Samira Carolina Oliva Madrigal

Personal Site ◆ Google Scholar ◆ GitHub ◆ LinkedIn ◆ scolivamadrigal@gmail.com

RELEVANT COURSEWORK

- TTL Logic Gate Design, Digital Design (Verilog), Computer Architecture and Design (MIPs, Verilog), Advanced Computer Design (Verilog), Application-Specific Design for Cryptosystems (Verilog/SystemVerilog), Microprocessor Design (Linux, C), Embedded-System Design (MIPs), Real-Time Embedded System Co-Design, Information Security, Algorithms and Data Structure Design (C/C++), Advanced Algorithm Design (C), System Software (C), Operating System Design (Linux, C), Compiler Design (Linux, C, x86, Lex), Software Engineering, Software Quality Assurance and Testing, Software Security Technologies, Computer Networks, Computer Network Design, Cryptography & Network Security, Network Architecture and Protocols, Network Programming and Applications, Advanced C Programming, C++ for C Programmers, Server-Side Web Programming, Assembly Language for IA 32 x86 Processors, UNIX/Linux, Shell Scripting, Numerical Analysis and Scientific Computing, Linear Algebra, Calculus-based Physics (Mechanics, E&M, Optics & Waves, & Particle)

TECHNICAL SKILLS

- **Areas**: **Applied Cryptography & Internet TCP/IP Protocol Suite**
- **Work**: System Design, Implementing, Prototyping, and Testing
- **Domains**: hardware, software, and firmware
- **Applied Math & Physics**: Field arithmetic, proofs, problems and instances of problems on which crypto constructions are built, IFP, DL, ECDLP, NP problems, J-Invariant, SIS, SIVP, HPP, SVP, LWE, R-LWE, RSD, oil + vinegar, nonlinear multivariate systems of equations, NP-hard, applied linear algebra (e.g. code-based schemes and quantum computing), algebraic constructions, rings, modular multipliers, statistics, probability distributions, FFTs, calculus, differential equations, interference, parallelism
- **Cryptography & Protocols/Algorithms**: symmetric & asymmetric cryptography, KEX, *x.509*, PKI (RFC4949), CA, Kerberos, Layer 3 authentication and/or encryption, elliptic curve cryptography, sieving, OWFs, cryptanalysis, block cipher constructions and analysis, cryptographic hash functions, MACs, HMACs, digital signatures, PRFs, Montgomery, Blakely, BMM, interleaved multipliers, DES, 3DES, AES, RSA, DH, EC-DH, KECCAK, quantum algorithms (Grover, Shor, Simons), post-quantum cryptography, hash-based, lattice-based, code-based, multivariate-based, supersingular elliptic curve schemes, rank-based, consensus algorithms, Fiat-Shamir, Rainbow, McEliece, QC-McEliece, NTRU, CFS, SIDH, qRNG, parameter models (e.g. MOSS), bugs (Hardware, Firmware, & Software)
- **Information Security**: confidentiality, authentication, integrity, secure coding, scanners, viruses, side-channel analysis, speculative execution, constant-time algorithms, gadgets, ROP/JOP, control-flow attacks, remote code execution, DDoS, oracles, buffer overflows, code injections, sniffers, backdoors, cloud, hypervisors, deep web, reconnaissance
- **Networking & Protocols/Algorithms**: topology setup, packet analysis, & testing of Internet protocols across all layers, signal processing, QAM-64, symbol/bit encoding schemes, error-correction, Media Access Control Schemes (e.g., CD-MAC, CA-MAC), ARP, NDP, Spanning Tree Protocol, IEEE 802.3, IEEE 802.11x, PPP, Tunneling, VNPs, VLANs, QoS, IP (v4/v6), CIDR, RFC 1918, MPLS, Multicast, PIM (sparse, dense), IGMP (v4), MLP (v6), IPSec, NAPT, ICMP/v6, DNS, TLS, TCP, UDP, DIJKSTRA, OSPF, IS-IS, iBGP, eBGP, inter-AS routing, intra-AS routing, switching fabric, SDNs, control plane, data plane, Cloud (I/S/P/B as a Service), containers, microservices, sockets, Network OS (e.g., IOS XR) CLI, packet analysis, platform-agnostic (BSPs) system software
- **Digital & Analog Design**: Combinational & Sequential Circuits, Microarchitecture, FSM, Control Unit, Data-Path, Hierarchical Design, System-level Design, System Memory, FreeRTOS, Raspbian, microcontrollers with ARM cortex, LACP1769, LCPExpresso, communication protocols (GPIO, UART, CAN, I2C, etc.), device drivers
- **Programming**: **C pointer-based language**, OOP, C++, Java, **Verilog/SystemVerilog** HDLs, RISC (MIPs) and CISC (x86) ISAs, **Python**, Shell Scripting (bash, tcsh, bourne shell), Multithreading, Concurrency, Parallel Processing (with Python Ray), Virtualization, SEI CERT C Coding Standard, low-level code
- **Computer Science**: linear, non-linear, & dynamic data structures (e.g., trees, forests, and graphs), red-black, m-way trees, hash merkle trees, dynamic programming, complexity theory, space and time algorithmic complexity analysis, hardware analysis (CC count, cell count, critical path delay)
- **Industry Tools**: **Vivado**/ISE, **FGPAs** (Nexsys3, COM-1800, Virtex7), Digilent, **Xcode/gcc/NASM/PyCharm**/Eclipse/Visual Studio/MIPs Assembler/MASM, MATLAB, Pytest, TextFSM, Wireshark, routers (ASR9K, NCSxx), switches, line cards, Spirent/Ixia traffic generators, testbed setup, Jenkins, VMs, OS: MacOS, Windows, UNIX/Linux distros (e.g., Fedora, Debian, Ubuntu, CentOS)
- **Public Learning Tools**: Cisco Dcloud, Amazon VPC, GNS3, IBM Quantum/Qiskit, virtual classrooms
- **Familiar with**: Rust, PKCS # 11, Open Source Projects (e.g., OQS), Go, DAPPs in Solidity, kernel programming, kernel modules, platform firmware, ARM TrustZone, EFI, UEFI, Docker & Kubernetes, building a container from scratch, FIPS-140-3 and related ISO standards, HSMs, PIN cracking, Payment Card Industry (PCI) Security Standards (e.g., Crypto Key Blocks), Quantum Algorithms & Protocols (Qiskit & Jupyter Notebook), LinuxBIOS and patching OpenSSL source code (assembly cryptographic code, BN, Envelope Encryption, and API), Homomorphic Encryption (e.g. Fan-Vercauteren, RLWE), Side-channels (e.g., table lookups and modular reductions), ensuring constant time algorithms, NIST PQC 3rd Round Finalist's documentation and implementations in C, zk-Proofs (from QAPs and EC pairings with HE), zk-SNARKs (e.g., Pincocchio & Aurora), zk trusted setup with Multi-Party Computation (e.g., Zcash), Number Theoretic Transforms

KEY FACETS

- Self-starter, likes to benchmark work against state-of-the-art, fast learner, works excellent in group or individual

EDUCATION

2025 **Télécom Paris / l'Institut Polytechnique de Paris. Palaiseau, France**
PhD Computer Science: Cryptology, Grade Scale 20/20
Thesis: Symmetric-key-based Post-Quantum Advanced Cryptography
Fully funded doctoral three year program with long stay talent researcher French VISA at the prestigious French grande école as part of:
Le Laboratoire de Traitement et Communication de l'Information (LTCI) lab within L'équipe Cybersécurité et Cryptographie [C^2] group
Objectives: considered opportunity to develop strongly abroad in ideal setting to contribute individual ideas as an independent researcher and interesting collaborations, write a good thesis, and become fluent in French. Rigorous study and construction of post-quantum secure cryptographic proofs from PIOP from (ideally) symmetric-key-based primitives with special interest for instances for SNARK-friendly signatures and verifiable encryption and contributions to other related advanced primitives as standalone areas, such as fully homomorphic encryption, post-quantum cryptography, and abstract algebra. Interests for contributions from quantum proofs sans quantum computation and continued work for bootstrapping for CKKS-RNS and verifiable computation.

Thesis concerned areas within my strengths: state-of-the-art in cryptographic proofs (PIOP+PCS constructions), abstract algebra, homomorphic and fully homomorphic encryption, distributed protocols, constructions from simulated MPC protocols, symmetric primitives (OWFs, PRFs, etc.), post-quantum cryptography, and others. Instances of focus: SNARK-friendly signatures, verifiable encryption (e.g. for AES, CKKS-RNS, etc.), using encryption as a commitment, anonymous credentials, and others. Incredibly vast and interesting applications from general transaction validation to path authentication in the notorious Border Gateway Protocol (BGP).

Successfully conducted research for areas of interest ~ 912 hours ⋆ reviewed dozens of articles ⋆ applied rigorous treatment of material ⋆ most recent work verified two major improvements to works of interest ⋆ proposed various novel improvements which qualified for standalone publications and applications to improve distinct problems ⋆ contributed several ideas for original and improved work in the area of cryptographic proofs (zkSNARKs and zkSTARKs) and homomorphic encryption ⋆ **provided immediate direction, explained material in detail, quickly verified results in paper and implemented, and verified computations for the thesis director and advisor ...** ⋆ I was offered fully funded program for Fall school on Geometry in Cryptography and Communication October 2025 at UiT The Arctic University of Norway, Tromsø and invited to present RF-FIKO to mathematical community ⋆ successfully defended thesis on 29 September 2025 ⋆ successfully completed all planned work towards formation: 6 hours of Scientific Research Ethics and 37-38 hours of Advanced French with 100% completion and 99.30% GPA to validate 20h of a foreign language ⋆ participated in several conferences some which took place in Paris and others in Palaiseau; 2 reading group meetings at INRIA.

⋆ Targeted the 40h non-thesis related scientific formation of the 100h formation with geometry of polynomials and side-channel attacks in hardware with state-of-the-art prototyping boards.
⋆ I ended the program in October after a successful thesis defense to pursue independent research by myself back home and allow the opportunity for an honorary PhD. During the first two months I realized I can do so much more by myself with total freedom of deciding what to work on, with whom to collaborate, and attend fall schools/programs that support my special interests. Moreover, practice and 1 person I connect with is all I need to become fluent in French.

Paris is lovely ♡. France will always be in my heart but California is where I feel at home. Voilà.

2025 **l'Institut Polytechnique de Paris. Paris, France**
38h to validate 20h: Advanced French Certificate with 99.30% GPA & 6h Scientific Research Ethics - Certificate

2025 **De Componendis Cifris, Milano, Italy / Università di Trento, Trento, Italy**
Course Attendance Certificate - De Cifris Trends in Cryptographic Protocols - The French Magisterium (2024)
Attended and passed exam for Trends24 from Associazione De Componendis Cifris and Universtà di Trento, Department of Mathematics. Program consisted of 20 lectures in The Almost Perfect Nonlinearity of Substitution Boxes and its Consequences, Algebraic aspects in designing cryptographic functions in symmetric cryptography, Lightweight symmetric primitives, Symmetric Techniques for Advanced Protocols: Design Strategies, and Cryptanalysis, The Transition to Post-Quantum Cryptography, Lattice-based Cryptography (I) & (II), Hardness of the Module Learning With Errors Problem, Diving into Multivariate Cryptography, The Code Equivalence Problem and its Applications to Cryptography, Code-based Cryptography, The Alekhnovich cryptosystem: code-based cryptography with security proofs, Multi-Party Computation in the Head: Techniques and Applications, Polynomial System Solving and Application to Algebraic Cryptanalysis, Tools for cryptanalysis of symmetric primitives, Side-Channel Attacks and Masking Countermeasures, Fully Homomorphic Encryption, Hybrid Homomorphic Encryption, Cryptography for anonymity and accountability, Anonymous Tokens from leading French Cryptographers.

2022 - 2024 **Villanova University, Villanova, PA**
Research and bootstrapping for CKKS-RNS with hardware draft in SystemVerilog based on state-of-the-art work from the Lattigo library implementation in Golang. Collaborated for two excellent publications in 2024 & 2025 (CASA and SMALL). Proposal for 2 year remote formal PhD in ZKP & hardware-based bootstrapping.

2024 **De Componendis Cifris, Milano, Italy / Università di Trento, Trento, Italy**
Course Attendance Certificate - De Cifris Trends in Cryptographic Protocols 2023
Attended and passed exam for Trends23 from Associazione De Componendis Cifris and Universtà di Trento, Department of Mathematics. Program consisted of lectures in Security and Composition of Cryptographic Protocols,

Zero-Knowledge Protocols, Sigma protocols, Vector commitments, Fully Homomorphic Encryption, Threshold Cryptographic Protocols, Private Set Intersection, Hierarchical Key assignment, Protocols for Peer Rating Systems, and Advanced Cryptography in E-Voting from leading Cryptographers.

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

PUBLICATIONS

P. He, S. C. Oliva Madrigal, Ç. K. Koç, T. Bao, and J. Xie. SMALL: Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-based Post-Quantum Cryptography. *International Workshop on Arithmetic of Finite Fields (WAIFI)* Ottawa, Canada, to appear, June 10-12, 2024., Publication

P. He, S. C. Oliva Madrigal, Ç. K. Koç, T. Bao, and J. Xie. CASA: A Compact and Scalable Accelerator for Approximate Homomorphic Encryption. *International Association for Cryptologic Research (IACR) Transactions on Cryptographic Hardware and Embedded Systems* , Volume 2024, No. 2, to appear, 2024., Publication

S. C. Oliva Madrigal, G. Saldamlı, C. Li, Y. Geng, T. Jing, Z. Wang, and Ç. K. Koç. 2023. Reduction-Free Multiplication for Finite Fields and Polynomial Rings. *In Arithmetic of Finite Fields: 9th International Workshop, WAIFI 2022,*Chengdu, China, August 29 September 2, 2022, Revised Selected Papers. SpringerVerlag, Berlin, Heidelberg, 53–78. Publication

Samira Carolina Oliva Madrigal 2019. Reduction-free Multiplication in GF(2n) Applicable to Modern and Post-quantum Cryptographic Schemes. *San Jose Staté University. Computer Engineering.* Publication

PRESENTATIONS

Presented recent work at WAIFI 2024: Scalable Matrix OriginAted Large Integer PoLynomial Multiplication Accelerator for Lattice-based Post-Quantum Cryptography (SMALL). *International Workshop on Arithmetic of Finite Fields (WAIFI)* Ottawa, Canada, to appear, June 10-12, 2024.

Presented paper on behalf of the authors, previous collaborators: Chen Li, Suwen Song, Jing Tian, Zhongfeng Wang, and Çetin Kaya Koç. An efficient hardware design for fast implementation of HQC. *IEEE 36th International System-on-Chip Conference (SOCC), Santa Clara, California, pages 1-6, September 5-8, 2023.* Publication

RESEARCH EXPERIENCE

Active Cryptographic Proofs, Abstract Algebra, MPC Protocols, Post-Quantum Cryptography, FHE ((**bootstrapping [Lattigo & SystemVerilog]**), hardware, embedded

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 & Distributed Applications

RELEVANT PROFESSIONAL EXPERIENCE

2025 - present **Cryptologia, LLC**
Cryptology Consultancy Services.

2022 - 2024 **Academic Research Team**
Researcher in FHE and PQC (Remote)
- Collaboration with small group of Cryptography and Engineering experts and PhD students
- Focus is optimized arithmetic for FHE and PhD work
- Published in IARC for leading RNS-CKKS work (2024)
- Initial draft for bootstrapping in hardware for RNS-CKKS based on Lattigo library
- Published & presented work for WAIFI 2024 (competitive selection) for optimized arithmetic in Lattice-based PQC with applications to HE (2024)

2022 - 2024 **Marvell, Santa Clara, CA**
Senior Engineer, Cryptology
Applied Cryptography and development work in Post-Quantum Cryptography
- algorithm breakdown & analysis and Protocols
- OpenSSL, TLS, FIPS 203, 204, 205, Falcon, Hash-based Signature Schemes (HBS) e.g., HSS & LMS
- underlying mechanism based on Fiat-Shamir paradigm and zero knowledge proofs

- Cryptographic firmware in C; Interfacing with hardware; Software-Hardware Co-Design mapping in Verilog/SystemVerilog and interfacing and mapping for cryptographic core(s) and microcode mapping
- lead cryptographer and developer for PQC; trained and collaborated with two teams
- Platform-agnostic proof of concept solution for acceleration with software-hardware co-design
- vast span across cryptographic engineering work: algorithm assessment and recommendations, cryptoghaphic software, firmware, hardware, research, prototyping, library patching, software requirements specifications, design documents, product mapping, production level development, benchmarking, gtest, unit testing, scripting, end-to-end testing, algorithm optimizations

2021 - 2022 **Startup**

Research Scientist for architecture and development of quantum-secure cryptographic protocols for p2p application.

Fall 2019 **San José State University, San José, CA**

Instructional Student Assistant for graduate course in Cryptography and Network Security.
- Course covered Galois Field Arithmetic, Public-key & Symmetric-key Cryptosystems, Digital Signatures, Authentication, Kerberos, PKIs, Certificates, and L5/3 Security Protocols.
- Prepared review notes for students and graded homework assignments, quizzes, and exams.

2017 - 2018 **Cisco Systems, Inc., Milpitas, CA**

Software Engineer for feature testing and automation of next-generation Service Provider.
- Automated testing of network operating system protocols on different router platforms.
- Unit testing, code review, bug resolution with developers, regression testing, and mentored a remote colleague.
- Technology Stack: Routers, Switches, Traffic Generators, Testbed setup, VMs, GitHub, Jenkins, Linux, Python, and Shell Scripting.

RELEVANT ACADEMIC PROJECTS

2022 Fundamental Zero-Knowledge Protocols with RSA, Schnorr, and discrete log zk-SNARK
2022 Partially Homomorphic Encryption with RSA
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 AES Hardware Implementation in SystemVerilog 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

2024 Marvell Recognition: 7 awards from post-quantum cryptography development team members, including technical leader and director.
2023 Marvell CEO - Game Changer Engineer Award for contributions to Post-Quantum Cryptography (PQC)
2023 Marvell VP Award for PQC
2022 Director & Team Recognition for rigor and innovation in PQC
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, Portuguese

ACTIVITIES

- IACR Crypto 2020 & 2021 and PKC 2022 Conferences, EITCI, Volunteering at St. Lucy Catholic Parish
- Running & Reading & Karaoke & Foreign Languages
- FHE research with academic group since July 2022 (hardware focused) and published work on leading cryptographic journal
- Participated in De Cifris Trends in Cryptographic Protocols 2023
- Participated in several special cryptography conferences in Paris & Palaiseau, France (2025)