

NAJMEH SOROUSH

I am computer scientist, specialist in cryptography and information security.
Skilled in mathematics, secure electronic voting protocols and verifiable, secure and privacy preserving computation.

@ njm.soroush@gmail.com

📍 Luxembourg

🌐 njm-soroush



EXPERIENCE

Postdoctoral Researcher

Interdisciplinary Centre for Security, Reliability and Trust (SnT)

📅 January 2022 - Ongoing

📍 Luxembourg

Doctoral Researcher

Interdisciplinary Centre for Security, Reliability and Trust (SnT)

📅 2017-2022

📍 University of Luxembourg

E-Learning Manager and Digital Content designer

Mandegar Learning Development Company

📅 2007-2013

📍 Tehran, Iran

Mathematics lecturer

Elm-O-Farhang University, Tehran Virtual University, Sharif University

📅 2002-2007

📍 Tehran, Iran

EDUCATION

Ph.D. in Computer Science

Université Du Luxembourg

📅 August 2017 – January 2022

📍 Luxembourg

- Field: Information Security, Cryptography
- Thesis: Verifiable, Secure and Privacy-Preserving Computation

M.Sc. in Computer Science

Université Du Luxembourg

📅 Sept 2015 – July 2017

📍 Luxembourg

- Field: Information Security
- Remark: Due to having a M.Sc in mathematics in mathematics, the master thesis was not submitted and the doctoral research started.

M.Sc. in Pure Mathematics

Sharif University of Technology

📅 Sept 2001 – June 2002

📍 Tehran, Iran

- Field: Geometry and Combinatorics
- Thesis Title: Manifolds of Non-Positive Curvature

HARD SKILLS

Cryptography

Information Security

Zero-Knowledge Proof Systems

Secure Electronic Voting Protocols

Mathematics

Programming

Data Analysis

TECHNICAL SKILLS

Python, C/C++ , Rust

CyberSecurity, Ethical Hacking

NumPy, Pandas, TensorFlow

Github

SOFT SKILLS

Creative Thinking

Active Learning

Communication

Hard-working

Adaptability

Collaboration

LANGUAGES

Persian



English



French



Luxembourgish



B.Sc. in Pure Mathematics

Sharif University of Technology

📅 1997 – 2001

📍 Tehran, Iran

PUBLICATIONS

👥 Conference Proceedings

- Estaji, E., Haines, T., Gjøsteen, K., Rønne, P. B., Ryan, P. Y. A., & Soroush, N. (n.d.). Revisiting practical and usable coercion-resistant remote e-voting. In *Electronic voting - 5th international joint conference, e-vote-id 2020, bregenz, austria*, Springer.
- Ryan, P. Y. A., Roenne, P. B., Ostrev, D., Orche, F. E., Soroush, N., & Stark, P. B. (n.d.). Who was that masked voter? the tally won't tell! In *Electronic voting - 6th international joint conference, e-vote-id, virtual event, october, 2021*, Springer.
- Soroush, N., Iovino, V., Rial, A., Rønne, P. B., & Ryan, P. Y. A. (n.d.). Verifiable inner product encryption scheme. In *Public-key cryptography - PKC 2020 - 23rd IACR international conference on practice and theory of public-key cryptography, uk, may, 2020*, Springer.

HONORS AND AWARDS

- Winning the scholarship for academic achievements at master studies (Luxembourg).
- Winning two honorary diplomas in the national Computer Olympiads (Iran).
- Third place in the national programming competition (Iran).
- Winning the honorary diploma in the national Mathematics Olympiads (Iran).

INTERESTS

Psychology and Philosophy

Gardening and Cooking

Badminton and Volleyball