# 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
Thesis: "Secure Biometric Computation and Outsourcing"
Advisor: Prof. Marina Blanton | Co-Advisor: Prof. Aaron Striegel
GPA: 3.71/4.00

July 2016 — Master of Science in Computer Science and Engineering
**University of Notre Dame**, Notre Dame, IN
Proposal: "Secure Computation on Biometric Data"
Advisor: Prof. Marina Blanton
GPA: 3.71/4.00

August 2012 — Master of Science in Computer Science
**Shahid Beheshti University**, Tehran, Iran
Thesis: "A Comparison Between Laguerre, Hermite, and Sinc Orthogonal Functions"
Advisor: Prof. Kourosh Parand
GPA: 17.44/20.00 (3.75/4.00)

June 2010 — Bachelor of Science in Computer Science
**Shahid Beheshti University**, Tehran, Iran
GPA: 16.84/20.00 (3.57/4.00)

## 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<br>August 2018 | School of Information<br>University of California–Berkeley, Berkeley, CA<br>Postdoctoral scholar |
| present<br>August 2018 | School of Information<br>University of California–Berkeley, Berkeley, CA<br>Lecturer |
| present<br>August 2018 | Computable Labs, San Francisco, CA<br>Research fellow |
| August 2018<br>November 2017 | School of Informatics, Computing, and Engineering<br>Indiana University–Bloomington, Bloomington, IN<br>Postdoctoral fellow under advice of Prof. Ryan Henry |
| May 2018<br>January 2018 | School of Informatics, Computing, and Engineering<br>Indiana University–Bloomington, Bloomington, IN<br>Lecturer |
| August 2017<br>August 2013 | Department of Computer Science and Engineering<br>University of Notre Dame, Notre Dame, IN<br>Graduate research assistant under advice of Prof. Marina Blanton |
| June 2013<br>January 2011 | Technical and Vocational High Schools, Tehran, Iran<br>Co-authoring series of ten books in ICDL skills |
| June 2013<br>September 2010 | Department of Computer Science<br>*Shahid Beheshti University, Tehran, Iran*<br>Graduate research assistant under advice of Prof. Kourosh Parand |

## Teaching Experience

| | |
|---|---|
| Fall 2018 | **Instructor** for "Cryptography for Cyber and Network Security" for graduate **online** students<br>School of Information, University of California–Berkeley |
| Spring 2018 | **Guest Lecturer** for "Introduction to the Mathematics of Cybersecurity Course" for undergraduate students<br>School of Informatics, Computing, and Engineering, Indiana University–Bloomington |

| | |
|---|---|
| Spring 2018 | **Instructor** of "Systems & Protocol Security & Information Assurance" for graduate students<br>School of Informatics, Computing, and Engineering, Indiana University–Bloomington |
| Spring 2018 | **Instructor** of "Systems & Protocol Security & Information Assurance" for graduate **online** students<br>School of Informatics, Computing, and Engineering, Indiana University–Bloomington |
| Spring 2011 | **Instructor** of 10 hours course of "MAPLE" for graduate students<br>Department of Computer Science, Shahid Beheshti University |
| Spring 2010 | **Undergraduate Teaching Assistant** for "Discrete Mathematics"<br>Department of Computer Science, Shahid Beheshti University |
| Fall 2009 | **Undergraduate Teaching Assistant** for "Data Structures & Algorithms"<br>Department of Computer Science, Shahid Beheshti University |

## 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<br>**Remark:** Because of this rank I was permitted to pursue my graduate studies as an "Exceptional Talents" without having to attend the "National Graduate Schools Entrance Exam" at Shahid Beheshti University, Tehran, Iran |
| 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 |

## 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 |

## Publications

**In Refereed Journals**

1. Fattaneh Bayatbabolghani, Marina Blanton, Mehrdad Aliasgari, Michael Goodrich (**Submitted**). Secure Fingerprint Alignment and Matching Protocols, to *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2017 (It is also available on *arXiv Report*

*1702.03379*, February 2017)

2. Marina Blanton, Fattaneh Bayatbabolghani. An Approach to Improving Security and Efficiency of Private Genomic Computation using Server Aid, to *IEEE Security and Privacy (IEEE S&P) Magazine* (IF: 1.382), 2017
3. Mehrdad Aliasgari, Marina Blanton, Fattaneh Bayatbabloghani. Secure Computation on Hidden Markov Models and Secure Flouting Point Arithmetic in the Malicious Model, to *International Journal in Information Security (IJIS)* (IF: 1.915), 2017
4. Marina Blanton, Fattaneh Bayatbabolghani. Efficient Server-Aided Secure Two-Party Function Evaluation with Applications to Genomic Computation, to *The annual Privacy Enhancing Technologies Symposium (PETS)*, 2016 (It is also available on *Cryptology ePrint Archive Report 2015/422*, May 2015)
5. Fattaneh Bayatbabolghani, Kourosh Parand. Using Hermite functions for solving Thomas–Fermi equation, to *International Journal of Mathematical, Computational Science and Engineering*, 2014
6. Kourosh Parand, Zahra Roozbahani, Fattaneh Bayatbabolghani. Solving Nonlinear Lane-Emden Type Equations with Unsupervised Combined Artificial Neural Networks, to *International Journal of Industrial Mathematics (IJIM)*, 2013
7. Kourosh Parand, Fattaneh Bayatbabolghani. Modified generalized Laguerre functions for a numerical investigation of flow and diffusion of chemically reactive species over a nonlinearly stretching sheet, to *World Applied Science*, 2012
8. Kourosh Parand, Fatemeh Baharifard, Fattaneh Bayatbabolghani. Comparison between rational Gegenbauer and modified generalized Laguerre functions collocation methods for solving the case of heat transfer equations arising in porous medium, to *International Journal of Industrial Mathematics (IJIM)*, 2012
9. Kourosh Parand, Fattaneh Bayatbabolghani. Applying the Modified Generalized Laguerre Functions for Solving Steady Flow of a Third Grade Fluid in a Porous Half Space, to *World Applied Science*, 2012

**In Refereed Conference Proceedings**

10. Fattaneh Bayatbolghani, Marina Blanton. Secure Multi-Party Computation, to *ACM Conference on Computer and Communications Security (CCS'18)*, Toronto, Ontario, Canada, October 2018 (It is a tutorial proposal)
11. Yihua Zhang, Marina Blanton, Fattaneh Bayatbabolghani. Enforcing Input Correctness via Certification in Garbled Circuit Evaluation, to *The European Symposium on Research in Computer Security (ESORICS'17)*, Oslo, Norway, September 2017 (Acceptance rate is 16%) (It is also available on *Cryptology ePrint Archive Report 2017/569*, June 2017)
12. Ali Shahbazi, Fattaneh Bayatbabolghani, Marina Blanton. Private Computation with Genomic Data for Genome-Wide Association and Linkage Studies, to *International Workshop on Genome Privacy and Security (GenoPri'16)*, Chicago, November 2016
13. Fattaneh Bayatbabolghani, Kourosh Parand. Comparison between Hermite and Sinc functions collocation methods for solving Steady Flow of a Third Grade Fluid in a Porous Half Space, to *International Conference on Scientific Computing (CSC'13)*, Nevada, July 2013

**In Books**

14. Faezeh Sadat Babamir, Fattaneh Bayatbabolghani. Linearly Time Efficiency in Unattended Wireless Sensor Networks, to *open access book project: Real-Time Systems, Archi-*

*tecture, Scheduling, and Applications, INTECH*, 2012

### Theses

15. Fattaneh Bayatbabolghani. Secure Biometric Computation and Outsourcing, *Ph.D.'s Thesis*, University of Notre Dame, June 2017
16. Fattaneh Bayatbabolghani. A Comparison Between Laguerre, Hermite, and Sinc Orthogonal Functions, *Master's Thesis*, Shahid Behehsti University, September 2012 (It is also available on *arXiv Report 1709.10352*, September 2017)

### Posters

17. Fattaneh Bayatbabolghani, Marina Blanton, Mehrdad Aliasgari, Michael Goodrich. Secure Computations of Trigonometric and Inverse Trigonometric Functions, to *IEEE Symposium on Security and Privacy (IEEE S&P'17)*, San Jose, May 2017
18. Fattaneh Bayatbabolghani. Efficient Ancestry, Paternity, and Genomic Compatibility testings in Server-Aided Secure Two-Party Function Evaluation, to *Grace Hopper*, Houston, October 2015
19. Fattaneh Bayatbabolghani, Marina Blanton. Secure Computation of Fingerprint Alignment and Matching, to *IEEE Symposium on Security and Privacy (IEEE S&P'15)*, San Jose, May 2015 and to *10th Annual Student Research Symposium*, Department of Computer Science and Engineering, University of Notre Dame, November 2015
20. Marina Blanton, Fattaneh Bayatbabolghani. Efficient Server-Aided Secure Two-Party Function Evaluation with Applications to Genomic Computation, to *9th Annual Student Research Symposium*, Department of Computer Science and Engineering, University of Notre Dame, November 2014 and to *Indiana Celebration Women in Computing (INWIC'15)*, Indianapolis, March 2015
21. Fattaneh Bayatbabolghani. Secure Computation on Hidden Markov Models, to *CRA-Women Graduate Cohort Workshop*, Santa Clara, April 2014

### Selected Books

22. Kourosh Parand, Fattaneh Bayatbabolghani. Presentation (ICDL 5.0) 2012 (in Farsi)
23. Kourosh Parand, Fattaneh Bayatbabolghani. Web Browsing and Communication (ICDL 5.0) 2012 (in Farsi)
24. Kourosh Parand, Fattaneh Bayatbabolghani. Presentation (ICDL 4.0) 2012 (in Farsi)
25. Kourosh Parand, Fattaneh Bayatbabolghani. Information and Communication (ICDL 4.0) 2012 (in Farsi)

## 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) (short-talk), San Jose, CA |
| May 2017 | University of Notre Dame, Notre Dame, IN |
| November 2016 | International Workshop on Genome Privacy and Security (GenoPri'16), 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)

## 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)

## 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 |