Carleton University | Department of Systems and Computer Engineering

SCI-LAB

Carleton Secure Cryptographic Implementations Lab (SCI-LAB)

Research Day on:

Side-Channel-Resilient Post-Quantum Security in Digital-Twin Structural Health Monitoring Systems

10:00 am to 3:30 pm on Monday, June 29th, 2026

The Nicol Building, Room: NI4040, Carleton University [map]

Research Day Chair: Mostafa Taha

Time	Session
10:00 – 10:20	Arrival (coffee/tea)
10:20 – 10:30	Introduction and Welcoming
10:30 – 11:15	Keynote: Real-Time Infrastructure Intelligence Using IoT-Based Structural Health Monitoring Dr. Mohamed Abdelraheem, Rochester Institute of Technology - Dubai.
11:15 – 12:00	Side-Channel Leakage Resiliency in Resource-Constrained Embedded Systems Dr. Mostafa Taha, Carleton University.
12:00 – 13:00	Lunch Break
13:00 – 13:45	OHLF: A Novel Systemic and Secure Approach for Evaluating Encrypted Logic Functions Using Homomorphic Encryption Dr. Mahmoud Sayed, Carleton University.
13:45 – 14:30	Memory-Efficient GPU Acceleration for High-Throughput Falcon Post-Quantum Signatures Shazly Ahmed, PhD Candidate, Carleton University.
14:30 – 15:15	Post-Quantum Privacy-Preserving Deep Learning Inference with Logic Gate Networks under TFHE Mahmoud Yassin, PhD Candidate, Carleton University.
15:15 – 15:30	Networking and Closing Remarks.

This event is in-person, free, and open to the public.
Registration is required [registration link]

Carleton University | Department of Systems and Computer Engineering

SCI-LAB

Title: Real-Time Infrastructure Intelligence Using IoT-Based Structural Health Monitoring

Abstract: This talk presents an overview of our recent work on IoT-enabled Structural Health Monitoring (SHM), with a focus on vibration-based monitoring and smart infrastructure applications. The talk will describe two main system models: a cloud-based SHM framework, where monitoring data is processed remotely, and a hybrid fog–cloud framework, where part of the analysis is performed locally while more advanced assessment is handled in the cloud. These models demonstrate how IoT can support scalable, cost-effective, and practical SHM solutions.

The talk will also present applications of the proposed systems on different structural settings, including multi-story building models and suspension bridge experiments. In addition, related work on IoT-based drive-by road condition assessment, road roughness estimation, and road anomaly detection and classification will be discussed. Finally, the talk will highlight future research directions, particularly the use of AI and advanced learning models for automated structural health assessment, damage identification, and decision support.

Bio: MOHAMED ABDELRAHEEM (Senior Member, IEEE) is an Associate Professor of Electrical Engineering and Computing Science with Rochester Institute of Technology (RIT) Dubai, UAE. He also holds a Professor position with the Electrical Engineering Department, Assiut University, Egypt, from which he is currently on sabbatical leave. He has held several academic and administrative leadership positions, including serving as Chief Information Officer at Assiut University, Egypt, and as Head of the Information Technology Department at Assiut Universal Technological University, Egypt. He is a Royal Academy of Engineering Leaders in Innovation Fellow. He has served as a principal investigator on several funded research projects supported by STDF and ITIDA in Egypt and by the Academic Research Committee (ARC) at RIT Dubai. His research interests include wireless networking, the Internet of Things, embedded systems, and IoT-based structural health monitoring.

Title: Side-Channel Leakage Resiliency in Resource-Constrained Embedded Systems

Abstract: This talk introduces side-channel analysis (SCA) in embedded systems and the security challenges arising from physical information leakage in cryptographic implementations. The presentation begins with an overview of the principles of side-channel analysis and the main classes of countermeasures: hiding, masking, and leakage-resilient design. Particular attention will be given to the practical limitations of traditional defenses in resource-constrained devices and the motivation for leakage-resilient approaches that maintain security even in the presence of bounded information leakage.

The talk will then present recent advances in leakage resiliency based on limiting the amount of known or controlled input data. We will discuss applications of this approach to hashing (SHA-3), a new lightweight random number generator and stream cipher; Keymill, and a leakage-resilient mode of operation for the AES block cipher.

Bio: MOSTAFA TAHA (Senior Member, IEEE) is an Associate Professor in the Department of Systems and Computer Engineering at Carleton University, Canada, and the founder and director of the Secure Cryptographic Implementations (SCI) Lab. He earned his Ph.D. in Computer Engineering from Virginia Tech, USA. His research interests span hardware security, embedded systems, and applied cryptography, with a particular emphasis on the security-aware design, analysis, and evaluation of embedded and cyber-physical systems. His work focuses on understanding and mitigating implementation-level threats, including side-channel analysis, fault-injection attacks, and other attacks targeting cryptographic implementations. He is an active member of the Institute of Electrical and Electronics Engineers (IEEE) and the International Association for Cryptologic Research (IACR).

Title: OHLF: A Novel Systemic and Secure Approach for Evaluating Encrypted Logic Functions Using Homomorphic Encryption

Abstract: Privacy-preserving computation is becoming increasingly important in scenarios where one party owns sensitive data while another party owns a proprietary model, function, or algorithm. A central challenge in this setting is Private Function Evaluation (PFE): how can a private function be evaluated on private data without revealing the function to the data owner or the data to the function owner?

In this seminar, we will discuss this challenge and introduce Oblivious Homomorphic Logic Function (OHLF), a new framework for PFE that protects both data and functions, built on top of the TFHE fully homomorphic encryption scheme. Unlike traditional approaches based on universal circuits or secure multiparty computation, which often suffer from high computational and communication costs, OHLF uses generalized oblivious logic gates that combine logic evaluation and routing within a single homomorphic operation. This design significantly reduces the complexity of representing and evaluating private functions.

The talk will present the main ideas behind OHLF, its modes of operation including PFE, and explain how it differs from universal-circuit-based approaches and discuss its practical impact through experimental results.

Carleton University | Department of Systems and Computer Engineering

SCI-LAB

Bio: Dr. MAHMOUD ABDELHAFEEZ SAYED is a Postdoctoral Researcher in Systems and Computer Engineering at Carleton University and an IEEE Member. He received his Ph.D. from Carleton University, where he was awarded the Senate Medal for Outstanding Academic Achievement. His research focuses on secure and efficient embedded and edge systems, spanning applied cryptography, IoT platforms, sensing technologies, and hardware implementation. His academic services include multiple collaborations and projects with other industrial and academic partners in Canada and internationally and reviewing roles in multiple journals and international conferences.

Title: Memory-Efficient GPU Acceleration for High-Throughput Falcon Post-Quantum Signatures

Abstract: Post-quantum cryptography is moving from theoretical standardization to practical deployment, where digital signature schemes must support high-throughput services at cloud scale. Falcon/FN-DSA is a promising post-quantum signature scheme due to its compact signatures and strong security guarantees; however, scaling Falcon signing efficiently on GPUs remains challenging because of its high computational complexity and strict memory requirements. This presentation introduces saFalcon, a GPU-based implementation of Falcon-512 designed to improve the practicality of large-scale post-quantum signing. The talk highlights the motivation behind accelerating Falcon, the core architectural challenges in deploying it for high-volume services, and a comprehensive performance and security evaluation of saFalcon on modern NVIDIA GPUs. Our results demonstrate that saFalcon can achieve up to 755k Falcon-512 signatures per second, highlighting the potential of memory-efficient GPU acceleration for practical, large-scale post-quantum authentication

Bio: SHAZLY AHMED is a PhD candidate in Systems and Computer Engineering at Carleton University. His research focuses on hardware-accelerated cryptography, post-quantum cryptography, and fully homomorphic encryption. His portfolio includes implementing TFHE on FPGA platforms and developing high-performance GPU implementations of post-quantum cryptographic algorithms. His research aims to bridge the gap between cryptographic theory and practice by optimizing performance, memory efficiency, and scalability on modern hardware platforms.

Carleton University | Department of Systems and Computer Engineering

SCI-LAB

Title: Post-Quantum Privacy-Preserving Deep Learning Inference with Logic Gate Networks under TFHE

Abstract: Deep learning is widely used in applications such as image analysis, medical diagnosis, cybersecurity, and infrastructure monitoring. When inference is outsourced to cloud or edge servers, an important privacy question arises: how can a model make predictions on sensitive data without revealing that data to the server? In a post-quantum security context, this challenge becomes even more relevant.

Torus Fully Homomorphic Encryption (TFHE) enables computation directly on encrypted data. However, existing approaches that integrate conventional neural networks with TFHE remain expensive due to the cost of arithmetic operations, quantization, and programmable bootstrapping. To address this challenge, Mahmoud investigates Deep Differentiable Logic-Gate Networks, which are discretized after training into learned Boolean circuits. This allows encrypted inference to be performed through homomorphic evaluation of logic gates rather than arithmetic neural-network layers.

In this talk, Mahmoud will introduce a new framework, EI-DDLGN, and its client–server encrypted inference workflow. He will present experimental results on accuracy, latency, model architecture, gate distributions, and programmable-bootstrapping cost. The results show that EI-DDLGN achieves competitive accuracy while providing a more efficient and TFHE-aligned model for encrypted inference.

Bio: Mahmoud Yassin is a Ph.D. Candidate in the Department of Systems and Computer Engineering and the Secure Cryptographic Implementations Lab (SCI-Lab) at Carleton University, where his research focuses on privacy-preserving AI and secure machine learning systems, particularly deep learning models that operate directly on encrypted data for confidential and quantum-safe AI applications. He has received several awards and scholarships, including Carleton University's Outstanding Teaching Assistant Award, the GSA PhD Scholarship, and the Dr. Thomas Betz Memorial Award.