowers students to actively participate in their educational journey. Through a combination of traditional and modern approaches, I aim to cultivate critical thinking, communication skills, and a deep understanding of the subject matter.

- **Recorded Lecture** Engaging and informative lectures will form the foundation of the course, providing a comprehensive overview of key concepts and theories. Lectures would be enriched by utilizing multimedia resources, real-world examples, and case studies to enhance the learning experience. My plan is to record the lectures prior to the session ans share the video with with students. This way, there would be more time during the class students would be involved by discussions, questions and group projects.
- **Oral Questions by Teacher Answered Orally by Students:** I aim to actively ask questions to encourage students to understand the need to learn the topic and participate in discovering the solution to the problem that course address. This approach promotes critical thinking, reinforcing key concepts and fostering a collaborative learning atmosphere.
- **Class Discussion Conducted by Teacher:** Facilitating lively class discussions to encourage students to express their opinions, ask questions, and engage in critical analysis. Incorporating diverse perspectives to enrich the learning experience and promote a deeper understanding of the subject matter.
- **Presentations by Student Panels from the Class:** I am planning to incorporate student presentations in my courses, providing opportunities for them to develop research and communication skills. This approach not only encourages teamwork but also allows students to take ownership of their learning.
- **Reading Assignments in Academic Journals:** Assigning relevant readings from academic journals to deepen theoretical knowledge. Emphasizing the importance of staying current with scholarly literature and developing the ability to critically evaluate research.
- **Reading Assignments Related to Topic with Application in Industry:** I am planning to give reading assignment about application of course topics in the industry. The objective here is to explore real-world implications and connections between academic knowledge and industry practices.

In summary, by incorporating lectures, questions, discussions, student presentations, and a balance of academic and industry-related readings, I seek to equip students with a depp understanding of the subject, preparing them for success in both academic and professional pursuits.

Record of Teaching Effectiveness

Teaching at High School:

My first teaching experience was at a high school. I underwent a four-month intensive training before I started teaching, where I took courses on teaching methods, student evaluation, psychology, and the rules and regulations of teaching. I passed these courses with high grades and was very enthusiastic to start teaching and I was hoping that I would be a very good teacher. I prepared slides and course materials that went beyond the textbook and covered more advanced topics. I wanted to share all my knowledge with the students and I thought that would be great. However, after a few sessions, I noticed that the students couldn't answer my questions, which I thought were easy. Therefore, in the next session, I asked them for their feedback on the course. I received the following feedback from students:

"*Thank you for going the extra mile to ensure that we understand the material in depth, but we are confused and we lose track of what is essential and what is additional information just to support the course content.*"

I realized that it was not very helpful to go beyond the necessary materials for the course. It only caused confusion and difficulty for the students to understand the main topics. I revised the course materials and removed the extra ones. After a few more sessions, I asked the students for their feedback. They were happy that the course only covered the basic materials, but they still had difficulty because I explained the topics in a complex way. I realized that I should have considered their age and level of class.

Frankly, my teaching performance was below my expectations the first time I taught this class. This is evident in the average score that I received for the class, which was a 15/20. The department's average score for this course in the past years was a 18/20.The exams posed a challenge with questions that required a novel approach, designed by me. Subsequently, in the course review, I received feedback stating,

" *The exam questions are not covered by the teacher.*"

Although the topics were indeed covered, some questions demanded a deeper understanding and a certain level of creativity in responses, which I realized might be too much for high school students. Conducting a root cause analysis to identify the issues, I identified three main points:

- I deviated too much from the main course topics and covered unnecessary material.
- I explained topics in a detailed and complex manner.
- The exams were excessively difficult for high school students.

The key lesson learned is the need to focus more on the main course topics and use simpler language to explain the materials. Exam questions should also align more closely with the covered topics.

University Seasonal Lecturer:

My next teaching experience was as a seasonal lecturer at a university. This was very different from teaching high school students, as the audience and the course were more advanced. Here, the students had chosen to take this course this semester, and they had the option to delay it until later in their program. The first course I taught was computer architecture. When I prepared the course materials, I applied the lesson I had learned from teaching in high school. I tried to focus on the essential concepts and use simple language. Since my audience was college students, I avoided repeating basic concepts and only covered the course materials. I hoped that this course would go better than the previous one. During the course, I noticed that the students asked questions, which I saw as a positive sign compared to my last class where I hardly got any questions. I generally felt that the students were engaged. After a few sessions, I asked the students for their feedback again. This time, the feedback was mainly about the gap in the topics that I assumed the students already knew. Some of the feedbacks I received was such as:

"*You seem to be very excited about sharing your knowledge with the students, but you assume that we already know some things. Some of these concepts were not taught before and this makes the lectures hard to follow.*"

"*You don't explain the topics in a simple and clear language.*"

"*Using examples would make it easier to understand.*"

Based on this feedback, I updated the course materials and added more examples and simpler explanations. I also noted the concepts that I expected the students to know and checked their familiarity with them before proceeding with the course. The exam grades improved compared to my previous experience and the students achieved an average of 16/20, which was the usual grade for this course. At the end of the class, I received more feedback from the students. Some of the issues they raised were:

" *speaking too quickly, reading directly from the notes and not making eye contact, giving unclear definitions and examples*.

When I reviewed my class, I looked at the feedback again and thought about what I could do better. I realized that I had to understand who I was teaching. I had to know what year they were in, what they had learned before, and what courses they had taken. I had overestimated the students' level. So, the first thing I did was to adjust the course materials and include the concepts that had not been taught before. The next thing I did was to prepare a student course packet that had a more detailed outline of my lectures, diagrams, charts, and overheads. This course packet was more comprehensive and covered the concepts that were necessary to understand the course topics.

After implementing changes, I revised the information on slides, allowing for a higher-level explanation of the course. This approach clarified the concepts and the reasons behind the materials we were studying. Upon revisiting the course, I observed a notable reduction in student confusion, as they became more aware of what was crucial to understand and what details were less critical.

To enhance comprehension, I included simple examples into the slides, which proved highly effective in helping students' understanding of the concepts. Additionally, I introduced weekly assignments featuring more intricate problems. This strategy provided students with the opportunity to tackle complex questions and foster creativity in finding solutions.

To balance assessment, I allocated marks between exams and assignments. As a result, I received

overwhelmingly positive feedback this time. Despite the exams containing more challenging questions, the inclusion of assignments allowed students to successfully tackle these complexities. Consequently, overall grades improved compared to the previous semester.

In my role as a teaching assistant, I created materials and tutorials, answering student questions during labs. I helped students develop ideas into flowcharts and then into codes for implementation on boards like FPGA, Arduino, or Raspberry Pi, offering support in debugging. This experience deepened my understanding of including diversity and inclusion concepts. I assisted students during labs, office hours, and outside my assigned times, responding to their questions through email or in-person interactions. This is an example that even while preparing for my final exam, I set aside time for students.

During this period, the professor, who was originally teaching the course, requested me to conduct a session in his absence.

Hi Moslem:

If you are available and willing, please consider giving a lecture on VHDL in my next Monday (Jan. 14) from 1 to 2:20. I have an important meeting with industry people at 11:30 and I may not be able to start the class on time. If you can do this, please let me know ASAP.

It is totally up to you, you don't have to give this lecture if you are busy.

I gladly accepted the professor's request and promptly started preparing for the session, based on my prior experiences. Having served as a teaching assistant for the same course, I was already acquainted with the students. The session exceeded my expectations, allowing for a more discussion of theory rather than focusing solely on lab work. Despite being a single session and without creating course materials, I successfully covered all the necessary course content. Overall, I received positive feedback from students during my time as a teaching assistant at the University of Windsor.

Subsequently, I held a postdoctoral position at the University of Windsor, collaborating with master's and PhD. students, offering assistance with their projects. I shared the knowledge I had gathered during my PhD, aiding them in debugging their code and reviewing their papers. The outcomes were highly positive, as these students successfully graduated with a commendable record of publications. Throughout this period, I acquired valuable experience in leadership and mentorship.

This marked my initial experience as an instructor in Canada. Despite not being responsible for creating course materials and labs, I tried to introduce some changes, incorporating a few new labs to align the course more closely with my intended coverage.

After two sessions, I sought feedback from students through two questions:

What do you think I did well and would like me to continue doing? What do you think I can do better, and what suggestions do you have for improvement?

Regarding the positive feedback, students appreciated the way I explained the topics in a clear and understandable language.

" slides seems complicated but the way that you explain it make it much easier"

One of the positive feedbacks that I received was about the live drawing that I did in the class. From my experience teaching in college, I knew that I should not take for granted that students know basic concepts that may seem very simple to me. So, I always asked students if they were familiar with the concepts or not and if they were not, I used my skills with Inkscape to make quick drawings and explain the concepts.

Students were also positive about Real-world examples that I did during the class. For instance, when I discussed the concept of "Whaling" as a type of social engineering attack, I gave a real-life example of how in 2019, an attacker pretended to be the CEO of an Austrian aerospace manufacturer and fooled the company into sending 42 million euros to their account. I showed the page that described the attack and

shared the link in the meeting chat. I believe such examples really helped to interest the students and they were very useful in involving them in the course.

Positive feedback included appreciation for my ability to explain topics in an easy and understandable language, even when the slides were perceived as complex. I was pleased to have learned from past experiences that no concept is inherently too complex, and it ultimately depends on the instructor's experience and understanding to convey it in an accessible manner. The live drawing during class received praise as well, aiding in clarifying concepts and not assuming familiarity with basic ideas.

Real-world examples, such as illustrating the concept of "Whaling" with a specific case, were also positively received. Providing concrete examples, like the 2019 impersonation attack on an aerospace manufacturer, engaged students and enhanced their understanding of the course content.

I also received some suggestions to improve the course. The main issue was that the class was not interactive and I was talking most of the time. This was new for me as this was not a problem for the students in my previous classes and I quickly realized that they were right and this was something I completely overlooked. After the session, I thought about it and made a major change and later in the session I increased the student participation in the class significantly. When I wanted to introduce a new topic, I tried to help students understand why we were learning that topic and what was the challenge and how the technique taught in the topic could be a solution to the challenge. I asked them to share if they had any experience with any of the attacks or security measures and tools discussed in the course and to my surprise some of them had very good experience and by sharing their examples they enhanced the course greatly.Overall, after implementing these changes, the class received very positive written comments from students, indicating a successful adaptation to their feedback.

"Thanks so much Moslem. Enjoyed every minute. Fantastic job."

"Thank you Moslem good stuff"

"Thank you Moslem! Really enjoyed the session"

"Thank you very much for all of your effort with us"

In conclusion, my journey to become a better teacher has taken me from receiving disappointing feedback and doubting my teaching skills when I was a high school teacher to now where I have a fair amount of experience and my last teaching session was not flawless but it was close to what I envisioned. Thanks for your consideration

Diversity and Inclusion Statement

I am committed to create a welcoming environment in my classroom where everyone feels included. Diversity, to me, means embracing the different backgrounds and experiences that students bring. I believe each student have to feel valued and free to express themselves and a diverse classroom is essential for preparing students to thrive in an interconnected world.

Diversity, extends far beyond demographics; it comprises of a range of identities and experiences, including race, ethnicity, gender, sexual orientation, socioeconomic background, disability, and cultural heritage. I am committed to acknowledging and celebrating diversity within my teaching and throughout the academic community.

- Inclusive Teaching Practices: In my teaching, I employ inclusive practices that accommodate diverse learning styles and needs. I strive to create an environment where every student feels valued and heard. This involves employing a variety of instructional methods, offering diverse course content, and incorporating inclusive language.

- Accommodations for Diverse Learning Styles: Recognizing that students have varied learning styles and needs, I am dedicated to providing accommodations that ensure equal access to educational opportunities. This may involve adapting materials, implementing flexible assessment methods, and leveraging technology to enhance accessibility.

- Cultural Competence: I actively seek to enhance my cultural competence by engaging in ongoing education and self-reflection. I understand the importance of cultural sensitivity and strive to create an atmosphere that respects and appreciates diverse cultural perspectives.

- Creating a Welcoming Environment: I am dedicated to creating a welcoming and supportive environment for all students. My teaching philosophy emphasizes openness to diverse perspectives and a commitment to addressing any issues related to bias or discrimination in a proactive and constructive manner.

My commitment to promoting diversity and inclusion in academia is grounded in my personal experience. During my PhD in Canada, I was fortunate to work alongside insightful faculty members in University of Windsor. I was truly inspired by their commitment to social justice, diversity and inclusion. I have had the opportunity to address diversity and inclusion in my roles as Graduate Assistant and Postdoctoral Fellow at University of Windsor. I am committed to create an environment free from discrimination based on the race, religion, sex, economic status, sexual orientation, disability or other characteristics.