# Dr. Thomas Zacharias

Postdoctoral Researcher
Security and Privacy Group
School of Informatics
University of Edinburgh


# Curriculum Vitae


*Work Address*:
Informatics Forum, 10 Crichton St,
Edinburgh, EH89AB
United Kingdom
Tel: $+44\ (0)1316513835$

*E-mail* : tzachari@inf.ed.ac.uk

*Contact Number* : $+\ 44\ (0)7849524869$

*Personal Homepage*: `http://crypto.di.uoa.gr/~thomas/`

*Google Scholar*: `https://scholar.google.com/citations?user=h72OZv8AAAAJ&hl=en`


## Education

| | |
|---|---|
| April 2013 - July 2016 | **PhD** in Cryptography, Department of Informatics and Telecommunications, National and Kapodistrian University of Athens (*Grade*: Excellence). |
| October 2010 - July 2012 | **M.Sc.** in Logic and Theory of Algorithms and Computation, Department of Mathematics, National and Kapodistrian University of Athens (*Grade*: 9.54/10). |
| March 2006 - July 2010 | **Degree** in Pure Mathematics, National and Kapodistrian University of Athens (*Grade*: 8.62/10). |
| October 1999 - November 2005 | **Diploma** in Electrical and Computer Engineering, Aristotle University of Thessalonica (*Grade*: 6.98/10). |

## Research experience

| | |
|---|---|
| September 2016 - Present | Member of the PANORAMIX H2020 project research team (Project Coordinator: Professor Aggelos Kiayias). Design and development of a European infrastructure for secure communications based on mix-nets. *URL*: `https://panoramix-project.eu/` |
| May 2013 - September 2015 | Member of the FINER research team (Principal Investigator: Professor Aggelos Kiayias). Design, implementation and promotion of the DEMOS end-to-end verifiable electronic voting system. *URL*: `http://www.demos-voting.org` |

| | |
|---|---|
| October 2012 - August 2016 | Member of the CRYPTO.SEC group of Professor Aggelos Kiayias. |

## Publications

1. Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, Thomas Zacharias. *MCMix: Anonymous Messaging via Secure Multiparty Computation*. In USENIX Security Symposium, 2017. Available in IACR Cryptology ePrint Archive 2017/778.
2. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *An Efficient E2E Verifiable E-voting System without Setup Assumptions*. In IEEE Security & Privacy 15(3): 14-23 (2017).
3. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *Ceremonies for End-to-End Verifiable Elections*. In PKC, 2017. Available in IACR Cryptology ePrint Archive: 2015/1166.
4. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *Auditing for Privacy in Threshold PKE e-Voting*. In Information & Computer Security 25(1): 100-116 (2017).
5. Foteini Baldimtsi, Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *Indistinguishable Proofs of Work or Knowledge*. In ASIACRYPT, 2016. Available in Cryptology ePrint Archive: 2015/1230.
6. Nikos Chondros, Bingsheng Zhang, Thomas Zacharias, Panos Diamantopoulos, Stathis Maneas, Christos Patsonakis, Alex Delis, Aggelos Kiayias, Mema Roussopoulos. *A Distributed, End-to-end Verifiable, Internet Voting System*. In ICDCS, 2016. Available in CoRR abs/1507.06812, 2015.
7. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *On the Necessity of Auditing for Election Privacy in e-Voting Systems*. In e-Democracy, 2015.
8. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *DEMOS-2: Scalable E2E Verifiable Elections without Random Oracles*. In CCS, 2015.
9. Aggelos Kiayias, Thomas Zacharias, Bingsheng Zhang. *End-to-end Verifiable Elections in the Standard Model*. In EUROCRYPT, 2015. Available in IACR Cryptology ePrint Archive, 2015:346, 2015.
10. Alex Delis, Konstantina Gavatha, Aggelos Kiayias, Charalampos Koutalakis, Elias Nikolakopoulos, Lampros Paschos, Mema Roussopoulos, Georgios Sotirellis, Panos Stathopoulos, Pavlos Vasilopoulos, Thomas Zacharias, Bingsheng Zhang. *Pressing the Button for European Elections: Verifiable e-Voting and Public Attitudes Toward Internet Voting in Greece*. In EVOTE, 2014.
11. Nikos Chondros, Alex Delis, Dina Gavatha, Aggelos Kiayias, Charalampos Koutalakis, Ilias Nicolacopoulos, Lampros Paschos, Mema Roussopoulos, Giorge Sotirelis, Panos Stathopoulos, Pavlos Vasilopoulos, Thomas Zacharias, Bingsheng Zhang, Fotis Zygoulis. *Electronic Voting Systems - From Theory to Implementation*. In e-Democracy, 2013.
12. Aggelos Kiayias, Stavros Papadopoulos, Nikos Triandopoulos, Thomas Zacharias. *Delegatable Pseudorandom Functions and Applications*. In CCS, 2013. Available in IACR Cryptology ePrint Archive, 2013:379, 2013.

## Scientific Interests

- Privacy-preserving technologies.
- Electronic voting.
- Formal modelling of security.

- Modelling human-computer interaction in secure multi-party protocols.
- End-to-end verifiable secure computation.

## Selected Oral Presentations

- *Communication Privacy on the Internet: the Current Status and Technical Challenges*. In e-Democracy, Workshop III: The present and the prospect of privacy-preserving technologies in Europe, December 2017.
- *Addressing the Challenges of e-Voting Through Crypto Design*. In Scotland's Democratic Future: Exploring Electronic Voting, November 2017.
- *MCMix: Anonymous Messaging via Secure Multiparty Computation* (joint talk with Nikolaos Alexopoulos). In USENIX Security Symposium, August 2017.
- *Ceremonies for End-to-end Verifiable Elections*. In PKC, Session: Real-World Schemes, March 2017.
- *Indistinguishable Proofs of Work or Knowledge*. In ASIACRYPT, Session: Cryptographic Protocol, December 2016.
- *The DEMOS e-Voting system and the Role of the Human Factor in End-to-end Verifiable Elections*. Invited talk at the University of Tartu, November 2016.
- *The DEMOS Family of e-Voting Systems: End-to-end Verifiable Elections in the Standard Model*. PhD defense, July 2016.
- *Motivating Voters to Active Participation: End-to-end Verifiability Without Trust Assumptions*. In e-Democracy, e-Voting Workshop, December 2015.
- *On the Necessity of Auditing for Election Privacy in e-Voting Systems*. In e-Democracy, Session: Privacy in e-voting, e-polls and e-surveys, December 2015.
- *The DEMOS e-Voting System* (in Greek). In INNOVATHENS, FINER project dissemination event, October 2015.
- *End-to-End Verifiable Elections in the Standard Model* (joint talk with Bingsheng Zhang). In EUROCRYPT, Session: Obfuscation and E-Voting, April 2015.
- *Pressing the Button for European Elections: Verifiable e-Voting and Public Attitudes Toward Internet Voting in Greece*. In EVOTE, Session: Electronic Voting in Polling Stations, October 2014.
- *Beyond Traditional Public Key Encryption: an Introduction to the Fine-grained Encryption Concept*. In e-Democracy, Workshop III, December 2013.
- *Delegatable Pseudorandom Functions and Applications*. In CCS, Session: Randomness, November 2013.

## Teaching

| | |
|---|---|
| Academic year 2016-2017, Fall Semester: | - Co-supervision of the visiting Master's student Tamara Finogina. |
| Academic year 2015-2016, Spring Semester: | - TA for *Mathematics of Computer Science* class (marking coursework). |

| | |
|---|---|
| Academic year 2015-2016,<br>Fall Semester: | - TA for *Cryptography* class<br>(tuition, marking coursework). |
| Academic year 2014-2015,<br>Spring Semester: | - TA for *Mathematics of Computer Science* class (marking coursework).<br>- Invited Lecture under the title<br>"*End-to-end verifiability in e-voting systems* "<br>for the Info Sec Lab of the Department of Information & Communication Systems Engineering of the University of the Aegean. |
| Academic year 2014-2015,<br>Fall Semester: | - TA for *Cryptography* class<br>(tuition, marking coursework).<br>- TA for *Discrete Mathematics* class<br>(tuition, marking coursework). |
| Academic year 2013-2014,<br>Fall Semester: | - TA for *Cryptography* class<br>(tuition, marking coursework).<br>- TA for *Discrete Mathematics* class<br>(tuition, marking coursework). |