Zahra Jafargholi

Contract Information	Office 266 West Village H Northeastern University 440 Huntington Avenue Boston, MA. 20115	Phone: (617) 756-5633 E-mail: zahra@ccs.neu.edu Web: ccs.neu.edu/home/zahra

Research Interests

I am interested in cryptography and more broadly theoretical computer science. I am especially interested in:

- Analyzing security of cryptographic primitives against adaptive attacks.
- Cryptography with weak sources of randomness.
- Authentication and Privacy amplification schemes.
- Resilience to side-channel leakage and tampering attacks.

Education

Northeastern University, Boston, MA. *Sept 2011 - present*
PhD Candidate, College of Computer and Science
Research Advisor: Daniel Wichs

Shahid Beheshti University, Tehran, Iran *Sept 2003 - June 2008*
B.S. in Computer Science. June, 2009.

Research Experiences

Northeastern University, Boston, MA. *Sept 2015 - present*
Research Assistant

Working on proving the adaptive security of Yao's garbled circuits with non-trivial parameters.

Simons Institute, Berkeley, CA. *May 2015 - Aug 2015*
Research Assistant

Research on adaptive security of Garbled circuits. Developed a new primitive, Somewhere Equivocal Encryption. Developed a new garbling scheme using Yao's gabling scheme and Somewhere equivocal encryption scheme. Proved the new garbling scheme is adaptively secure, with online complexity proportional to the space complexity of the circuit.

Northeastern University, Boston, MA. *Sept 2013 - Dec 2014*
Research Assistant

Research on Continuous non-malleable codes. Devised a method to add the tamper-resilience feature to cryptographic primitives that are secure in tamperfree settings. Constructed codes that can tolerate continuous attacks without re-encoding after every execution, making these codes more efficient and keeping the system state-free.

Institute of Science and Technology Austria, Klosterneuburg, Austria *June 2014 - Aug 2014*
Research Assistant

Research on applying nested hybrid arguments to Generalized Selective Decryption (GSD) Game. GSD problem is used as a theoretical abstraction of security requirements of multicast encryption protocols. Improved the security analysis of these protocols from an exponential security loss in the reduction to only a quasi-polynomial security loss in the reduction.

Northeastern University, Boston, MA. *June 2013 - Sept 2013*
Research Assistant

Research on privacy amplification protocols. Improved parameters of many different privacy amplification protocols, including message authentication protocols and key agreement protocols. In Bounded Retrieval Model, where the shared secret source between parties is too big to be transferred or to be read in entirety by any adversary, the amount of wasted entropy during the communication of the protocols was reduced to minimum, enabling the parties to use the same shared sources to arrive at many more secret keys.

Northeastern University, Boston, MA. *June 2012 - Sept 2012*
Research Assistant

Research on complexity of problems with known quadratic time upper-bounds.

Publications

[1] Brett Hemenway, Zahra Jafargholi, Rafail Ostrovsky, Alessandra Scafuro and Daniel Wichs
Adaptively Secure Garbled Circuits from One-Way Functions
Under submission at *CRYPTO 2016 - Advances in Cryptology*

[2] Zahra Jafargholi and Emanuele Viola
3SUM, 3XOR, Triangles
***Algorithmica**, January 2016 - an International Journal in Computer Science*

[3] Georg Fuchsbauer, Zahra Jafargholi and Krzysztof Pietrzak
A Quasipolynomial Reduction for Generalized Selective Decryption on Trees
***CRYPTO 2015** - Advances in Cryptology*

[4] Zahra Jafargholi and Daniel Wichs
Tamper Detection and Continuous Non-malleable Codes
***TCC 2015** - Theory of Cryptography Conference*

[5] Divesh Aggarwal, Yevgeniy Dodis, Zahra Jafargholi, Eric Miles and Leonid Reyzin
Amplifying Privacy in Privacy Amplification
***CRYPTO 2014** - Advances in Cryptology*

Presentations & Invited Talks

Adaptive Security of Garbled Circuits Revisited
Charles River Crypto Day at MIT. Cambridge, MA. Oct 23, 2015.

A Quasipolynomial Reduction for Generalized Selective Decryption on Trees
CRYPTO Conference. Santa Barbara, CA. Aug 22, 2015.

Tamper Detection and Continuous Non-malleable Codes
Theory of Cryptography Conference, TCC 2015. Warsaw, Poland. March 24, 2015.
MIT Cryptography Reading Group. Cambridge, MA. March 10, 2015.
Security Seminar at Boston University. Boston, MA. Feb 11, 2015.

TEACHING	**Northeastern University, Boston, MA.** Teaching Assistant, College of Computer and Science.	
	Theory of Computation, Undergraduate course	*Spring 2015*
	Advanced Algorithm, Masters course	*Spring 2013*
	Advanced Algorithm, Masters course	*Fall 2012*
	Advanced Algorithm, Masters course	*Spring 2012*
	Advanced Algorithm, Masters course	*Fall 2011*