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 D.Eng. in Information Science specializing in agentic AI, confidential computing, distributed systems, and applied cryptography. Engineered a LangGraph-based CI Failure Triage Agent and a confidential AI agent using Intel SGX, sealed secrets, and DCAP remote attestation as portfolio projects. Implemented SGX-based secure key storage for cross-chain infrastructure at Ava Labs, protecting digital assets worth more than $2B. Contributed performance improvements of up to 246× to zk-SNARK primitives at Horizen Labs and participated in a record-setting computation solving the 112-bit elliptic curve discrete logarithm problem in collaboration with Microsoft Research. Active CISSP.

WORK EXPERIENCE

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

Cloud Migration & Geospatial Processing (ESA Initiative)

- Migrated SNAP and MAPscape satellite-processing systems from standalone desktop environments to the CGI cloud platform, designing Python and Docker-based processing pipelines for multi-terabyte Earth observation datasets.
- Developed and containerized 14 modular satellite-processing pipelines (Docker, Python) for Sentinel-1 SAR and Sentinel-2 optical imagery under the European Space Agency's CRISP program, supporting the transition from desktop software to scalable cloud-based processing services.

Agentic AI Prototypes & Automation

- Shipped an AI-assisted test automation prototype (OpenAI SDK, Python, Gradio, SendGrid) capable of executing satellite-processing test suites through a conversational interface and automatically generating email reports.
- Delivered a web-based editor for correcting ground-truth points used in satellite rice classification, addressing a recurring data-quality problem where points were measured along roads rather than field centers and degraded downstream results. Prototyped and shipped the tool using agentic coding tools (Cline, Claude).

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

Enclave-Based Distributed Key Management · Intel SGX / OpenEnclave

- Developed Intel SGX–based protections for private keys used in Bitcoin and Ethereum cross-chain infrastructure, implementing enclave sealing and secure key handling mechanisms that protected digital assets worth more than $2B.
- Migrated and redesigned Ethereum bridge infrastructure from Intel SGX SDK to OpenEnclave, eliminating memory corruption issues that had forced daily bridge restarts.
- Stabilized integration test infrastructure by resolving Docker and Linux system-level issues, reducing deployment failures by 50%.
- Hardened a Shamir secret sharing CLI for secure handling of mnemonic-based cryptographic secrets.

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× speedup 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.

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

- Designed ML and image processing algorithms for currency recognition systems, implemented in C++ on embedded systems and validated in MATLAB.

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.
- Served as General Chair of CHES 2009, a top-tier cryptographic hardware conference with ~300 participants.
- Implemented cryptographic algorithms on GPUs using CUDA and OpenCL.

OTHER EXPERIENCE

Independent Consulting & Cloud 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
Security Infrastructure	Cross-chain bridges, zk tooling (Noir, Circom), HSM, key management
Infrastructure	Docker, AWS (Solutions Architect certified), CI/CD, Linux
Human Languages	English (C2), Japanese (C2), Spanish (Native), French (B2), Italian (B2), German (B1)

EDUCATION

D.Eng. 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.