

# Kasra EdalatNejad

 [kasra.edalat.dev](https://kasra.edalat.dev)  
 [kasra.edalat@epfl.ch](mailto:kasra.edalat@epfl.ch)  
 [keybase.io/kasraedalat](https://keybase.io/kasraedalat)  
 [github.com/kasra-edalat](https://github.com/kasra-edalat)  
 [kasra-edalatnejad](https://kasra-edalatnejad)

## EDUCATION

---

**École polytechnique fédérale de Lausanne** Lausanne, Switzerland  
Ph.D. in Computer Science, Advisor: Prof. Carmela Troncoso 2017–Current  
– Thesis title: *“Bridging the gap between theoretical and practical privacy technologies for at-risk populations”*

**Sharif University of Technology** Tehran, Iran  
B.S. in Computer Engineering - Software Engineering 2011–2016

**Salam Tajrish high school** Tehran, Iran  
Diploma in mathematics and physics 2008–2011

## EXPERIENCE

---

**IMDEA Software Research Institute** Madrid, Spain  
Research intern, Advisor: Prof. Dario Fiore, Dr. Claudio Soriente July 2021–Nov 2021  
– Topic: *“Speeding up privacy-preserving deep learning by enhancing FHE operations with both TEE and GPU”*

**University of Michigan** Ann Arbor, Michigan  
Research assistant, Advisor: Prof. Harsha V. Madhyastha 2016–2017  
– Topic: *“Privacy-preserving recommendation sharing”*

**Atomic Energy high school** Tehran, Iran  
Teacher: Combinatory and programming 2011–2015

**Salam Tajrish high school** Tehran, Iran  
Teacher: Algorithm, combinatory, and programming 2011–2012

## PUBLICATIONS

---

1. **Kasra EdalatNejad**, Theresa Stadler, Martin Strohmeier, Vincent Lenders, Wouter Lueks, Carmela Troncoso: *“Brutus: a decision support system to prevent the use of insecure communication in aircraft”*. Under submission.
2. **Kasra EdalatNejad**, Mathilde Raynal, Wouter Lueks, Carmela Troncoso: *“Private Collection Matching Protocols”*. Proceedings on Privacy Enhancing Technologies, 2023.
3. **Kasra EdalatNejad**, Wouter Lueks, Julien Pierre Martin, Soline Ledésert, Anne L’Hôte, Bruno Thomas, Laurent Girod, Carmela Troncoso: *“DatashareNetwork: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists”*. USENIX Security Symposium 2020.
4. Manu Drijvers, **Kasra EdalatNejad**, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, Igors Stepanovs: *“On the Security of Two-Round Multi-Signatures”*. in IEEE Symposium on Security and Privacy (IEEE S&P) 2019.
5. Manu Drijvers, **Kasra EdalatNejad**, Bryan Ford, Gregory Neven: *“Okamoto Beats Schnorr: On the Provable Security of Multi-Signatures”*. IACR Cryptol. ePrint Arch. 2018: 417 (2018)
6. Han Zhang, **Kasra EdalatNejad**, Amir Rahmati, Harsha V. Madhyastha: *“Towards Comprehensive Repositories of Opinions”*. HotNets 2016.

## Contributed talks

1. **Kasra EdalatNejad**: “*DatashareNetwork: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists*”. Real world crypto (RWC), 2023.
2. **Kasra EdalatNejad**: “*Automatic detection and decryption of insecure ciphertxts in ACARS*”. Cyber Alp Retreat, 2021.
3. **Kasra EdalatNejad**, Soline Ledéser: “*DatashareNetwork: The use of Tor in supporting document search for Investigative Journalists*”. Tor Demo Day, September 2020.











## HONORS AND AWARDS

---

- Runner up for CNIL-Inria data protection award 2022
- Runner up for the Caspar Bowden award for outstanding research in privacy enhancing technologies 2021
- EPFL IC distinguished service award 2020
- EPFL teaching assistance award 2019
- EPFL EDIC fellowship for doctoral studies 2017
- **Ministerial award** from ministry of science, research, and technology for outstanding performance in olympiad 2017
- **Gold medal** (Ranked 1st) in the national computer science olympiad for graduate students 2016
- Ranked 6th in the Iranian national graduate examination (Konkur) 2016
- Ranked 23rd (top 1%) in the 9th IEEEExtreme Oct 2015
- **Presidential award** from **Pres. M. Ahmadinejad** for outstanding performance in olympiad 2011
- **International Silver medal** in 23th international olympiad in informatics (IOI), Pattaya, Thailand July 2011
- **Silver medal** in 5th Asia-Pacific informatics olympiad (APIO) May 2011
- **Ministerial award** from ministry of science, research, and technology for outstanding performance in olympiad 2010
- National **Gold medal** (ranked 1st) in Iranian national olympiad in informatics (INOI) Sep 2010
- National **Silver medal** in Iranian national olympiad in informatics (INOI) March 2010
- Member of Iranian national elite foundation since 2011

## PROJECTS

---

- **PCM**: A framework for private collection matching  Repo
- **DatashareNetwork**: A decentralized privacy-preserving search engine
  - Proof of concept for cryptographic primitives  crypto
  - Production code  core,  server,  client
  - For more information visit  kasra.edalat.dev
- **SSCred**: Single show anonymous credentials
  - Source code  Repo
  - Pypi package  sscred
- **KSSH**: An SSH server as a plugin for Sharif HoneyPot  Repo
- **KilliCent**: A micropayment system based on MilliCent  Repo

## SKILLS

---

### Programming languages

- Proficient in: C++, Python, Go, Java, Android, JavaScript
- Familiar with: C, Lisp, Verilog, Haskell, Racket

## TEACHING AND SUPERVISION

---

### Student Supervision

- Pierugo Pace, Master project: “Biometric deduplication in humanitarian aid distribution”. 2023
- Eva Luvison, Master project: “Wallets for Privacy-Preserving Aid Distribution”. 2022
- Lorenzo Carlo Rovati, Master project: “Using smartcards for privacy-friendly aid distribution”. 2022
- Jodok Vieli, Master project: “Automatic decryption of classical ciphers with neural networks”. 2021
- Ma Ke, Master project: “Securing biometric authentication data with trusted hardware”. 2021
- Sacha Kozma, Master project: “Efficiently updatable accumulator”. 2020
- Omid Karimi, Bachelor project: “Automatic cryptanalysis of classical ciphers”. 2020
- Mathilde Raynal, Master project: “Secure Multiparty Computation for PSI”. 2019
- Bradley Mathez, Bachelor project: “An SMC Approach to Multi-Device Key Management”. 2019
- Valentyna Pavliv, Bachelor project: “Efficient Blacklisting of Anonymous Users”. 2019

### Teaching assistant

- CS-523: Advanced topics on privacy enhancing technologies 2020, 2021
- COM-301: Computer security 2018, 2019, 2020
- COM-412: Software security 2019
- MATH-232: Probability and statistics 2018

## ACADEMIC SERVICE

---

### Program committee

- IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2020
- IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2019

### External reviewer

- PoPETS 2023
- PoPETS 2022
- EuroCrypt, USENIX Security, OSDI, IEEE Trans. on Information Forensics and Security 2021
- NSDI 2020
- PoPETS, FC 2019