Fattaneh Bayatbabolghani

Personal Information

Phone:	+1 (574) 387 0379
email:	fbayatba@berkeley.edu, fattaneh.bayat@gmail.com
URL:	http://ischool.berkeley.edu/~fbayatba

Research Interests

Information Security, Privacy, and Applications of Cryptography (Privacy-Preserving Computation, Privacy-Preserving Protocols in Cloud Computing, Secure Biometric and Genomic Computations, Privacy-Preserving Machine Learning Algorithms, Private Information Retrieval, Security and Privacy for Internet of Things Ecosystems)
Applications of Spectral Method in Scientific Computations (Collocation Method for Engineering Problems Defined in Unbounded Domains)

Education

August 2017	Doctor of Philosophy in Computer Science and Engineering **University of Notre Dame**, Notre Dame, IN
July 2016	Master of Science in Computer Science and Engineering **University of Notre Dame**, Notre Dame, IN
August 2012	Master of Science in Computer Science **Shahid Beheshti University**, Tehran, Iran
June 2010	Bachelor of Science in Computer Science **Shahid Beheshti University**, Tehran, Iran

Skills

Computer Security	Cryptography, Cryptanalysis, Secure Two-Party Computation, Secure Multi-Party Computation, Homomorphic Encryption, Secret Sharing, Garbled Circuit Evaluation, Private Information Retrieval
Programming Languages	C/C++, Java, Python, MAPLE, MATLAB
Network Programming	Socket Programming in C/C++
Database Configuration	MySQL, Microsoft SQL Server

Work Experience

present August 2018	Postdoctoral Scholar in School of Information University of California–Berkeley, Berkeley, CA
present August 2018	Lecturer in School of Information University of California–Berkeley, Berkeley, CA
present August 2018	Computable Labs, San Francisco, CA Research Fellow

AUGUST 2018	Postdoctoral Fellow in School of Informatics, Computing, and Engineering
NOVEMBER 2017	Indiana University–Bloomington, Bloomington, IN
MAY 2018	Lecturer in School of Informatics, Computing, and Engineering
JANUARY 2018	Indiana University–Bloomington, Bloomington, IN
AUGUST 2017	GRA in Department of Computer Science and Engineering
AUGUST 2013	University of Notre Dame, Notre Dame, IN
JUNE 2013	Technical and Vocational High Schools, Tehran, Iran
JANUARY 2011	Co-authoring series of ten books in ICDL skills
JUNE 2013	GRA in Department of Computer Science
SEPTEMBER 2010	*Shahid Beheshti University, Tehran, Iran*

SELECTED TEACHING EXPERIENCE

FALL 2018	**Teaching** of "Cryptography for Cyber and Network Security" for graduate **online** students School of Information, University of California–Berkeley
SPRING 2018	**Guest Lecturer** for "Introduction to the Mathematics of Cybersecurity Course" for undergraduate students School of Informatics, Computing, and Engineering, Indiana University–Bloomington
SPRING 2018	**Teaching** of "Systems & Protocol Security & Information Assurance" for graduate students School of Informatics, Computing, and Engineering, Indiana University–Bloomington
SPRING 2018	**Teaching** of "Systems & Protocol Security & Information Assurance" for graduate **online** students School of Informatics, Computing, and Engineering, Indiana University–Bloomington

SELECTED PUBLICATIONS

1. Fattaneh Bayatbolghani, Marina Blanton. Secure Multi-Party Computation, to *CCS'18*, Toronto, Ontario, Canada, October 2018 (It is a tutorial proposal)

2. Fattaneh Bayatbabolghani, Marina Blanton, Mehrdad Aliasgari, Michael Goodrich (**Submitted**). Secure Fingerprint Alignment and Matching Protocols, to *TDSC*, 2017

3. Marina Blanton, Fattaneh Bayatbabolghani. An Approach to Improving Security and Efficiency of Private Genomic Computation using Server Aid, to *IEEE S&P Magazine*, 2017

4. Yihua Zhang, Marina Blanton, Fattaneh Bayatbabolghani. Enforcing Input Correctness via Certification in Garbled Circuit Evaluation, to *ESORICS'17*, Oslo, Norway, September 2017

5. Mehrdad Aliasgari, Marina Blanton, Fattaneh Bayatbabloghani. Secure Computation on Hidden Markov Models and Secure Flouting Point Arithmetic in the Malicious Model, to *IJIS*, 2017

6. Ali Shahbazi, Fattaneh Bayatbabolghani, Marina Blanton. Private Computation with

Genomic Data for Genome-Wide Association and Linkage Studies, to *GenoPri'16*, Chicago, November 2016

7. Marina Blanton, Fattaneh Bayatbabolghani. Efficient Server-Aided Secure Two-Party Function Evaluation with Applications to Genomic Computation, to *PETS*, 2016

Selected Programming Projects & Experiences

Implementation and evaluation of fingerprint spoof detection models, Fall 2015
Evaluation of unarchive Libor Masek's open source iris matching on an unarchive data set iris images from University of Notre Dame, Fall 2015
Implementation and evaluation of face detection and recognition in the popular OpenCV library framework, Fall 2015
Implementation of GPU acceleration of Hidden Markov Models, Spring 2014
Design and implementation of building concurrency into existing biometric algorithmic processes for voice patterns, Fall 2013
Implementation and presentation of search on encrypted data, Fall 2013

Awards and Honors

August 2012	Best thesis research and presentation (19.75/20) among all 2010 M.Sc. students of Computer Science program, Shahid Beheshti University, Tehran, Iran
June 2010	2nd rank in terms of total GPA (16.84/20) among all B.Sc. students of Computer Science program of Shahid Beheshti University
April 2008	Elected as the chair of CS Student Advisory Board, Shahid Beheshti University, Tehran, Iran
July 2006	Admitted to Shahid Beheshti University's Computer Science Undergraduate Program, one of the high ranked universities in Iran
April 1999	3rd rank in the "Olympiad in Mathematics" among regional middle schools, Tehran, Iran

Refereeing for Journals

IEEE Transactions on Information Forensics and Security
Information Sciences Journal
Applied Mathematics and Computation
An Interactive Workshop on the Human aspects of Smarthome Security and Privacy
Soft Computing Journal

Refereeing for Conferences

The Network and Distributed System Security Symposium (NDSS'18)

Travel Grants

May 2018	Mathematics of Modern Cryptography (Institute for Advanced Study at Princeton)
May 2017	GREPSEC III Workshop
May 2015	IEEE Symposium on Security and Privacy (IEEE S&P'15)
May 2015	GREPSEC II Workshop
April 2014	CRA-Women Grad Cohort Workshop

Talks

October 2018	ACM Conference on Computer and Communications Security (CCS'18) (tutorial), Toronto, Ontario, Canada
August 2018	Workshop on the Human aspects of Smarthome Security and Privacy at Fourteenth Symposium on Usable Privacy and Security (SOUPS'18), Co-located with USENIX Security'18, Baltimore, MD
May 2018	Bosch Research and Technology Center, Pittsburgh, PA
May 2018	Mathematics of Modern Cryptography (WAM), at Institute for Advanced Study at Princeton University, Princeton, NJ
April 2018	The Midwest Security Workshop (MSW) (light-talk), at University of Illinois Urbana-Champaign, Champaign, IL
September 2017	Boston University, Boston, MA
September 2017	University of Connecticut, Storrs, CT
August 2017	Cornell University, Ithaca, NY
July 2017	The Ohio State University, Columbus, OH
July 2017	Purdue University, West Lafayette, IN.
May 2017	IEEE Symposium on Security and Privacy (IEEE S&P'17), San Jose, CA
May 2017	University of Notre Dame, Notre Dame, IN
November 2016	International Workshop on Genome Privacy and Security, Chicago, IL
August 2015	Student Knowledge Exchange on Technical Aspects of Privacy, University of Notre Dame, Notre Dame, IN

Graduate Coursework

Cryptography, Computer Security, Bioinformatics Computing, Biometrics (Ph.D. Major)
Operating Systems, Complexity & Algorithms, Advanced Computer Architecture (Ph.D. Core)
Case Study–Computer Based Entrepreneurship (Ph.D. Miscellaneous)
Matrix Computations, Advanced Mathematical Software, Special Subjects in Numerical Analysis, Subjects in Scientific Computing (M.Sc. Major)

Services

August 2018	Organized An Interactive Workshop on the Human aspects of Smarthome Security and Privacy at Fourteenth Symposium on Usable Privacy and Security (SOUPS'18), Co-located with USENIX Security'18, Baltimore, MD
May 2018- July 2018	Mentoring Visiting Undergraduate Students at School of Informatics, Computing, and Engineering at Indiana University, Bloomington, IN
May 2018	Organizing WAM Research Seminar Series at Institute for Advanced Study at Princeton University, Princeton, NJ
April 2018	Leading Privacy-Enhancing Technologies Discussion Session in MSW at University of Illinois Urbana-Champaign, Champaign, IL
April 2018	Served as a Judge for the Annual CEWiT Women's Research Competition at School of Informatics, Computing, and Engineering at Indiana University, Bloomington, IN
November 2017	Served as a Judge for Fall Projects and Research Symposium at School of Informatics, Computing, and Engineering at Indiana University, Bloomington, IN
April 2008- June 2010	Chair of Computer Science Student Advisory Board at Shahid Beheshti University, Tehran, Iran