Saif Eddine Nouma, PhD Candidate

Address: Tampa, FL 33612
Cell: (+1) 813-859-9830
E-mail: saifeddine.nouma@gmail.com
Webpage: https://saifnouma.github.io/

Research Interests

My research interests include **applied cryptography, network security, and machine learning**, with a focus on advancing the security and efficiency of emerging computing platforms. I am also interested in the security and optimization of digital twins by leveraging post-quantum cryptography, edge computing, and distributed machine learning.

Education

Doctor of Philosophy in **Computer Science** — Aug 2021-Feb 2026
University of South Florida — Tampa, FL, USA
- GPA: 3.9/4.0
- Advisor: Dr. Attila Altay Yavuz
- Thesis: Lightweight and Resilient Cryptographic Protocols for Internet of Things

Bachelor of Science in **Computer Science** — Aug 2017-Jan 2020
University of Carthage — Tunis, Tunisia
- Advisor: Dr. Khalil Drira
- Thesis: Applications of Machine Learning in Networking and IoT

Associate of Science in **Mathematics** — Aug 2015-Jun 2017
University of Monastir — Monastir, Tunisia

Experience

Graduate Research Assistant — Aug 2021-present
University of South Florida, Tampa, FL, USA

System Administrator — Aug 2023-Jun 2024
University of South Florida, Tampa, FL, USA

Graduate Teaching Assistant — Aug 2021-Dec 2021
University of South Florida, Tampa, FL, USA

Software Engineer — Jul 2020-Jul 2021
Kopileft Services Inc., Tunis, Tunisia

ML Engineer Intern — Jan 2020-Jul 2020
LAAS-CNRS, France, Toulouse

ML Engineer Intern — Jun 2019-Aug 2019
Wevioo, Tunis, Tunisia

patents & publications

Patent

[P2] Attila A. Yavuz, **Saif E. Nouma**. System and Method for Cryptographic Forensic Audits on Lightweight IoT and Digital Archives. **US Patent** US20240007300A1, 2024.

[P1] Attila A. Yavuz, **Saif E. Nouma**. Hardware Supported Authentication and Signatures for Wireless, Distributed and Blockchain Systems. **US Patent** US20230308289A1, 2023.

Journals

[J5] Attila A. Yavuz, Saleh Darzi, **Saif E. Nouma**. LiteQSign: Lightweight and Quantum-Safe Signatures for Heterogeneous IoT Applications. ***IEEE Access***, 2025. (*Impact factor: 3.6*)

[J4] Aaron Pendino, Nghia Nguyen, **Saif E. Nouma**, Jing Wang, Attila A. Yavuz, Yasin Yilmaz, Gokhan Mumcu. (2025). Additively Manufactured RF Electronics with Structurally Integrated Physically Unclonable Functions for Wireless System Security. ***IEEE Access***, 2025. (*Impact factor: 3.6*)

[J3] Kiarash Sedghighadikolaei, Attila A. Yavuz, **Saif E. Nouma**. Signer-Optimal Multiple-Time Post-Quantum Hash-Based Signature for Heterogeneous IoT Systems. ***Internet of Things***, 2025. (*Impact factor: 7.6*)

[J2] **Saif E. Nouma**, Attila A. Yavuz. Lightweight and Resilient Signatures for Cloud-Assisted Embedded IoT Systems. *Wiley Security and Privacy. arXiv preprint arXiv:2409.13937. (Impact factor: 2.1)*

[J1] **Saif E. Nouma**, Attila A. Yavuz. Post-Quantum Hybrid Digital Signatures with Hardware-Support for Digital Twins. *ACM Transactions on Multimedia Computing, Communications, and Applications* ***(ACM TOMM)***, 2024. *(Impact factor: 6.0)*

CONFERENCES

[C7] **Saif E. Nouma**, Attila A. Yavuz. Lightweight and Breach-Resilient Authenticated Encryption Framework for Internet of Things. In *43rd IEEE Military Communications Conference* ***(IEEE MILCOM)***, 2025.

[C6] **Saif E. Nouma**, Attila A. Yavuz. Practical Cryptographic Forensic Tools for Lightweight Internet of Things and Cold Storage Systems. In *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation* ***(ACM/IEEE IoTDI)***, 2023.

[C5] **Saif E. Nouma**, Attila A. Yavuz. Post-Quantum Forward-Secure Signatures with Hardware-Support for Internet of Things. In *58th IEEE International Conference on Communications* ***(IEEE ICC)***, 2023.

[C4] **Saif E. Nouma**, Attila A. Yavuz. Lightweight Digital Signatures for Internet of Things: Current and Post-Quantum Trends and Visions. In *6th IEEE Conference on Dependable and Secure Computing* ***(DSC)***, 2023.

[C3] Attila A. Yavuz, Kiarash Sedghighadikolaei, Saleh Darzi, **Saif E. Nouma**. Beyond Basic Trust: Envisioning the Future of NextGen Networked Systems and Digital Signatures. In *5th IEEE Conference on Trust, Privacy and Security in Intelligent Systems and Applications* ***(IEEE TPS-ISA)***, 2023.

[C2] Attila A. Yavuz, **Saif E. Nouma**, Thang Hoang, Duncan Earl, Scott Packard. Distributed Cyber infrastructures and Artificial Intelligence in Hybrid Post-Quantum Era. In *4th IEEE Conference on Trust, Privacy and Security in Intelligent Systems and Applications* ***(IEEE TPS-ISA)***, 2022.

[C1] Attila A. Yavuz, Duncan Earl, Scott Packard, **Saif E. Nouma**. Hybrid Low-Cost Quantum-Safe Key Distribution. In ***Quantum 2.0*** – *Optica*, May 2022, MA, USA.

E-PRINTS

[E3] Saleh Darzi, **Saif E. Nouma**, Kiarash Sedghi, Attila A. Yavuz. QPADL: Post-Quantum Private Spectrum Access with Verified Location and DoS Resilience. *arXiv preprint arXiv:2510.03631*, 2025. *Under review at IEEE Transactions on Information Forensics and Security (IEEE TIFS). (Impact factor: 8.0).*

[E2] **Saif E. Nouma**, Attila A. Yavuz. Lightweight and High-Throughput Secure Logging for Internet of Things and Cold Cloud Continuum. *arXiv preprint arXiv:2506.08781*, 2025. ***Minor revision*** *at ACM Transactions on Internet of Things (TIoT). (Impact factor: 3.5)*

[E1] **Saif E. Nouma**. (2020). Applications of Machine Learning (ML) in Networking and IoT. hal-02932494.

Teaching Experience

Guest Lecturer

- CIS 4930/6930: Cryptography: Theory and Practice	Fall 2025
- CIS 4212/6214: Privacy-Preserving and Trustworthy Cyber-Infrastructures	Spring 2024

Graduate Teaching Assistant

- CIS 4212/6214: Privacy-Preserving and Trustworthy Cyber-Infrastructures	Spring 2026
- COP 4538 IT Data Structures	Fall 2021

Research Experience

Graduate Research Assistant Aug 2021 - Present

University of South Florida, Tampa, FL

I designed and implemented efficient authenticated encryption primitives, including:

- Graphene: Designed efficient and compromise-resilient authenticated encryption constructions based on AES-GCM and Chacha20-Poly1305 standards, with full-fledged implementation on 32-bit ARM Cortex-M4, achieving orders-of-magnitude performance improvements and low-latency compared to the state-of-the-art counterparts, presented at IEEE MILCOM 25. My implementation is open-source at `https://github.com/saifnouma/graphene`

- Diamond: Improved the Graphene scheme by incorporating an efficient key update and more algorithmic formality with provable security. Extensive performance evaluation on embedded devices, 64-bit ARM Cortex-A72 and 8-bit AVR ATmega2560 confirms the efficiency of Diamond over Graphene and NIST lightweight cryptographic standard Ascon. My implementation is open-source at `https://github.com/saifnouma/diamond`

I designed and implemented efficient digital signature primitives for constrained devices, including:

- LRSHA: Designed and implemented an efficient and resilient digital signatures by leveraging distributed cloud assistance and secure hardware Intel SGX. Extensive performance evaluation on 8-bit AVR ATmega2560 and commodity hardware confirms LRSHA's efficiency. My implementation is open-source at `https://github.com/saifnouma/lrsha`
- POSLO: Designed efficient secure logging protocol, achieving extended battery longevity on constrained devices. Developed a novel GPU-accelerated algorithm for batch verification of large logs on the cloud, resulting in significant speedup compared to baseline CPU. Our work resulted in filing one US patent and publications at ACM/IEEE IoTDI 23 and ACM TIoT 25. My implementation is open-source at `https://github.com/saifnouma/poslo`
- HYHASES: Designed efficient, forward-secure, and post-quantum digital signatures with TEE hardware support, implemented on 8-bit AVR ATmega2560 and Intel SGX, achieving 34× better efficiency than NIST ML-DSA standard, presented at IEEE ICC 23. I later extended this work to a hybrid signature, leveraging a conventional aggregate signature to significantly reduce bandwidth overhead and energy usage on low-powered devices. The extended work is published in ACM TOMM 2024. My implementation is open-source at `https://github.com/saifnouma/hyhases`

Professional Experience

System Administrator Aug 2020-Jun 2021

University of South Florida, Tampa, FL

- Developed and configured real-time dashboards and alert rules using Prometheus and Grafana stacks, tracking I/O network throughput and node/container health across an HPC cluster and the machines of the college infrastructure
- Developed Ansible roles and playbooks to support continuous integration and task automation

Software Engineer Jul 2020-Jul 2021

Kopileft Services Inc., Tunis, Tunisia

- Improved e-commerce backends by migrating Java-based SOAP web services to Kotlin, developed services on Apache Tomcat, and implemented Exposed-based data-access layers with PostgreSQL
- Implemented the BI reporting and dashboard infrastructure by optimizing ≈ 50% of SQL queries and stored procedures written in PostgreSQL, improving data freshness and reliability

ML Engineer Intern Jan 2020-Jul 2020

LAAS-CNRS, Toulouse, France

- Implemented and benchmarked LSTM/GRU models using TensorFlow and scikit-learn on a real-world network traffic (1.6 TB capture), achieving 3% MAPE and halving error compared to SVR. My implementation is open-source at https://github.com/SaifNOUMA/Network-Traffic-Prediction
- Implemented a distributed early-exit CNN model for edge IoT networks using TensorFlow, containerized with Docker, and performed communication using ZeroMQ, enabling faster inference. My implementation is open-source at https://github.com/SaifNOUMA/Edge-Computing/tree/master/dnn_partitioning
- Developed and implemented a DQN algorithm for dynamic task offloading and resource allocation in multi-user edge computing, using ns3-gym, achieving improved latency-energy tradeoffs. My implementation is open-source at https://github.com/SaifNOUMA/Edge-Computing/tree/master/task_offloading_optimization

ML Engineer Jun 2019-Aug 2019

Wevioo, Tunis, Tunisia

- Developed, trained, and fine-tuned a Siamese CNN (S-CNN) with contrastive loss on a collected real-world dataset of genuine/forged handwritten signature pairs for fake signature detection
- Collaborated with computer-vision team on signature extraction from handwritten bank checks and deployed the prototype to local banks, which served as a major step towards mitigating fraud

skills

Programming Languages: C/C++, Assembly, Python, Java, Kotlin, MATLAB, CUDA

Machine Learning: TensorFlow, PyTorch, Scikit-learn, Pandas, NumPy, Matplotlib

Security & Cryotography: OpenSSL, WolfSSL, Mbed-TLS, MITRE ATT&CK, SGX

DevOps: Git, SVN, Docker, Ansible, Prometheus, Grafana, Nagios, Slurm

Database: PostgreSQL, MySQL

Embedded Hardware: ARM Cortex-M4, ARM Cortex-A72, 8-bit AVR ATMega series

PUBLIC TALKS

Research paper presentation at IEEE MILCOM, Los Angeles, CA, USA 2025

PhD major area Presentation at Tampa, FL, USA 2024

Research paper presentation at IEEE DSC, Tampa, FL, USA 2023

Research paper presentation at ACM/IEEE IoTDI, San Antonio, TX, USA 2023

SERVICES

Reviewer

- Blockchain: Research and Applications (Elsevier), Computer Networks (Elsevier), Reliability Engineering and System Safety (Elsevier), Security and Privacy (Wiley) 2025
- IEEE Transactions on Information Forensics and Security (IEEE TIFS) 2024

REFERENCES

References are available upon request

Last updated: December 14, 2025