MARCELO E. KAIHARA

Agentic AI Engineer · Confidential Computing · Applied Cryptographer

Milan, Italy · mkaihara@pm.me · marcelokaihara.com · linkedin.com/in/mkaihara · github.com/mkaihara

Senior software engineer and PhD in cryptographic hardware with production experience at the intersection of agentic AI, confidential computing, and applied cryptography. Engineered enclave-based key management protecting $2B+ in digital assets at Ava Labs; built a confidential AI agent where secrets are sealed inside Intel SGX with cryptographic attestation; achieved a 246× speedup on zk-SNARK hash primitives; and set a computational record solving the 112-bit ECDLP on a PS3 cluster in collaboration with Microsoft Research. Active CISSP.

WORK EXPERIENCE

Senior Software Engineer Consultant | Sarmap SA · Caslano, Switzerland *06/2024 – 12/2025*

Agentic AI

- Built an AI-agent test automation system (OpenAI SDK, Python, Gradio, SendGrid) that runs satellite-processing test suites via a chat interface and auto-generates email reports. Presented internally as a candidate foundation for a broader testing platform initiative.
- Engineered a multi-agent web application (CrewAI, OpenAI API, Claude API) using a crew of specialized agents (frontend, backend, lead engineer, tester) to build an ML training data editor — reducing delivery from months to weeks.

Satellite Processing & Cloud Migration (ESA CRISP)

- Developed and containerized 14 modular satellite processing pipelines (Docker, Python) for the ESA CRISP programme, covering SAR preprocessing, vegetation indices, flood detection, crop classification, and yield estimation.
- Engineered multi-terabyte data pipelines processing Sentinel-1 SAR and Sentinel-2 optical imagery from raw .SAFE files through to Cloud-Optimized GeoTIFF output.
- Migrated a standalone satellite processing system to a cloud platform (CGI/ESA initiative), eliminating 5 hours/week of manual processing through automated Docker-based orchestration.

Senior Software Engineer Consultant — Bridge | Ava Labs · New York, USA (Remote) *04/2022 – 06/2023*

Enclave-Based Distributed Key Management · Intel SGX / OpenEnclave

- Engineered enclave-side key reconstruction for a distributed bridge-signing system: Shamir key shares from each node were combined exclusively inside the Intel SGX trusted execution environment, eliminating plaintext key exposure to the host OS or any single operator.
- Secured Bitcoin and Ethereum bridge signing infrastructure protecting over **$2 billion in digital assets** — enclave attestation guaranteed no plaintext key exposure.
- Migrated and redesigned the Ethereum bridge infrastructure from Intel SGX SDK to OpenEnclave, eliminating memory corruption bugs and preventing daily bridge restarts.
- Stabilized integration test infrastructure by resolving Docker and Linux system-level issues, reducing deployment failures by 50%.

Senior Software Engineer · Cryptographer | Horizen Labs · Milan, Italy *10/2019 – 02/2021*

Rust Cryptographic Primitives · ginger-lib (open source)

- Implemented the Poseidon hash function in Rust, optimized for zk-SNARK constraint systems across MNT4, MNT6, and BN382 elliptic curves, achieving a **246× improvement** in constraint system performance.
- Contributed hash primitives, large-scale Merkle tree constructions, and multi-scalar multiplication (Pippenger's algorithm) to ginger-lib, Horizen's open-source Rust library for zk-SNARKs.

Cryptography Researcher | EPFL · Lausanne, Switzerland *07/2006 – 06/2011*

- Set a computational record solving the 112-bit elliptic curve discrete logarithm problem on a cluster of 200 PlayStation 3 systems, in collaboration with Microsoft Research.
- Led CHES 2009 as General Chair, a top-tier cryptographic hardware conference with ~300 participants.
- Implemented cryptographic algorithms on GPUs using CUDA and OpenCL.

Algorithm Engineer | Glory Global Solutions International · Bern, Switzerland *10/2011 – 10/2017*

- Designed ML and image processing algorithms for currency recognition systems. Implementation in C++ on embedded systems; simulation in MATLAB.
- Collaborated directly with Japanese engineering leadership, delivering technical presentations on algorithm performance to Glory's Japanese engineering division.

OTHER EXPERIENCE

Independent Consulting & AWS/Docker Certification — *07/2023 – 05/2024*
Independent Research — Algorithmic Trading Platform — *03/2021 – 03/2022*
Research Associate, HES-SO Valais-Wallis — Sion, Switzerland — *02/2018 – 07/2019*
Research Assistant, Nagoya University — Nagoya, Japan — *04/2000 – 03/2006*

SKILLS

Agentic AI	LangGraph, CrewAI, OpenAI SDK, Claude API, multi-agent orchestration
Conf. Computing	Intel SGX, OpenEnclave, TEE architecture, DCAP attestation, Shamir Secret Sharing
Cryptography	Elliptic curves, Poseidon hash, MSM (Pippenger), Merkle trees, zk-SNARK primitives
Languages	Python, Rust, C++ (certified), Go
Blockchain	Cross-chain bridges, zk tooling (Noir, Circom), HSM, key management infrastructure
Infrastructure	Docker, AWS (Solutions Architect certified), CI/CD, Linux
Human Languages	English (C2), Japanese (C2), Spanish (Native), French (B2), Italian (B2)

EDUCATION

Ph.D. in Information Science (Cryptographic Hardware) · Nagoya University, Japan
M.E. in Information Engineering · Nagoya University, Japan
B.E. in Electronics Engineering (cum Laude, top 1–5%) · University of Buenos Aires, Argentina

CERTIFICATIONS & AWARDS

Certifications: CISSP · AWS Certified Solutions Architect – Associate · C++ Certified Professional Programmer · ZK Scaling Bootcamp
Awards: Best Paper Award — CHES 2005 · 1st Place, Horizen Labs Private Proof of Ownership Hackathon Track (ZeroKnowledgeVoting)

SELECTED PUBLICATIONS

J.W. Bos, M.E. Kaihara et al., *"Solving a 112-bit Prime Elliptic Curve Discrete Logarithm Problem on Game Consoles using Sloppy Reduction,"* Int. J. Applied Cryptography, Vol. 2, Issue 3, pp. 212–228, Feb. 2012.
M.E. Kaihara and N. Takagi, *"Bipartite Modular Multiplication Method,"* IEEE Transactions on Computers, Vol. 57, No. 2, pp. 157–164, Feb. 2008.