JOSE ANGEL CONTRERAS

Tartu, Estonia • +372-5633-9804 •contrerasgedler@gmail.com

EDUCATION

Lomonosov Moscow State University, Moscow, Russia — Jul 2014
MSc Information Security and Cryptography
Thesis topic: *Implementation of a public-key cryptosystem based on Algebraic Surfaces*. Post-quantum cryptography

Universidad Lisandro Alvarado, Barquisimeto, Venezuela — Nov 2010
B.S. in Mathematics
Thesis topic: *A Study of n-forms and De Rham Cohomology*. Algebraic Topology, Differential Geometry

PROFESSIONAL EXPERIENCE

HexTrust, Remote — Oct 2022 - Present
Cryptographer Engineer

- Implemented in Rust an MPC ECDSA protocol with identifiable aborts and integrated into the HexSafe wallet. Optimized the key-generation process and reduced the execution time to less than 400 ms.
- Researched the extension of the protocol into a threshold ECDSA version.
- Implemented the key-derivation process for MPC ECDSA.
- Improved the protocol's security by including non-interactive ZKP protocols in the pre-signing phase, such as Pedersen parameters, Paillier-Blum, and Schnorr.

University of Tartu, Part-time — Apr 2023 - Feb 2024
Scientific Researcher

- Collaborated in the SPATIAL project by adding Homomorphic Encryption for private evaluation of Explainability metrics, enhancing the SPATIAL platform and the trustworthiness of AI algorithms.

Humanode, Remote — Apr 2021 – Oct 2022
Cryptographer

- Successfully combined Fully Homomorphic Encryption of biometric templates, Multiparty Computation, and Zero-Knowledge Proofs to generate private preserving schemes in a decentralized network of ~100 nodes.
- Implemented the feature extraction of biometric templates using a Neural Network in Python with a Rust wrapper. A 50-layer ResNet was adapted to preserve the user's privacy in combination with Lattice-based encryption and Verifiable Secret Sharing.
- Developed an algorithm for generating the parameters of a new decentralized version of the BFV encryption scheme for 128 bits of security and prime numbers with lengths according to homomorphic encryption standards.
- As a result, we published a paper: https://eprint.iacr.org/2022/1673.

Upwork, Remote — May 2017 – Present
Freelancer: Blockchain Developer and Cryptographer

- Worked with more than 20 projects in Blockchain, deployed to Ethereum mainnet different tokens and smart contracts in Solidity.
- Developed the token and was the adviser of a successful ICO for the Mexican Agave industry: https://icoholder.com/en/agavecoin-25742.
- Implemented a food supply network based on Ethereum, which increased transparency and efficiency in the supply chain and connected producers with final consumers.

Cenditel, Merida, Venezuela Sep 2014 - Apr 2017
Research Analyst

- Led a post-quantum cryptography research project, contributing to advancing quantum-safe security solutions using algebraic techniques. The key length was 2x shorter than RSA and ElGamal and was based on a problem with NP-complete complexity. The result was presented at a Conference and published here [paper on Spanish]: http://dx.doi.org/10.13140/RG.2.1.5050.3842.

- Participated in a Machine Learning project on Natural Language Processing, analyzing a corpus of 1000 texts and extracting around 80 topics using Latent Dirichlet Allocation. As a result, a book was published: https://www.researchgate.net/publication/329572272_Analisis_del_Discurso_Procesamiento_de_lenguaje_natural_con_Tecnologias_Libres

SKILLS & OTHER

Skills: Python, Rust, Solidity, Unix/Linux. https://github.com/tanogedler
Language: Spanish (native), and fluent in English and Russian

Other publications:

- Cognitive Cryptography using behavioral features from linguistic-biometric data: https://eprint.iacr.org/2023/46
- Private Neural Network using Zero-Knowledge Proofs during Inference: https://medium.com/@tanogedler/private-neural-network-using-zero-knowledge-proofs-during-inference-1601e444be77