

Research Interests

Security and privacy

Privacy-enhancing technologies

Applied cryptography

Education

École polytechnique fédérale de Lausanne, Switzerland	2017-Present
Ph.D. candidate in Computer Science, Security and Privacy Engineering lab Thesis Advisor: Prof. Carmela Troncoso	
Sharif University of Technology, Tehran, Iran	2011-2016
B.S. in Computer Engineering - Software Engineering Grade Point Average: 18.29 out of 20 GPA(3.8)	
Diploma in Mathematics and Physics Discipline	2008-2011
Salam Tajrish high school, Tehran, Iran	

Work Experience

University of Michigan, Ann Arbor, Michigan	May 2016 – Aug 2017
Research assistant: Privacy-preserving recommendation sharing Advisor: Prof. Harsha V. Madhyastha	
Atomic Energy high school, Tehran, Iran	2011– 2015
Teacher: Combinatory and programming	
Salam Tajrish high school, Tehran, Iran	2010-2012
Teacher: Algorithm, Combinatory and programming	

Honors & Awards

EDIC's Ph.D. fellowship award	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, Tehran, Iran	2016
Ranked 6th in the National Graduate Examination (Konkur), Tehran, Iran	2016
Ranked 23rd among more than 2400 teams in the 9 th IEEEExtreme, Tehran, Iran	Oct 2015
Presidential Award from president 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	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), Tehran, Iran	Sep 2010
National Silver medal in Iranian National Olympiad in informatics (INOI), Tehran, Iran	March 2010
Member of Iranian National Elite Foundation	Since 2010

Kasra EdalatNejad

Research Interests

Security and privacy

Privacy-enhancing technologies

Applied cryptography

Academic services

Technical program committee in IEEE ICBC

2019-2020

Papers

K. EdalatNejad, W. Lueks, J. Martin, S. Ledésert, A. Lhôte, B. Thomas, L. Girod and C. Troncoso, "**DatashareNetwork: A Decentralized Privacy-Preserving Search Engine for Investigative Journalists**", in USENIX Security 2020

M. Drijvers, K. EdalatNejad, B. Ford, E. Kiltz, J. Loss, G. Neven and I. Stepanovs, "**On the Security of Two-Round Multi-Signatures**", in IEEE Symposium on Security and Privacy (S&P 2019) 2019

M. Drijvers, K. EdalatNejad, B. Ford, and G. Neven, "**Okamoto Beats Schnorr: On the Provable Security of Multi-Signatures**", in IACR Cryptology ePrint archive 2018

H. Zhang, K. EdalatNejad, A. Rahmati and H. V. Madhyastha, "**Towards Comprehensive Repositories of Opinions**", In 15th ACM Workshop on Hot Topics in Networks (HotNets'16) [[pdf](#)] 2016

Projects

DatashareNetwork - a peer-to-peer privacy-preserving document search engine for investigative journalists ([Link](#))

SSCred - a python library to facilitate anonymous credentials ([Git](#))

KSSH - Developing an SSH server as a plugin for Sharif HoneyPot ([Git](#))

ViraConvertor - an scalable online Office to PDF convertor

KilliCent - a micropayment system based on MilliCent ([Git](#))

DaneshGostar - a Persian Web-Based Knowledge Management System ([Git](#))

Kalendar - a calendar (Gregorian and Jalali) with internal ToDo and Event management for android

KToDo - a work management app for Android

MSAutomata - a GUI to draw nondeterministic finite automaton (NFA) and convert them to Regex and vice versa ([Jar](#))

Skills & Information

Programming languages

Proficient in: C, C++, Java, Python, Django framework, Go, Android, HTML, CSS, JavaScript

Familiar with: Lisp, Matlab, Verilog, OpenGL, Node.js, Haskell, Racket

Natural languages

Persian (native), English (fluent)

Email: kasra.edalat@epfl.ch
Website: kasra.edalat.dev