Samira C. Oliva Madrigal

Curriculum Vitae

samira.oliva@sjsu.edu
linkedin.com/in/samiracolivamadrigal
https://samiracolivamadrigal.github.io

CAREER INTERESTS

- Algorithms, Cryptography, Networking L5/3 Security and IP Routing Algorithms & Protocols

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*
Advisor: Gökay Saldamlı.
Fully-interleaved Montgomery-type product. Tested with FIPS 186-4 ECDSA curves.
Studied applications in all the PQC categories, particularly lattice-based schemes.

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

RELEVANT COURSEWORK

- TTL Logic Gate Design, Digital Design, Computer Architecture and Design, Advanced Computer Design, Application-Specific Design for Cryptosystems, Information Security, Embedded-System Design, Microprocessor Design, Real-Time Embedded System Co-Design, Advanced Algorithm Design, System Software, Operating System Design, Compiler Design, Software Engineering, Software Quality Assurance and Testing, Software Security Technologies, Computer Networks, Computer Network Design, Network Security, Network Architecture and Protocols, Network Programming and Application, Advanced C Programming, C++ for C Programmers, Numerical Analysis and Scientific Computing, Linear Algebra

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	Shodan Port Scanning Research Project
2018	Network Enterprise Project on Embedded Devices
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

PUBLICATIONS

Oliva Madrigal, Samira Carolina, "Reduction-free Multiplication in GF(2n) Applicable to Modern and Post-quantum Cryptographic Schemes" (2019). *Master's Theses*. 5074. https://scholarworks.sjsu.edu/etd_theses/5074

TECHNICAL SKILLS

- Research; System Design, Prototyping, Validation, & Testing in Software and Hardware
- Areas: Applied Cryptography & Internet TCP/IP suite
- Programming: C/C++/Java/Go/Python, HDLs: Verilog/SystemVerilog, ISAs: MIPs/x86, Scripting: Shell
- Multithreading, Concurrency, Parallel Processing, Virtualization
- Industry tools: Vivado/ISE, FGPAs, embedded devices, Xcode/Pycharm/Eclipse, Visual Studio/MIPs Assembler, MATLAB, Pytest, TextFSM, ASR9K, NCSxx, Spirent/Ixia, VMs, OS: UNIX/Linux/Windows

LANGUAGES

- Native: English, Spanish; Full professional working: Italian; Professional working: French

ACTIVITIES

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