

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>

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, Inc., Tokyo, Japan

CRYPTOGRAPHER

November 2019 - April 2022

Research & Development of cryptographic protocols, focusing on zero-knowledge proofs. Part-time until March 2020.

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

Crédit Mutuel Arkéa, Rennes, France

DATACENTER SUPERVISOR

June 2017 - August 2017

- Supervised a nationwide park of ATMs.
- Remotely assisted maintenance of those ATMs and organized technicians intervention scheduling.

CONTACT

Cambridge, MA 02139

+1 (617)-251-2021

salenrobin@gmail.com

SKILLS

Cryptography

Mathematics

Rust

C++

Python

Product development

Team management

LANGUAGES

French: native

English: full proficiency

Japanese: basic
conversational

HOBBIES

Photography

Hiking

Piano

Tennis

EDUCATION

Université Rennes I, Rennes, France — *M.D.*

Mathematics and Cryptography, September 2020

Master's courses 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

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

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

Université Rennes I, Rennes, France — *B.S.*

Mathematics, June 2017

Graduated with honors.

ACADEMIC WORK

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

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
Under submission

Two additional instantiations from the Tip5 hash function construction

R Salen
Toposware whitepapers