Robin Salen

Dedicated cryptographer always *thriving for new challenges* that will help his company and the entire ecosystem grow.

Supportive team leader conscientious of every individual needs to design a *friendly and performing* work environment.

EXTERNAL LINKS

Linkedin: https://www.linkedin.com/in/robin-salen/
Github: https://github.com/Nashtare
Twitter: https://twitter.com/RobinSalen
Website: https://nashtare.github.io/

EXPERIENCE

Toposware, Inc., Cambridge, USA

LEAD CRYPTOGRAPHER

April 2022 - PRESENT

Research & Development of cryptographic protocols, focusing on zero-knowledge proofs.

- Development of core cryptographic libraries.
- Academic research on both cryptographic primitives and protocols.
- Management of junior team members.
- In charge of hiring for the cryptographer's team, and conducting technical interviews.

Toposware, Tokyo, JAPAN

CRYPTOGRAPHER

November 2019 - April 2022

Research & Development of cryptographic protocols, focusing on zero-knowledge proofs.

- Development of core cryptographic libraries.
- Academic research on both cryptographic primitives and protocols.

CONTACT

Cambridge, MA 02139

salenrobin [at] gmail [dot] com

SKILLS

Cryptography

Mathematics

Rust

C++

Python

Team management

LANGUAGES

French: native

English: full proficiency

Japanese: basic conversational

HOBBIES

Photography

Hiking

Piano

Tennis

EDUCATION

Université Rennes I, Rennes, France — *MSc.*

Mathematics and Cryptography, September 2020

Master in Mathematics, with a specialization in computer science and cryptography.

- Graduated with honors.
- M2 Thesis: *Implementation and development of encryption schemes*, September 2020
- M1 Thesis: *Lattice-Based Cryptography*, May 2018

Tokyo Institute of Technology, Tokyo, Japan — *Research Student*

Computer Science, August 2019

Research student at the Tokyo Institute of Technology (東京工業大学). Conducted a research project: "*Fully Homomorphic Encryption over an Artificial Neural Network*" under the supervision of Haruiko Kaneko.

Université Rennes I, Rennes, France — *BSc.*

Mathematics, June 2017

Graduated with honors.

ACADEMIC WORK

New Design Techniques for Efficient Arithmetization-Oriented Hash Functions: Anemoi Permutation and Jive Compression Mode

C Bouvier, P Briaud, P Chaidos, L Perrin, **R Salen**, V Velichkov, D Willems
CRYPTO'23, 2023

Two additional instantiations from the Tip5 hash function construction

R Salen
Toposware whitepapers, 2023

Identifiable Cheating Entity Flexible Round-Optimized Schnorr Threshold (ICE-FROST) signature protocol

A González, H Ratoanina, **R Salen**, S Sharifian, V Soukharev
Cryptology ePrint Archive, 2021

Security Analysis of Elliptic Curves over Sextic Extension of Small Prime Fields

R Salen, V Singh, V Soukharev
Cryptology ePrint Archive, 2021