# Samira C. Oliva Madrigal

Personal Site ◆ GitHub ◆ LinkedIn

## RELEVANT COURSEWORK

- Computer Architecture and Design (MIPs), Advanced Computer Design (Verilog), Application-Specific Design for Cryptosystems (Verilog/SystemVerilog), Microprocessor Design (Linux, C), Real-Time Embedded System Co-Design, Algorithms and Data Structure Design (C/C++), Advanced Algorithm Design (C), System Software (Linux, C), Operating System Design (Linux, C), Compiler Design (Linux, C, NASM x86, Lex), Software Engineering, Software Quality Assurance and Testing, Software Security Technologies (Shodan, Python), Computer Network Design (Linux), Cryptography & Network Security, Network Architecture and Protocols, Network Programming and Applications, Advanced C Programming, C++ for C Programmers, Assembly Language for IA 32 x86 Processors (MASM), Shell Scripting, Numerical Analysis and Scientific Computing, Linear Algebra, Calculus-based Physics Series

## TECHNICAL SKILLS

- Applied Cryptography (Modern & PQC schemes), Internet TCP/IP protocol suite (topology setup, packet analysis, and testing of protocols across all layers), LACP, IP, BGP, TLS, IPSec, System Software, Software Engineering, Hardware Design (Embedded), Digital Design (FPGAs), Research, Requirement Specification, System Design, Implementation, and Testing
- 10+ years with C and Linux. Experience with C++, Java, Python, x86 (MASM/NASM), MIPs, Verilog, SystemVerilog, Pytest, Traffic Generators (IXIA/Spirent), Wireshark Packet Analysis
- Familiar with: Quantum Algorithms & Protocols; LinuxBIOS and OpenSSL source code, BN, Envelope Encryption, and API; FHE; Side-channels (e.g., speculative execution, table lookups, and modular reductions); ensuring constant time algorithms; NIST PQC 3rd Round Finalist's documentation and implementations in C; Multi-Party Computation, SNARKS, and ZK-Proofs (IACR Crypto 2021)

## EDUCATION

2021 **University of Buenos Aires (virtual ECI34), Argentina**
Certificate of Achievement - Quantum Random Number Generators.

2018 - 2019 **San José State University, San José, CA**
M.Sc. Computer Engineering with 3.571 GPA
Double Specialization: Networking Systems & Secure Systems
Thesis: *Reduction-free Multiplication in GF($2^n$) Applicable to Modern and PQC schemes*

2013 - 2017 **San José State University, San José, CA**
B.Sc. Computer Engineering, Minor Computer Science with 3.362 GPA
Senior Project: *FPGA-based Blockchain Accelerator for Ethereum Proof-of-Work*

2010 - 2013 **San José State University, San José, CA**
A.A. Systems Programming with 3.46 GPA; French & Italian Studies with 4.0 GPA

## RESEARCH EXPERIENCE

2022 ZK-Proofs, SNARKS, Multi-Party Computation, Fully Homomorphic Encryption,
Proofs → Algorithms → Implementation

2021 Quantum Computing & qRNG; BaaS: Hyperledger Forks, Quantum-Securing the Blockchain,
Programmable Blockchain SDKs, token-agnostic bartering, & variants

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

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

2016 **San José State University, San José, CA**
Blockchain Industry

## RELEVANT PROFESSIONAL EXPERIENCE

2021 - present **Stealth Mode Startup, Campbell, CA**
Research Scientist in Applied Cryptography & Networking.

Fall 2019 **San José State University, San José, CA**
Instructional Student Assistant for graduate course in Cryptography and Network Security.

2017 - 2018 **Cisco Systems, Inc., Milpitas, CA**
Software Engineer for feature testing and automation of next-generation Service Provider.

## RELEVANT ACADEMIC PROJECTS

2021 AES Software Implementation in C based on FIPS-197
2021 KECCAK Software Implementation in C based on FIPS-202
2021 RSA Software Implementation in C using OpenSSL BN data structure
2021 RSA Software Implementation in C using OpenSSL Envelope Encryption API
2021 $GF(2^n)$ Multiplication in x86 NASM assembly (32/64-bit)
2019 (Group) Steganography Python Application with TLS (OpenSSL, virtual datastore, & sockets)
2019 Public-Key Infrastructure Application using x.509 certificates
2019 Index-Calculus Research Project
2016 (Team) Hardware Implementation of KECCAK based on FIPS-202
2016 Hardware Implementation of AES based on FIPS-197
2015 (Team) 32-bit Pipelined MIPs Processor (Verilog)
2014 Crypto Workhorse: Block-Cipher Study with Focus on AES and DES

## AWARDS & HONORS

2019 Best Homework for graduate course in network programming and applications.
2017 Cisco You Inspire 2 Award - Energetic engineer who takes up lab activities.
2017 Dean's Scholar - 55th annual Honor's Convocation for GPA of 3.64+ for 2+ contiguous semesters.

## LANGUAGES

- Excellent written and verbal communication skills. - Native: English, Spanish; Full professional working: Italian; Professional working: French; Beginner: Russian (reads most Russian; basic speak and written).

## ACTIVITIES

- IACR, EITCI, St. Lucy Catholic Parish, Running, & Active in my areas (learning the latest works presented at IACR etc.)