Saif Eddine Nouma

3720 Spectrum Blvd, IDR 400, Tampa, FL, 33620
saifeddine.nouma@gmail.com https://saifnouma.github.io

Education

Ph.D. 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

B.S. in **Computer Science** *Aug 2017-Jan 2020*
École Polytechnique de Tunisie *Tunis, Tunisia*
- Advisor: Dr. Khalil Drira
- Thesis: Applications of Machine Learning in Networking and IoT

A.S. in **Mathematics** *Aug 2015-Jun 2017*
Institut Préparatoire aux Études d'Ingénieurs de Monastir *Monastir, Tunisia*

Experience

Graduate Research Assistant *Aug 2021-present*
University of South Florida *Tampa, FL, USA*
- Funded by: NSF, DoE, Cisco Systems
- Working on efficient and breach-resilient digital signatures and AEs for Internet of Things.
- Working on the design of lightweight and high-throughput cryptographic protocols.

System Administrator *Aug 2023-Jun 2024*
University of South Florida *Tampa, FL, USA*
- Developed real-time monitoring dashboards using Grafana and Prometheus.
- Automated routine tasks with Ansible playbooks to improve efficiency.

Graduate Teaching Assistant *Aug 2021-Dec 2021*
University of South Florida *Tampa, FL, USA*
- Courses: COP 4538 IT Data Structures.

Software Engineer *Jan 2021-Aug 2021*
Kopileft Services Inc. *Tunis, Tunisia*
- Developed web services using Kotlin, Gradle, and the Exposed framework.
- Enhanced 50% of BI infrastructure via optimized SQL queries and Java-based dashboard.

Research intern *Jan 2020-Dec 2020*
LAAS-CNRS *Toulouse, France*
- Developed and benchmarked RNNs to forecast network traffic.
- Designed and implemented early-exit distributed CNNs for Internet of Things.

Intern *Jun 2019-Aug 2019*
Wevioo Consulting *Tunis, Tunisia*
- Implemented a Siamese CNN model for the verification of handwritten signatures.
- Deployed in client infrastructures to authenticate handwritten bank checks.

PATENTS & PUBLICATIONS

PATENT

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

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

JOURNALS

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

2. 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. (*IF: 3.6*)

3. 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. (*IF: 7.6*)

4. **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. *(IF: 6.0)*

CONFERENCES

1. **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.

2. **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.

3. **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.

4. **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.

5. 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.

6. 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.

7. 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

1. 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). (IF: 8.0).*

2. **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). (IF: 3.5)*

3. **Saif E. Nouma**, Attila A. Yavuz. Lightweight and Resilient Signatures for Cloud-Assisted Embedded IoT Systems. *arXiv preprint arXiv:2409.13937. Minor revision at Wiley Security and Privacy. (IF: 2.1)*

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

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

SELECTED PROJECTS

Graphene: https://github.com/SaifNOUMA/Graphene *2025*
• Designed a breach-resilient authenticated encryption (AE) framework for IoT

POSLO: https://github.com/SaifNOUMA/POSLO *2024*
• Introduced a GPU-accelerated secure logging framework for cold-storage servers

HYHASES: https://github.com/SaifNOUMA/HyHASES *2024*
• Proposed the first hybrid post-quantum digital signature scheme with hardware support

NTP: https://github.com/SaifNOUMA/Network-Traffic-Prediction *2020*
• Built RNN-based predictive models to forecast fine-grained network traffic patterns

PUBLIC TALKS

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

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

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

Services

Reviewer

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

References

Attila Altay Yavuz, Ph.D., University of South Florida

Yao Liu, Ph.D., University of South Florida

Srinivas Katkoori, Ph.D., University of South Florida

Mehran Mozaffari Kermani , Ph.D., University of South Florida

Last updated: October 31, 2025