Antigoni Polychroniadou

✉ antigoni@cornell.edu
www.cs.cornell.edu/~polychroniadou
Born in Thessaloniki, Greece, 1989

Research Interests

Theoretical Computer Science. In particular, cryptography and its interplay with complexity theory.

Education

2012–2016 **Ph.D. in Computer Science**,
Aarhus University, Denmark,
Thesis title: On the Communication and Round Complexity of Secure Computation.
Supervisor: Prof. Ivan Damgård
Jury: Prof. Ran Canetti, Daniel Wichs

2011–2012 **M.Sc. in Mathematics of Cryptography and Communications**,
Royal Holloway University of London, UK,
HE Masters Level Distinction (First class honors, top 1%),
Thesis title: New Directions in Recovering Noisy RSA Keys (An Information Theoretic Approach).
Supervisor: Prof. Kenneth G. Paterson

2007–2011 **B.A. in Computer Science and Economics**,
University of Macedonia, Greece,
GPA : 8.86 / 10 (Ranked 1st),
Thesis title: Compatibility between IBE-related Schemes.
Supervisor: Prof. George Stephanides

Professional Experience

Jul 2018–current **Postdoctoral researcher/Simons society junior Fellow**, *Cornell Tech*, New York, NY.
Hosts: Prof. Rafael Pass and Prof. Elaine Shi

2017–Jun 2018 **Postdoctoral researcher**, *Cornell University*, New York, NY.
Hosts: Prof. Rafael Pass and Prof. Elaine Shi

Summer 2016 **Intern**, *IBM Research T.J. Watson*, New York
Mentor: Tal Rabin.

Summer 2015 **Intern**, *Simons Institute* , Berkeley University, CA
Special summer program on Cryptography.

Summer 2014 **Intern**, *IDC Herzliya*, Israel
Mentor: Alon Rosen.

Mar.–Oct. 2015 **Research Scholar**, *Berkeley University*, CA
Mentor: Sanjam Garg.

Jan.–Feb. 2015 **Research visit**, *Technion*, Israel
Mentor: Prof. Yuval Ishai.

Teaching

Spring 2013 **Teaching assistant**, *Aarhus University*.
Course: Security

Fall 2013 and Fall 2014 **Teaching assistant**, *Aarhus University*.
Course: Concurrency

Spring 2014 **Teaching assistant**, *Aarhus University*.
Course: Algorithms and Data Structures

Honors & Awards

Junior Simons Fellowship by the Simons Society of Fellows, 2018 (only computer scientist out of nine awardees). Fellows

Named in the 2017 Rising Stars list of 60 women in computer science and electrical engineering.

M.Sc Scholarship for Royal Holloway University of London by Lilian Voudouri Foundation.

M.Sc Scholarship by IKY State Scholarships Foundation (declined).

Dean's Prize from University of Macedonia, Greece, for ranking 1st in B.A.

Excellence Award and Scholarship from University of Macedonia for being the best student during B.A. in 2010 and 2011.

Awarded Degrees of excellence from the Greek Ministry of National Education in the following years: 2002-2003, 2003-2004, 2005-2006, 2006-2007.

Professional Activities

Program Committees

PKC 2019, TCC 2018, SCN 2018, PKC 2018

External reviewer

CRYPTO 2018, EUROCRYPT 2018,TCC 2017, CRYPTO 2017, EUROCRYPT 2017, PKC 2017, ASIACRYPT 2017, TCC 2016, ASIACRYPT 2016, CRYPTO 2016, EUROCRYPT 2016, PKC 2016, Indocrypt 2016, CCS 2016, TCC-A 2016, SCN 2016, ACNS 2016, ASIACRYPT 2015, CRYPTO 2015, TCC 2015, PKC 2015, ICALP 2014, ProvSec 2014, ASIACRYPT 2014, PETS 2013, InsCrypt 2013, Journal of Cryptology.

Administration and organization

2013-current International Association for Cryptologic Research (IACR) member.

Spring 2013 Organizer of the study group on Efficient Secure Computation, Aarhus University.

2008–2011 Teaching high school students Algebra and Geometry

Invited Talks

Round-Optimal Secure Multi-Party Computation.
Theory and Practice of Multi-Party Computation Workshop (TPMPC), 2018.

Laconic Oblivious Transfer and its Applications.
Boston University Theory Seminar, 2018.
IBM Research T.J. Watson, New York, 2017.
Athens Cryptography Day, 2017 (at National Technical University of Athens).
Aarhus University Theory Seminar, 2016.
Tsinghua-Cornell Workshop on security and Cryptography, 2016.

The Exact Round Complexity of Secure Computation.
DIMACS Workshop on Cryptography for the RAM Model, 2016 (at MIT).
CryptoAction Symposium 2016, Budapest, 2016.
University of Maryland Theory Seminar, 2016.
IBM Research T.J. Watson, New York, 2016.

On the Communication required for Unconditionally Secure Multiplication.
Rutgers/DIMACS Theory of Computing Seminar, 2017 (at Rutgers University).
IvanFest, Symposium on the Work of Ivan Damgård for his 60th birthday, 2016.
IBM Research T.J. Watson, New York, 2016.
Cryptography Reunion Workshop at the Simons Institute, 2016 (at Berkeley University).

Composable Security in the Tamper Proof Model under Minimal Complexity.
New York Area Crypto Day, 2017.
Theory and Practice of Multi-Party Computation Workshop (TPMPC), 2017 (University of Bristol).

Efficient Multi-Party Computation: from Passive to Active Security via Secure SIMD Circuits.
Securing Computation Workshop at the Simons Instituite, 2015 (at Berkeley University).

Two-Round Adaptively Secure MPC from Indistinguishability Obfuscation.
Athens Cryptography Day, 2015 (at National Technical University of Athens).
COST Action workshop co-located with TCC 2015, 2015.

Adaptively Secure UC Constant Round Multi-Party Computation Protocols.
Theory of Cryptography workshop, 2014 (at Tsinghua University).
Technion University Theory Seminar, 2014.
Greater Tel Aviv Cryptography Seminar,Tel Aviv University, 2014.

A Coding-Theoretic Approach to Recovering Noisy RSA Keys.
IDC Herzliya Computer Science Seminar, 2014.
Aarhus University Theory Seminar, 2012.

Exploring Relations Between IBE-related schemes.
CrossFyre for female researchers workshop, 2011 (at TU Darmstadt).

Publication List

Note about author ordering conventions: The convention in theory papers (including cryptography) is alphabetical order. All listed papers (except from 3 postgraduate publications) use alphabetical order.

Two-Round Adaptively Secure Protocols from Standard Assumptions. In TCC'18.
Fabrice Benhamouda, Huijia Lin, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam.

More is Less: Perfectly Secure Oblivious Algorithms in the Multi-Server Setting. In ASIACRYPT'18.
Hubert Chan, Jonathan Katz, Kartik Nayak, Antigoni Polychroniadou, and Elaine Shi.

Limits of Practical Sublinear Secure Computation. In CRYPTO'18.
Elette Boyle, Yuval Ishai, and Antigoni Polychroniadou.

Round-Optimal Secure Multi-Party Computation. In CRYPTO'18.
Shai Halevi, Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam.

Four Round Secure Computation without Setup. In TCC'17.
Zvika Brakerski, Shai Halevi, and Antigoni Polychroniadou.

Laconic Oblivious Transfer and Its Applications. In CRYPTO'17.
Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou.

Constant Round Adaptively Secure Protocols in the Tamper-Proof Hardware Model. In PKC'17.
Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam.

Composable Security in the Tamper-Proof Hardware Model Under Minimal Complexity. In TCC'16.
Carmit Hazay, Antigoni Polychroniadou, and Muthuramakrishnan Venkitasubramaniam.

The Exact Round Complexity of Secure Computation. In EUROCRYPT'16.
Sanjam Garg, Pratyay Mukherjee, Omkant Pandey, and Antigoni Polychroniadou.

On the Communication Required for Unconditionally Secure Multiplication. In CRYPTO'16.
Ivan Damgård, Jesper Buus Nielsen, Antigoni Polychroniadou, and Michael Raskin.

Adaptively Secure Multi-Party Computation from LWE (via Equivocal FHE). In PKC'16.
Ivan Damgård, Antigoni Polychroniadou, and Vanishree Rao.

Efficient Multi-party Computation: From Passive to Active Security via Secure SIMD Circuits. In CRYPTO'15.
Daniel Genkin, Yuval Ishai, and Antigoni Polychroniadou.

Two-Round Adaptively Secure MPC from Indistinguishability Obfuscation. In TCC'15.
Sanjam Garg and Antigoni Polychroniadou.

Efficient Leakage Resilient Circuit Compilers. In CT-RSA'15.
Marcin Andrychowicz, Ivan Damgård, Stefan Dziembowski, Sebastian Faust, and Antigoni Polychroniadou.

Postgraduate Research Publications

A Coding-Theoretic Approach to Recovering Noisy RSA Keys. In ASIACRYPT'12.
Kenneth G. Paterson, Antigoni Polychroniadou, and Dale L. Sibborn.

The Concept of Compatibility between Identity-based and Certificateless Encryption Schemes. In SECRYPT'12.
Antigoni Polychroniadou, Konstantinos Chalkias, and George Stephanides.

Improved NetArgus - A Suite of Wi-fi Positioning & SNMP Monitor. In SIGMAP and WINSYS'12.
Tryfon Theodorou, George E. Violettas, Antigoni Polychroniadou, and Christos K. Georgiadis.

A Compatible Implementation between Identity-based and Certificateless Encryption Schemes. In WEBIST'12.
Antigoni Polychroniadou, Konstantinos Chalkias, and George Stephanides.