Samira Oliva Madrigal

linkedin.com/in/samiracolivamadrigal
https://samiracolivamadrigal.github.io

CAREER INTERESTS

- Cryptography (PQC), Networking L5/3 Security & IP Routing Algorithms & Protocols, Quantum Computing

EDUCATION

2019 - 2018 **San José State University, San José, CA**
M.Sc. Computer Engineering
Double Specialization: Networking Systems & Secure Systems
Thesis: *Reduction-free Multiplication in GF(2^n) Applicable to Modern and PQC schemes*
Fully-interleaved Montgomery-type product. Tested with FIPS 186-4 ECDSA curves.
Bit-parallel hardware implementation matches speed of BMM.
Applications to PQC schemes, particularly lattice-based schemes.
Software simulation in Python.

2013 - 2017 **San José State University, San José, CA**
B.Sc. Computer Engineering, Minor Computer Science

2010 - 2013 **San José State University, San José, CA**
A.A. Systems Programming

RELEVANT COURSEWORK

- TTL Logic Gate Design, Digital Design (Verilog), Computer Architecture and Design (MIPs), Advanced Computer Design (Verilog), Application-Specific Design for Cryptosystems (Verilog/SystemVerilog), Information Security, Embedded-System Design, Microprocessor Design, Real-Time Embedded System Co-Design, Algorithms and Data Structure Design (C/C++), Advanced Algorithm Design (C), System Software (C), Operating System Design, Compiler Design (x86), Software Engineering, Software Quality Assurance and Testing, Software Security Technologies, Computer Networks, Computer Network Design, Network Security, Network Architecture and Protocols, Network Programming and Applications, Advanced C Programming, C++ for C Programmers, Server-Side Web Programming, x86 Assembly Language, UNIX/Linux, Shell Scripting, Numerical Analysis and Scientific Computing, Linear Algebra, Calculus-based Physics (Mechanics, E&M, Optics & Waves, & Particle)

RESEARCH EXPERIENCE

2019 **San José State University, San José, CA**
NSF Post-Quantum Cryptography Proposal

2019 **San José State University, San José, CA**
Modular Multiplication in $GF(2^n)$

PROFESSIONAL EXPERIENCE

2019 **San José State University, San José, CA**
Graduate Instructional Student Assistant for Network Security
- Galois Field Arithmetic, Public-key & Symmetric-key Cryptosystems, Digital Signatures, Authentication, Kerberos, PKIs, Certificates, L5/3 Security Protocols
- Prepared review notes and graded assignments, quizzes, and exams.

2018 - 2017 **Cisco Systems, Inc., Milpitas, CA**
Software Engineer
- Feature Testing and Automation for next-generation Service Provider.

ACADEMIC PROJECTS AT SJSU

2019 Steganography-based Application with TLS using virtual datastore
2019 Public-Key Infrastructure Application
2019 Index-Calculus Research Project
2018 Port Scanning Research Project
2018 Network Enterprise Project on Embedded Devices
2018 - 2017 Testing & Automation for CPU Infrastructure, BSP, & IEEE 802.3ad
2017 Numerical Methods to Approximate IVPs

2016	FPGA-based Blockchain Accelerator for Ethereum Proof-of-Work
2016	Hardware Implementation of AES based on FIPS-197
2015	32-bit Pipelined MIPs Processor
2014	Crypto Workhorse: Block-Cipher Study with Focus on AES and DES

TECHNICAL SKILLS

- Areas: Applied Cryptography, Internet TCP/IP suite, Post-Quantum Cryptographic Schemes
- Research; System Design, Prototyping, Validation, & Testing in software and hardware
- Systems Programming, Embedded System Design, RTOS, device drivers; assembly language
- Combinational & Sequential Circuits; System Memory; linear, non-linear, & dynamic data structures (e.g., trees, forests, and graphs)
- Spans expertise in hardware, software, & firmware domains.
- Experience: implementing cryptographic algorithms (sw & hw) and testing Internet protocols
- Programming: C/C++/Java, HDLs: Verilog/SystemVerilog, ISAs: RISC (MIPs) and CISC (x86), Scripting: Python/Shell
- OOP (C++/Python), Multithreading, Concurrency, Parallel Processing, Virtualization, Blockchain
- Industry tools: Vivado/ISE, FGPAs, embedded devices, Xcode/Pycharm/Eclipse, Visual Studio/MIPs Assembler, MATLAB, Pytest, TextFSM, routers, switches, line cards, ASR9K, NCSxx, Spirent/Ixia traffic generators, Jenkins, VMs, OS: UNIX/Linux/Windows
- Public/learning tools: Cisco Dcloud, Amazon VPC, GNS3, IBM Quantum/Qiskit
- Familiar with: Quantum Protocols and Algorithms, Quantum Mechanics, Qiskit Quantum Computing Simulator, jupyter-lab, jupyter-notebook, Go, DAPPs in Solidity

LANGUAGES

- Excellent written and verbal communication skills.
- Native: English, Spanish; Full professional working: Italian; Professional working: French; Beginner: Russian.

ACTIVITIES

- IEEE, ACM, IACR, Volunteering at St. Lucy Catholic Parish, Running, Mentoring

AVAILABILITY

- Available to start full-time, preferably in all three tracks (sw, hw, & fw).
- 2020 and part of 2021 were interrupted but remained active with research and development in crypto and networking areas, implementing in Python/C and Verilog. Also learned the fundamentals of quantum computing from qiskit book in Python.