Mariana Raykova

Computer Science Laboratory, SRI International,
333 Ravenswood Ave, Menlo Park, CA 94025
Phone: 347 209 6679 Email: mariana@cs.columbia.edu Homepage : http://www.cs.columbia.edu/∼mariana

EDUCATION

Columbia University, New York, NY 2006-2012

- **Ph.D.**, Computer Science, 2012
- **M.Phil.**, Computer Science, 2010; **GPA** : 4.08/4.00
- **M.S.**, Computer Science, 2008; **GPA** : 4.08/4.00
- Thesis: *Secure Computation in Heterogeneous Environments: How to Bring Multiparty Computation Closer to Practice?*
- Advisors: *Tal Malkin* and *Steven Bellovin*

Bard College, Annandale-on-Hudson, NY 2006

- **B.A.**; Majors : Mathematics, Computer Science; **GPA** : 4.00/4.00

RESEARCH AND DEVELOPMENT EXPERIENCE

SRI, Computer Scientist, *Computer Science Laboratory* September 2013–Present

IBM T.J.Watson Research Center, Postdoc, *Cryptography Group* August 2012–August 2013

Columbia University, Visiting Researcher, *Computer Science Department* August 2012–Present

Columbia University, Research Assistant, *Computer Science Department* 2006–2012

- Developed cryptographic protocols for efficient secure computation, encrypted search, verifiable computation and collaborated on implementation of secure search protocols.

Microsoft Research, Redmond, WA, Intern, *Security Group* June - September, 2011

- Worked on protocols for verifiable computation on outsourced data, studied relationships between verifiable computation and other cryptographic primitives.

Microsoft Research, Redmond, WA, Intern, *Cryptography Group* June - August, 2010

- Worked on protocols for outsourced computation for specific functionalities with applications to genomic computation, study of social graphs, auctions in the model of cloud computing.

UC Berkeley, Visiting Student Researcher, *advisor: David Wagner* January - May, 2010

- Worked on cryptographic protocols for remote voting.
- Analysis and evaluation of a proposal for electronic voting protocol in Norway.

Microsoft Research, Redmond, WA, Intern, *Cryptography Group* June - August, 2009

- Worked on protocols for efficient secure outsourced computation in the presence of non-colluding adversaries.

Telcordia Technologies (former Bellcore), Piscataway, NJ, Intern June - August, 2008
Applied Research Group

- Participated in the policy team of the ZODIAC project developing a new model for communication over mobile ad-hoc networks with strict network security requirements. Contributed to the definitions, the design, the implementation, and the security analysis of the policy system.

Google Inc., Mountain View, CA, Intern, *Security Team* June - August, 2007

- Contributed to the extension and implementation of security protocols for server authentication aiming at good efficiency and parallel execution.

University of Minnesota, Duluth, MN, Undergraduate Researcher June - August, 2005
Research Experience for Undergraduates (REU), director: Joseph Gallian

- Conducted research in discrete mathematics and published a paper on permutation reconstruction.

Los Alamos National Laboratory, Los Alamos, NM, Intern, *CCS-5* June - August, 2004

- Collaborated on the development of mathematical models for simulation and the generation of large amount of simulation data with statistics corresponding to real survey data.

University of California Los Angeles, Los Angeles, CA, Intern June - August, 2003

Research in Industrial Projects for Undergraduates (RIPS)

- Developed and implemented algorithms for improving quality of images from film scanners as a team of four in the project of Image Correction given by Los Alamos National Laboratory.

PUBLICATIONS

Semantically Secure Order-Revealing Encryption: Multi-Input Functional Encryption Without Obfuscation, Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, Joe Zimmerman, *Proceedings of the* 34^{th} *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2015*

Outsourcing Private RAM Computation, Craig Gentry, Shai Halevi, Mariana Raykova, Daniel Wichs, *Proceedings of the* 55^{th} *IEEE Symposium on Foundations of Computer Science (FOCS), 2014*

Garbled RAM Revisited, Craig Gentry, Shai Halevi, Steve Lu, Rafail Ostrovsky, Mariana Raykova, Daniel Wichs, *Proceedings of the* 33^{d} *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2014*

Two-round secure MPC from Indistinguishability Obfuscation, Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, *Proceedings of the* 11^{th} *Theory of Cryptography Conference (TCC), pp. 74-94 2014*

Co-Location-Resistant Clouds, Yossi Azar, Seny Kamara, Ishai Menache, Mariana Raykova, Bruce Shepherd, *Proceedings of the ACM Cloud Computing Security Workshop (CCSW), 2014*

Scaling Private Set Intersection to Billion-Element Sets, Seny Kamara, Payman Mohassel, Mariana Raykova, Saeed Sadeghian, *Proceedings of the 18th International Conference on Financial Cryptography and Data Security (FC), 2014*

Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits, Sanjam Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Amit Sahai, Brent Waters, *Proceedings of the IEEE* 54^{th} *Symposium of Foundations of Computer Science (FOCS), pp.40-49, 2013*

Pinocchio: Nearly Practical Verifiable Computation, Bryan Parno, Craig Gentry, Jon Howell, Mariana Raykova, *Proceedings of the* 34^{th} *IEEE Symposium on Security and Privacy, pp.238-252, 2013,* ***Best Paper Award***

Quadratic Span Programs and Succinct NIZKs without PCPs, Rosario Gennaro, Craig Gentry, Bryan Parno, Mariana Raykova, *Proceedings of the* 32^{nd} *Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp.626-645, 2013*

Optimizing ORAM and Using It Efficiently for Secure Computation, Craig Gentry, Kenny A. Goldman, Shai Halevi, Charanjit S. Jutla, Mariana Raykova, Daniel Wichs, *Proceedings of the* 13^{th} *Privacy Enhancing Technologies Symposium (PETS), pp.1-18, 2013*

Adaptive and Concurrent Secure Computation from New Notions of Non-Malleability, Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Muthuramakrishnan Venkitasubramaniam, *Proceedings of the 19th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT), pp.316-336, 2013*

Shroud: Enabling Private Access to Large-Scale Data in the Data Center, Jacob R. Lorch, James Mickens, Bryan Parno, Mariana Raykova, Joshua Schiffman, *Proceedings of the 11th USENIX conference on File and Storage Technologies (FAST), pp.199-214, 2013*

Parallel Homomorphic Encryption, Seny Kamara, Mariana Raykova, *Workshop on Applied Homomorphic Cryptography (WAHC), pp. 213-225, 2013*

Secure Computation with Sublinear Amortized Work, Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Fernando Krell, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis, *Proceedings of the* 19^{th} *ACM Conference on Computer and Communications Security (CCS), pp. 513-524, 2012*

How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption, Bryan Parno, Mariana Raykova, Vinod Vaikuntanathan, *Proceedings of the 9^{th} Theory of Cryptography Conference (TCC), pp. 422-439, 2012*

Privacy Enhanced Access Control for Outsourced Data Sharing, Mariana Raykova, Hang Zhao, Steven Bellovin, *Proceedings of the 16th International Conference on Financial Cryptography and Data Security (FC), pp. 223-238, 2012*

Efficient Robust Private Set Intersection, Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung, *International Journal of Advancements in Computing Technology (IJACT), Vol. 2, No. 3, pp.289-303, 2012*

Outsourcing Multi-Party Computation, Seny Kamara, Payman Mohassel, Mariana Raykova, *Cryptology ePrint Archive: Report 2011/272, 2011*

Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications, Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung, *Proceedings of the 9th International Conference Applied Cryptography and Network Security (ACNS), pp.130-146, 2011*

Private Search in the Real World, Vasilis Pappas, Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin, *Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC), pp.83-92, 2011*

Amortized Sublinear Secure Multi Party Computation, Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis, *Workshop on Cryptography and Security in Clouds, IBM Zurich, 2011*

Secure Outsourced Computation in a Multi-Tenant Cloud, Seny Kamara, Mariana Raykova, *Workshop on Cryptography and Security in Clouds, IBM Zurich, 2011*

Usable Secure Private Search, Mariana Raykova, Ang Cui, Binh Vo, Bin Liu, Tal Malkin, Steven M. Bellovin, Salvatore J. Stolfo, *IEEE Security & Privacy, vol.10, issue 5, pp.53-60, 2012*

Verifiable Remote Voting with Large Scale Coercion Resistance, Mariana Raykova, David Wagner, *Technical Report CUCS-041-11, Columbia University, 2011*

Secure Anonymous Database Search, Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin, *Proceedings of the 1^{st} Cloud Computing Security Workshop (CCSW), pp.115-126, 2009*

Efficient Robust Private Set Intersection, Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung, *Proceedings of the 7th International Conference Applied Cryptography and Network Security (ACNS), pp. 125-142, 2009*

The Zodiac Policy Subsystem: a Policy-Based Management System for a High-security MANET, Yuu-Heng Cheng, Scott Alexander, Alexander Poylisher, Mariana Raykova, Steven Bellovin, *Proceedings of the 10th IEEE international Conference on Policies for Distributed Systems and Networks (POLICY), pp.174-177, 2009*

PAR: Paying for Anonymous Routing, Elli Androulaki, Mariana Raykova, Shreyas Srivatsan, Angelos Stavrou, and Steven M. Bellovin, *Proceedings of the 8th International Symposium on Privacy Enhancing Technologies Symposium (PETS), pp.219-236, 2008*

RUST: A Retargetable Usability Testbed for Web Site Authentication Technologies, Maritza Johnson, Chaitanya Atreya, Adam Aviv, Mariana Raykova, Steven Bellovin, Gail Kaiser,*Proceedings of the 1^{st} Conference on Usability, Psychology, and Security (UPSEC), pp.11:1-11:7, 2008*

Permutation Reconstruction from Minors, Mariana Raykova, *Electronic Journal of Combinatorics, vol.13, issue 3, R66, 2006*

Research Project on SHA1, Mariana Raykova, *Senior Project, Bard College, 2006*

Sequential Dynamical Systems, Mariana Raykova, *Senior Project, Bard College, 2005*

Image Correction, Mariana Raykova, Hayward Chan, Balint Felszeghy, Jiashen You, *Final Report, RIPS, IPAM, UCLA, 2003*

GRANTS

NSF CNS 1421102: TWC: Small: Collaborative: Computation and Access Control on Big Multiuser Data, $320,941, August 2014 - July 2017

PATENTS

Secure Computation Using a Server Module, Mariana Raykova, Seny Kamara, *United States Patent and Trademark Office, Patent No.: US 8,539,220 B2, Sep 17, 2013*

Counting Delegation Using Hidden Vector Encryption, Mariana Raykova, Seny Kamara, *United States Patent and Trademark Office, Patent No.: US 8,370,621 B2, Feb 5, 2013*

Secure Computing in Multi-Tenant Data Centers, Seny Kamara, Mariana Raykova, *United States Patent and Trademark Office, Publication number: US 2012/0185946 A1, Jul 19, 2012*

Polynomial Evaluation Delegation, Seny Kamara, Mariana Raykova, *United States Patent and Trademark Office, Publication number: US 2012/0151205 A1, Jun 14, 2012*

PROGRAM COMMITTEES

The 35th IACR International Cryptology Conference (CRYPTO), Santa Barbara, USA, 2015

The 12th IACR Theory of Cryptography Conference (TCC), Warsaw, Poland, 2015

The 21st ACM Conference on Computer and Communications Security (CCS), Scottsdale, Arizona, USA, 2014

The 17th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC), Buenos Aires, Argentina, 2013

The ACM Cloud Computing Security Workshop (CCSW), Berlin, Germany, 2013

The ACM Cloud Computing Security Workshop (CCSW), Raleigh, USA, 2012

The 8th China International Conference on Information Security and Cryptology (INSCRYPT), Beijing, China, 2012

PRESENTATIONS and POSTERS

Conference Talk: **Interesting Questions in Cryptography**

- Grace Hopper Celebration of Women in Computing, October 8-10, 2014

Invited Talk: **Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits**

- 52nd Annual Allerton Conference on Communication, Control, and Computing, October 1-3, 2014

Workshop Talk: **Secure Computation with Random Access Machines**

- Workshop on Applied Multi-Party Computation, Microsoft Research Redmond, February 20-21, 2014

Research Talk: **Candidate Indistinguishability Obfuscation and Functional Encryption for All Circuits**

- Microsoft Research, Silicon Valley, 2014
- Microsoft Research Redmond, 2014

Research Talk: **Succinct NIZKs from Quadratic Span Programs (QSPs) and Quadratic Arithmetic Programs (QAPs), and Pinocchio - a system for nearly practical verifiable computation.**

- Stanford University, 2013
- NYC Crypto Day, 2013

Conference Talk: **Quadratic Span Programs and Succinct NIZKs without PCPs**

- Eurocrypt, Athens, Greece, 2013

Research Talk: **Quadratic Span Programs and Succinct NIZKs without PCPs**

- University of Toronto, 2012

Research Talk: **How to Delegate and Verify in Public: Verifiable Computation from Attribute-based Encryption**

- Microsoft Research, Redmond, 2011; IBM Research, Hawthorne, 2011; New York University, 2011; Columbia University, 2011

Conference Talk: **Secure Computation with Sublinear Amortized Work**

- Conference on Computer and Communications Security (CCS), Raleigh, USA, 2012;
- IBM Research, Hawthorne, 2011; Microsoft Research, Redmond, 2011; PARC, 2011; Stanford University, 2011; UC Berkeley, 2011; Technical University of Catalonia (UPC), 2011

Conference Talk: **Multiparty Secure Computation over Multivariate Polynomials**

- Applied Cryptography and Network Security (ACNS), Nerja, Spain, 2011

Poster Presentation: **Trade-offs in Private Search**

- IEEE Symposium on Security and Privacy, Oakland, USA, 2010

Poster Presentation: **Secure Anonymous Database Search**

- ACM Conference on Computer and Communications Security (CCS), Chicago, USA, 2009

Conference Talk: **Secure Anonymous Database Search**

- The ACM Cloud Computing Security Workshop (CCSW), Chicago, USA, 2009

Conference Talk: **Efficient Robust Private Set Intersection**

- Applied Cryptography and Network Security (ACNS), Paris-Rocquencourt, France, 2009

TEACHING EXPERIENCE

Columbia University, *Teaching Assistant in* ***Network Security*** 2009

- Prepared and taught lectures, graded homework and exams.

Columbia University, *Teaching Assistant in* ***Introduction to Cryptography*** 2008

- Graded homework and exams, taught review sessions.

Columbia University, *Teaching Assistant in* ***Calculus*** 2006

- Graded homework and exams, hold office hours and review sessions.

Bard College, *Tutor in Mathematics* 2002-2006

- Taught review sessions, conducted individual and group tutoring sessions.

AWARDS

Departmental Fellowship, Columbia University Computer Science Department 2006-2007

Distinguished Scientist Scholar, Bard College 2002-2006
Full tuition awarded by Bard College

Awards for Excellence in Mathematics, Bard College 2003, 2004, 2005, 2006

The C.V. Starr Scholarship, Bard College 2003, 2004, 2005
Awarded by Bard College for academic excellence.

Included in The National Dean's List 2003