SeyedSaeed Sadeghian

Curriculum Vitae

Education

2011–2015 **Doctor of Philosophy**, *University of Calgary*, Calgary, *GPA – A*.
PhD in Computer Science.

2007–2010 **Master of Science**, *Amirkabir University of Technology*, Tehran, *GPA – 17.22/20*.
Masters in IT - Specialized in Information Security

2003–2007 **Bachelor of Science**, *Islamic Azad University Tehran South Branch*, Tehran, *GPA – 18.02/20*.
Bachelors in Computer Engineering

Research Interest

- Security and Privacy
- Computer and Network Security

Experience

Industry Experience

2014 **Research Intern**, Microsoft Research, Redmond, WA, USA.
Cutting edge research involving Differential privacy and machine learning.

2013–2014 **Software and Cryptography Engineer**, Microsoft, Calgary, AB, Canada.
Scalable Implementation of Private Set Intersection Protocol.

Teaching Experience

2011–2013 **Teaching Assistant**, *University of Calgary*, Calgary.
- CPSC 526, Winter 2013
- CPSC 418/PMAT 418, Fall 2012
- CPSC 329, Winter 2012
- CPSC 418/PMAT 418, Fall 2011

Recent Publications

2015 Helger Lipmaa, Payman Mohassel, Saeed Sadeghian, "More Efficient Private Function Evaluation: Universal Circuits and Beyond", *manuscript*.

2014 Payman Mohassel, Saeed Sadeghian, "Private Set Intersection via Cuckoo Hashing", *manuscript*.

2014 Payman Mohassel, Saeed Sadeghian, Nigel P. Smart, "Actively Secure Private Function Evaluation", In Advances in Cryptology, **Asiacrypt 2014**.

602 ICT Building, 2500 University Dr. NW – Calgary, Alberta T2N 1N4
✉ *sadeghian@gmail.com* • *pages.cpsc.ucalgary.ca/∼sadeghis*

2014 Seny Kamara, Payman Mohassel, Mariana Raykova, Saeed Sadeghian, "Scaling Private Set Intersection to Billion-Element Sets", Financial Cryptography and Data Security 2014, **FC'14**.

2013 Payman Mohassel, Saeed Sadeghian, "How to Hide Circuits in MPC: An Efficient Framework for Private Function Evaluation", In Advances in Cryptology, **Eurocrypt 2013**.

2012 Payman Mohassel, Saeed Sadeghian, Salman Niksefat, "ZIDS - A Privacy-Preserving Intrusion Detection System using Secure Two-Party Computation Protocols", **The Computer Journal**, doi: 10.1093/comjnl/bxt019.

2012 Payman Mohassel, Salman Niksefat, Saeed Sadeghian, Babak Sadeghiyan, "An Efficient Protocol for Oblivious DFA Evaluation and Applications", RSA Conference, **CT-RSA 2012**.

Honours and Awards

2014 Eyes High International Doctoral Scholarship, Department of Computer Science, University of Calgary, Calgary, Canada.

2013 Eyes High International Doctoral Scholarship, Department of Computer Science, University of Calgary, Calgary, Canada.

2013 Second Place Team, Microsoft Coding Competition, University of Calgary, Sep. 25th 2013.

2013 Computer Science Alumni Chapter Graduate Scholarship, Department of Computer Science, University of Calgary, Calgary, Canada (September 2013)

2013 Department Research Award, Department of Computer Science, University of Calgary, Calgary, Canada (September 2013)

2012 Department Research Award, Department of Computer Science, University of Calgary, Calgary, Canada (September 2012)

2012 *3rd Best Poster*, "General-Purpose and Customized Solutions for Private Function Evaluation. Industry Day 2012, University of Calgary.

2011 *Best Poster Award*, "Privacy-Preserving DFA Evaluation Protocol with application to DNA matching". ISPIA research planning day, University of Calgary. 19 Nov, 2011.

2011 Department Research Award, Department of Computer Science, University of Calgary, Calgary, Canada (September 2011)

2005-2007 Ranked as the Top BSc Student in Computer Engineering, Islamic Azad University South Tehran Branch, Tehran, Iran

2007 Ranked 18th in Iranian National University Entrance Exam for Information Technology Graduate Studies

2007 Ranked 40th in Iranian National University Entrance Exam for Computer Engineering: Artificial Intelligence Graduate Studies

Communication Skills

2015 "Valiant's Universal Circuit Construction", Talk at Theory group seminars, Department of Computer Science, University of Calgary, Jan, 2015.

2014 Presented "Actively Secure Private Function Evaluation", Asiacrypt Conferene, Kaohsiung, Taiwan, 2014.

2013 Presented "How to Hide Circuits in MPC: An Efficient Framework for Private Function Evaluation", Eurocrypt Conferene, Athens, Greece, 2013.

2012 Presented "General-Purpose and Customized Solutions for Private Function Evaluation. Industry Day 2012. *3rd Best Poster*

2012 Presented "An Efficient Protocol for Oblivious DFA Evaluation and Applications", RSA Conference, San Francisco, USA, 2012.

2012 "Optimal Constructions for Private Function Evaluation", Talk at Theory group seminars, Department of Computer Science, University of Calgary, March 30, 2012.

2011 Presented "Privacy-Preserving DFA Evaluation Protocol with application to DNA matching". ISPIA research planning day, University of Calgary. 19 Nov, 2011. *Best Poster*