Curriculum Vitae

Vassilis Zikas

Associate Professor, University of Edinburgh
Vice-director, Blockchain Technology Lab

University of Edinburgh
School of Informatics
Edinburgh, EH8 9AB, UK
homepages.inf.ed.ac.uk/vzikas

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

2018–present **Associate Professor (Sr. Lecturer,)** School of Informatics, University of Edinburgh.
Vice-director of the Blockchain Technology Laboratory

2018–present **Research Fellow,** IOHK.
Area Leader: Multi-Party Computation

May 2018–present **Visiting Faculty,** Department of Computer Science, UCLA

2016–2018 **Assistant Professor,** Department of Computer Science, RPI.

May–Aug 2015 **Research Fellow,** Simons Institute for the Theory of Computing, UC Berkeley.

2014–2016 **Senior Research Associate,** Department of Computer Science, ETH Zurich.

2012–2014 **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.

Awards and Fellowships

2015 **Simons Fellowship for Summer 2015**
Simons Institute for Theoretical Computing, UC Berkeley.

2011 **Fellowship for Prospective Researchers**
Swiss National Science Foundation.

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

Research Grants

2014 **Ambizione Grant (Career development grant, ETH Zurich, Switzerland)**
Swiss National Science Foundation $ ETH Zurich. *($500,000)*

2016 **Research Gift**
IOHK. *($25,000)*

2017 **Research Gift**
IOHK. *($127,000)*

2017 **Research Grant**
US Army Research Labs. *($25,000)*

Publications in Peer-reviewed Conferences

ACM CCS '18 "Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability," with C. Badertscher, P. Gazi, A. Kiayias, and A. Russell.
ACM Conference on Computer and Communications Security – ACM CCS 2018, ACM, pp. 913–930, 2018.

EUROCRYPT '18 "But Why does it Work? A Rational Protocol Design Treatment of Bitcoin," with C. Badertscher, J. Garay, U. Maurer, and D Tschudi.
Advances in Cryptology – EUROCRYPT 2018, LNCS, Springer, vol. 10821, pp. 34–65, 2018.

SCN '18 "Secure Two-Party Computation over Unreliable Channels," with R. Gelles, A. Paskin-Cherniavsky.
Security and Cryptography for Networks – SCN 2018, LNCS, Springer, vol. 11035, pp. 445–463, 2018.

CRYPTO '17 "Bitcoin as a Transaction Ledger: A Composable Treatment," with C. Badertscher, U. Maurer, and D Tschudi.
Advances in Cryptology – CRYPTO 2017, LNCS, Springer, vol. 10401, pp. 324–356, 2017.

CRYPTO '17 "The Price of Low Communication in Secure Multi-party Computation," with J. Garay, Y. Ishai, R. Ostrovsky.
Advances in Cryptology – CRYPTO 2017, LNCS, Springer, vol. 10401, pp. 420–446, 2017.

ICALP '17 "Round-Preserving Parallel Composition of Probabilistic-Termination Cryptographic Protocols," with R. Cohen, S. Coretti, J. Garay.
International Colloquium on Automata, Languages and Programming – ICALP 2017, Leibniz International Proceedings in Informatics, pp. 32:1–37:15, 2017.

CRYPTO '16 "Network-Hiding Communication and Applications to Multi-Party Protocols," with M. Hirt, U. Maurer, and D. Tschudi.
Advances in Cryptology – CRYPTO 2016, LNCS, Springer, vol. 9816, pp. 335–365, 2016.

CRYPTO '16 "Probabilistic Termination and Composability of Cryptographic Protocols," with R. Cohen, S. Coretti, and J. Garay.
Advances in Cryptology – CRYPTO 2016, LNCS, Springer, vol. 9816, pp. 240–269, 2016.

EUROCRYPT '16 "Fair and Robust Multi-Party Computation using a Global Transaction Ledger," with A. Kiayias, and H.-S. Zhou.
Advances in Cryptology – EUROCRYPT 2016, LNCS, Springer, vol. 9666, pp. 705–734, 2016.

ASIACRYPT '16 "Constant-Round Asynchronous Multi-Party Computation," with S. Coretti, J. Garay, and M. Hirt.
Advances in Cryptology – ASIACRYPT 2016 (to appear).

ICALP '16 "Provably Secure Virus Detection: Using The Observer Effect Against Malware," with R. J. Lipton, and R. Ostrovsky.
International Colloquium on Automata, Languages and Programming – ICALP 2016, Leibniz International Proceedings in Informatics, pp. 32:1–32:14, 2016.

DISC '15 "Fair distributed computation of reactive functions," with J. Garay, and B. Tackmann.
International Symposium on Distributed Computing – DISC 2015, LNCS, Springer, vol. 9363, pp. 497–512, 2015.

CRYPTO '15 "Incoercible Multi-Party Computation and Universally Composable Receipt-Free Voting," with J. Alwen, R. Ostrovsky, and H.-S. Zhou.
Advances in Cryptology – CRYPTO 2015, LNCS, Springer, vol. 9216, pp. 763–780, 2015.

PODC '15 "How Fair is Your Protocol? A Utility-based Approach to Protocol Optimality," with J. Garay, J. Katz, and B. Tackmann.
ACM Symposium on Principles of Distributed Computing – PODC 2015, ACM, pp 281–290.

ITCS '15 "The Hidden Communication Graph Model: Achieving Communication Locality and Optimal Resilience in the Presence of Adaptive Faults," with N. Chandran, W. Chongchitmate, J. Garay, S. Goldwasser, and R. Ostrovsky.
Innovations in Theoretical Computer Science – ITCS 2015, ACM, pp 153–162.

CRYPTO '14 "Secure Multi-Party Computation with Identifiable Abort," with Y. Ishai and R. Ostrovsky.
Advances in Cryptology – CRYPTO 2014, LNCS, Springer, vol. 8617, pp. 369-386, 2014.

CRYPTO '14 "Efficient Three-Party Computation from Cut-and-Choose," with S. G. Choi, J. Katz, and A. Malozemoff.
Advances in Cryptology – CRYPTO 2014, LNCS, Springer, vol. 8617, pp. 513-530, 2014.

PODC '14 "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, ACM, pp. 20-29, 2014.

FOCS '13 "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 '13 "Universally Composable Synchronous Computation," with J. Katz, U. Maurer, and B. Tackmann.
Theory of Cryptography Conference – TCC 2013, LNCS, Springer, vol. 7785, pp. 477-498, 2013.

TCC '13 "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, vol. 7785, pp. 281-296, 2013.

CRYPTO '12 "Collusion-Preserving Computation," with J. Alwen, J. Katz, and U. Maurer.
Advances in Cryptology – CRYPTO 2012, LNCS, Springer, vol. 7417, pp. 124-143, 2012.

ICALP '12 "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, vol. 7392, pp. 561-572, 2012.

ICALP '11 "Player-Centric Byzantine Agreement," with M. Hirt.
International Colloquium on Automata, Languages and Programming – ICALP 2011, LNCS, Springer, vol. 6755, pp. 281–292, 2011.

EUROCRYPT '10 "Adaptively Secure Broadcast," with M. Hirt.
Advances in Cryptology – EUROCRYPT 2010, LNCS, Springer, vol. 6110, pp. 466–485, 2010.

TCC '09 "Realistic Failures in Secure Multi-Party Computation," with S. Hauser and U. Maurer.
Theory of Cryptography Conference – TCC 2009, LNCS, Springer, vol. 5444, pp. 274-293, 2009.

ASIACRYPT '08 "MPC vs. SFE: Unconditional and Computational Security," with M. Hirt and U. Maurer.
Advances in Cryptology – ASIACRYPT 2008, LNCS, Springer, vol. 5350, pp. 1–18, 2008.

TCC '08 "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, vol. 4948, pp. 231–250, 2008.

Other Publications, Patents, 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.

Proceedings Editor

"Security and Cryptography for Networks – SCN 2016," with R. De Prisco. LNCS, Springer, vol. 9841, 2016

Patents

"Provably Secure Virus Detection," with R.J. Lipton and R. Ostrovsky.
Application Number: 62/054,160.

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

• "Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake," with T. Kerber, M. Kohlweiss, and A. Kiayias. Manuscript 2018.

• "Timed Signatures and Zero-Knowledge Proofs: Timestamping in the Blockchain Era," with M. Ciampi, A. Kheirbakhsh Abadi, and A. Kiayias. Manuscript 2018.

• "Cryptography with Disposable Backdoors," with Kai-Min Chung, Marios Georgiou, and Ching-Yi Lai. Manuscript 2018.

• "Cryptographically Secure Detection of Injection Attacks," with Y. Lu, K. Mitropoulos, R. Ostrovsky, and A. Weinstock. Manuscript 2018.
Preliminary version appeared as poster at ACM CCS 2018.

• "How Private Is Your Voting? A Framework for Comparing the Privacy of Voting Mechanisms," with A. Liu, Y. Lu, and L. Xia. Manuscript 2018.
Preliminary version appeared at WADE 2018.

Other Written Work

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

• Three chapters for the lecture notes of the courses "Cryptography and Complexity" and "Number Theory and Cryptography", NTUA, 2004.

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

Teaching Experience and Student Supervision

Courses

2019 Introduction to Modern Cryptography.

2017 Cryptography and Network Security I.

2016-2017 Cryptography and Network Security II.

2016 Special Topics in Security (Anonymity, Cryptocurrencies, and Privacy).
Fall 2016 School of Science "SuperTeacher" Award

Student Supervision

2016–present Yun Lu (PhD student, University of Edinburgh)

2016–present Muhammad Ishaq (PhD Student, University of Edinburgh)

2017–present Konstantinos Mitropoulos (PhD Student, University of Edinburgh)

2016–2017 Michael Macceletti (Master's student, RPI)

2017–2018 Connor Hendley (Master's student, RPI)

2008 Sarah Hauser (Master's student, ETH Zurich)

Organized Seminars and Lectures

2012–2014 *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.

Selected Invited Talks

October 2018 "Rational Protocol Design: Security Against Incentive-driven Adversaries (and Applications to Blockchains)," Texas A&M and Boston University, TX and MA, USA.

July 2018 "Secure Multi-Party Computation," ECI-IACR School on Modern Cryptography, University of Buenos Aires, Argentina.

May 2018 "Cryptography on the Blockchain," Engineering School Colloquium, Bar Ilan University, Tel Aviv, Israel.

January 2017 "Blockchain and secure computation," Winter School on Cryptocurrency and Blockchain Technologies, Shanghai, China.

November 2016 "Fair and Robust Multi-Party Computation using a Global Transaction Ledger," MIT CIS Seminar, Cambridge, MA, USA.

June 2016 "Provable Virus Detection: Using the Observer Effect Against Malware," The Greater Tel Aviv Area Cryptography Symposium (GTACS), Tel Aviv University, Israel.

June 2016 "Cryptography on the blockchain," IACR Summer School on Blockchain Technologies, Corfu, Greece.

May 2016 "Fair and Robust Multi-Party Computation using a Global Transaction Ledger," New York City Crypto Day, Columbia University, New York, USA.

July 2015 "Provable Virus Detection: Using the Uncertainty Principle to End Computer Malware," Stanford University, USA.

May 2015 "Secure Computation and Games," Simons Institute for the Theory of Computing, UC Berkeley, USA.

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.

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

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

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.

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

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

Professional Activities

Program Committee Chair

2016 **SCN 2016**

Program Committee Member

2018 **EUROCRYPT 2018, TCC 2018, INDOCRYPT 2018**

2017 **CRYPTO 2017, PKC 2017, FC 2017**

2016 **TCC 2016-A, PODC 2016**

2015 **ASIACRYPT 2015, INSCRYPT 2015**

2014 **CRYPTO 2014, CANS 2014**

Conference Organization

2013 **EUROCRYPT 2013,** Finances Chair, Athens, Greece.

2010 **TCC 2010,** Local organizing committee, Zurich, Switzerland.

External Reviewer (Journals)

- Journal of Cryptology (Springer-Verlag)
- Transactions on Economics and Computation (ACM)
- Security & Privacy (IEEE)
- Transactions on Dependable and Secure Computing (IEEE)
- Transactions on Information Theory (IEEE)
- Journal of Computer and System Sciences (Elsevier)
- Distributed Computing (Springer-Verlag)
- Theoretical Computer Science (Elsevier)
- Information and Computation (Elsevier)

- Information Processing Letters (Elsevier).

Languages

English (Excellent), Greek (Excellent), German (Very Good), French (Basic)