Curriculum Vitae

University of California, Los Angeles
Department of Computer Science
Los Angeles, CA 90095-1596
☎ +1 (424) 781-7942
✉ vzikas@cs.ucla.edu
www.cs.ucla.edu/~vzikas

Vassilis Zikas

Postdoctoral Researcher, UCLA

Education

2006–2010 **PhD in Computer Science**, Information Security and Cryptography Group, ETH Zurich
Dissertation: Generalized Corruption Models in Secure Multi-Party Computation
Supervisor: Ueli Maurer.

1999–2004 **Diploma (5-year degree)**, School of Applied Mathematics and Physics, NTUA (Greece)
Major: Computer Science and Applied Mathematics.

Work Experience

Academic

2012–present **Postdoctoral Researcher,** Department of Computer Science, UCLA
Supervisor: Rafail Ostrovsky.

2010–2012 **Postdoctoral Researcher,** Department of Computer Science, University of Maryland
Supervisor: Jonathan Katz.

Aug–Oct 2005 **Research Intern**, Department of Computer Science, ETH Zurich.

2004–2005 **Graduate Research Associate**, School of Electrical and Computer Engineering, NTUA.

Other

2002–2005 **Network Administrator**, School of Applied Mathematics and Physics, NTUA.

Jul 2002 **Database Developer (Internship)**, 01 Informatics A.E., Athens, Greece.

Research Grants and Fellowships

2012 **Ambizione Grant (Senior Researcher at ETH Zurich, Switzerland)**
Swiss National Science Foundation – pending my acceptance *($400,000)*

2011 **Postdoctoral Fellowship for Prospective Researchers**
Swiss National Science Foundation *($42,500)*

2005 **Award for Academic Excellence**, *Technical Chambers of Greece*.

Publications in Peer-reviewed Conferences

CRYPTO 2014 “Secure Multi-Party Computation with Identifiable Abort,” with Y. Ishai and R. Ostrovsky.
Advances in Cryptology – CRYPTO 2014 (to appear).

CRYPTO 2014 “Efficient Three-Party Computation from Cut-and-Choose,” with S. G. Choi, J. Katz, and A. Malozemoff.
Advances in Cryptology – CRYPTO 2014 (to appear).

PODC 2014 “Distributing the Setup in Universally Composable Secure Multi-Party Computation,” with J. Katz, A. Kiayias, and H.-S. Zhou.
ACM Symposium on Principles of Distributed Computing – PODC 2014 (to appear).

FOCS 2013 “Rational Protocol Design: Cryptography Against Incentive-Driven Adversaries,” with J. Garay, J. Katz, U. Maurer, and B. Tackmann.
IEEE Symposium on Foundations of Computer Science – FOCS 2013, IEEE Computer Society, pp. 648-657, 2013.

TCC 2013 “Universally Composable Synchronous Computation,” with J. Katz, U. Maurer, and B. Tackmann.
Theory of Cryptography Conference – TCC 2013, LNCS, Springer-Verlag, vol. 7785, pp. 477-498, 2013.

TCC 2013 “Feasibility and Completeness of Cryptographic Tasks in the Quantum World,” with J. Katz, S. Fehr, F. Song, and H.-S. Zhou.
Theory of Cryptography Conference – TCC 2013, LNCS, Springer-Verlag, vol. 7785, pp. 281-296, 2013.

CRYPTO 2012 “Collusion-Preserving Computation,” with J. Alwen, J. Katz, and U. Maurer.
Advances in Cryptology – CRYPTO 2012, LNCS, Springer-Verlag, vol. 7417, pp. 124-143, 2012.

ICALP 2012 “Byzantine Agreement with a Rational Adversary,” with A. Groce, J. Katz, and A. Thiruvengadam.
International Colloquium on Automata, Languages and Programming – ICALP 2012, LNCS, Springer-Verlag, vol. 7392, pp. 561-572, 2012.

ICALP 2011 “Player-Centric Byzantine Agreement,” with M. Hirt.
International Colloquium on Automata, Languages and Programming – ICALP 2011, LNCS, Springer-Verlag, vol. 6755, pp. 281–292, 2011.

EUROCRYPT 2010 “Adaptively Secure Broadcast,” with M. Hirt.
Advances in Cryptology – EUROCRYPT 2010, LNCS, Springer-Verlag, vol. 6110, pp. 466–485, 2010.

TCC 2009 "Realistic Failures in Secure Multi-Party Computation," with S. Hauser and U. Maurer.
Theory of Cryptography Conference – TCC 2009, LNCS, Springer-Verlag, vol. 5444, pp. 274-293, 2009.

ASIACRYPT 2008 "MPC vs. SFE: Unconditional and Computational Security," with M. Hirt and U. Maurer.
Advances in Cryptology – ASIACRYPT 2008, LNCS, Springer-Verlag, vol. 5350, pp. 1–18, 2008.

TCC 2008 "MPC vs. SFE: Perfect Security in a Unified Corruption Model," with Z. Beerliova-Trubiniova, M. Fitzi, M. Hirt, and U. Maurer.
Theory of Cryptography Conference – TCC 2008, LNCS, Springer-Verlag, vol. 4948, pp. 231–250, 2008.

Other Publications and Preprints

Invited Chapter

"Secure Multiparty Computation," with U. Maurer.
Editors: M. Prabhakaran and A. Sahai. IOS Press, Cryptology and Information Security Series, vol 10, ISBN978-1-61499-168-7, 2013.

PhD Thesis (Book)

"Generalized Corruption Models in Secure Multi-Party Computation."
Editor: U. Maurer. ETH Series in Information Security and Cryptography, Hartung-Gorre Verlag, ISBN 3-86628-338-5, 2010.

In Submission

- "Optimally Resilient and Adaptively Secure Multi-Party Computation with Low Communication Locality," with N. Chandran, W. Chongchitmate, J. Garay, S. Goldwasser, and R. Ostrovsky. Manuscript 2014.

- "Fair Computation Against Incentive-driven Adversaries," with J. Garay, J. Katz, and B. Tackmann. Manuscript 2014.

- "Practical Fair Computation via a Public Ledger," with A. Kiayias, and H.-S. Zhou. Manuscript 2014.

Other Written Work

- "Zero-knowledge Proofs."
Diploma Thesis (Supervisor: S. Zachos), NTUA, 2004.

- One chapter for the lecture notes of the course "Cryptography and Complexity" (Instructor: S. Zachos), NTUA, 2004.

- Two chapters for the lecture notes of the course "Number Theory and Cryptography" (Instructor: A. Papaioannou), NTUA, 2004.

- “Side-Channel Attacks,” with G. Amanatidis and S. Zachos.
Workshop on Internet–Education–Science, Pristina, Serbia, 2004.

Teaching Experience and Student Supervision

Teaching Assistant

2010 “Kryptographische Protokolle (Cryptographic Protocols),” Department of Computer Science, ETH Zurich.

2009 “Kryptographische Protokolle (Cryptographic Protocols),” Department of Computer Science, ETH Zurich.

2008 “Kryptographie (Cryptography),” Department of Computer Science, ETH Zurich.

2008 “Information Security,” Department of Computer Science, ETH Zurich.

2007 “Kryptographische Protokolle (Cryptographic Protocols),” Department of Computer Science, ETH Zurich.

2006 “Information Security,” Department of Computer Science, ETH Zurich.

2003–2005 “Number Theory and Cryptography,” School of Applied Mathematics and Physics, NTUA.

2004–2005 “Cryptography and Complexity,” School of Electrical and Computer Engineering, NTUA.

2000–2004 “Introduction to Programming,” School of Electrical and Computer Engineering, NTUA.

2000–2004 “Introduction to Programming,” School of Applied Mathematics and Physics, NTUA.

Student Supervision

2008 “Modeling Failures in Byzantine Agreement,” S. Hauser.
Master’s Thesis, Department of Computer Science, ETH Zurich.

2008 “Perfectly Secure Message Transmission Tolerating a Mixed Adversary,” B. Lutz.
Semester Thesis, Department of Computer Science, ETH Zurich.

Organized Seminars and Lectures

2012–present *Theoretical Computer Science and Cryptography Colloquium,* Department of Computer Science, UCLA.

Fall 2005 *“Cryptography and Complexity,”* course taught jointly with A. Pagourtzis, School of Electrical and Computer Engineering, NTUA.

2005 *Cryptography Seminar,* School of Electrical and Computer Engineering, NTUA.

Other

2003–2004 Instructor for University Entrance Exams, Athens, Greece.

Invited Talks

February 2014 “Cryptography & Secure Computation: Theory and Applications,” University of Southern California, Los Angeles, USA.

July 2013 “Rational Protocol Design: Cryptography Against Incentive-Driven Adversaries,” University of Maryland, College Park, USA.

April 2013 “Rational Protocol Design: Cryptography Against Incentive-Driven Adversaries,” *DIMACS Workshop on Current Trends in Cryptology,* AT&T Building, New York, USA.

January 2013 “Universally Composable Synchronous Computation,” *Athens Cryptography Day (AtheCrypt 2013),* NTUA, Athens, Greece.

July 2012 “Realistic Models for Secure Computation,” Eurecom, Sophia Antipolis, France.

March 2012 “Realistic Models for Secure Computation,” Saarland University, Saarbruecken, Germany.

January 2012 “Secure Computation with Corruptible Setups,” IBM Zurich – Research, Zurich, Switzerland.

November 2011 “Player-Centric Byzantine Agreement,” *4th New York Colloquium on Algorithms and Complexity,* The Graduate Center, CUNY, New York, USA.

October 2011 “Universally Composable Synchronous Computation,” Department of Computer Science, Boston University, Boston, USA.

October 2011 “Secure Computation with Corruptible Setups,” Department of Computer Science, Boston University, Boston, USA.

September 2011 “Secure Computation with Corruptible Setups,” *Public-Key Cryptography,* Dagstuhl, Germany.

July 2011 “Player-Centric Byzantine Agreement,” *1st Cryptography and Security Day,* Department of Computer Science, University of Athens, Athens, Greece.

March 2011 “Adaptively Secure Broadcast,” AT&T Research Labs, New Jersey, USA.

June 2010 “Cryptographic Protocols and Secure Computation,” Department of Computer Science, University of Ioannina, Ioannina, Greece.

June 2010 “Generalized Corruption Models in Secure Multi-Party Computation,” *Theoretical Computer Science Seminar,* Computation and Reasoning Lab, NTUA, Athens, Greece.

June 2009 “Omission-Corruption in Secure Multi-Party Computation,” *Workshop on Cryptographic Protocols and Public-Key Cryptography – WPK 2009,* Bertinoro (Forlì-Cesena) Italy.

June 2008 “MPC vs. SFE: Perfect Security in a Unified Corruption Model,” *Theoretical Computer Science Seminar,* Computation and Reasoning Lab, NTUA, Athens, Greece.

Professional Activities

Program Committee Member

2014	**CRYPTO 2014**
2014	Conference on Cryptology and Network Security (**CANS 2014**)

Conference Organization

2013	**EUROCRYPT 2013,** Finances Chair, Athens, Greece.
2010	**TCC 2010,** Local organizing committee, Zurich, Switzerland.

External Reviewer (Conferences)

2014	EUROCRYPT
2013	TCC, EUROCRYPT, ICALP, PETS, DISC, ASIACRYPT
2012	CRYPTO, ASIACRYPT
2011	ICITS, TCC, EUROCRYPT
2010	TCC, SCN, PKC
2009	CRYPTO, TCC, ICALP, CT-RSA, AFRICACRYPT, ICITS
2008	CRYPTO, SCN

External Reviewer (Journals)

- Transactions on Economics and Computation (ACM)
- Transactions on Dependable and Secure Computing (IEEE)
- Distributed Computing (Springer-Verlag)
- Theoretical Computer Science (Elsevier)
- Information Processing Letters (Elsevier).

Languages

English	Excellent	*Diplomas: Proficiency of Cambridge, Proficiency of Michigan*
Greek	Excellent	
German	Very good	*Diploma: Mittelstuffe, Goethe Institute*
French	Basic	

Recommendation Letters

Rafail Ostrovsky

Professor and Director
Center for Information and Computation Security
Department of Computer Science
University of California, Los Angeles (UCLA)
url: http://www.cs.ucla.edu/~rafail/

Contact Info:
Department of Computer Science
UCLA
3732D Boelter Hall
Los Angeles, CA 90095-1596, USA
mail: rafail@cs.ucla.edu

Jonathan Katz

Professor and Director
Maryland Cybersecurity Center
Department of Computer Science and UMIACS
University of Maryland
url: http://www.cs.umd.edu/~jkatz/

Contact Info:
Department of Computer Science
University of Maryland
3225 A.V. Williams Building
College Park, MD 20742, USA
mail: jkatz@cs.umd.edu

Ueli Maurer (PhD Supervisor)

Professor
Department of Computer Science
ETH Zurich
url: http://www.crypto.ethz.ch/~maurer/

Contact Info:
Department of Computer Science
ETH Zurich
CH - 8092 Zurich, Switzerland
mail: maurer@inf.ethz.ch

Dr. Juan A. Garay

Sr. Principal Research Scientist
Yahoo Labs

Contact Info:
Yahoo Labs
701 First Avenue
Sunnyvale, CA 94089, USA
mail: garay@yahoo-inc.com