ΕΘΝΙΚΟΝ & ΚΑΠΟΔΙΣΤΡΙΑΚΟΝ ΠΑΝΕΠΙΣΤΗΜΙΟΝ ΑΘΗΝΩΝ
NATIONAL & KAPODISTRIAN UNIVERSITY OF ATHENS

DEPARTMENT OF INFORMATICS & TELECOMMUNICATIONS

Aggelos Kiayias

Title: Assistant Professor in Cryptography and Security
Sector: Theoretical Computer Science
Phone: **+30 210 7275239 (office)**
Fax: **+30 210 7275333 (office)**
Email: aggelos@di.uoa.gr Web page: http://crypto.di.uoa.gr

Academic Qualifications:

- Ph.D.(2002) City U. of New York. USA. Thesis : "Polynomial Reconstruction Based Cryptography"
- M.Phil.(2001) City U. of New York. USA.
- B.Sc. in Mathematics (1996), University of Athens. Greece.

Appointments:

- July 2008 - today : Assistant Professor, Dpt. of Informatics & Telecom., University of Athens
- 2008 : Associate Professor with tenure, Department of Computer Science and Engineering, U. of Connecticut, USA.
- 2002 – 2008 : Assistant Professor, Department of Computer Science and Engineering, U. of Connecticut, USA.
- 2001 : International Association for Cryptologic Research. Graduate assistant.

Teaching Activities: (current)

Undergraduate courses

- Discrete Mathematics
- Cryptography
- Computer Security

Postgraduate courses

- Cryptography.

Supervisor of 3 Ph.D. dissertations

Research Interests/Activities: (last 10 years)

- Head of the CRYPTO.SEC Lab
- Cryptography for digital content.
- Privacy-preserving computation and digital signatures.
- Electronic voting systems. Co-founded Voting Technology Research Center that manages the security aspects of all elections at the state of Connecticut.
- Security in wireless networks.
- Formal modeling of security.
- Tamper resilient cryptographic systems.
- Coding theory.
- Security analysis networks and systems.

Scientific Publications/Citations:

- More than 70 publications in refereed venues including 8 Crypto & Eurocrypt papers and 8 journal papers.
- 4 Invited papers in international journals
- More than 1300 citations. (H-index 19)
- 2 US patents

Top five publications

- "Traceable Signatures" A. Kiayias, Y. Tsiounis and M. Yung, Eurocrypt 2004. pp. 571-589
- "Anonymous Identification in Ad-Hoc Groups", Y. Dodis, A. Nicolosi, A. Kiayias and V. Shoup, Eurocrypt 2004. pp. 609-626.
- "Pirate Evolution : how to make the most of your traitor keys" , A. Kiayias, S. Pehlivanoglu, CRYPTO 2007. pp. 448—465.
- Cryptographic Hardness based on the Decoding of Reed Solomon Codes, A. Kiayias, M. Yung, IEEE Transactions on Information Theory. Volume 54, No. 6, June 2008, pp. 2752—2769.
- "A Framework for the Sound Specification of Cryptographic Tasks", J. Garay, A. Kiayias, H.S. Zhou, CSF 2010. IEEE Computer Society 2010, pp. 277-289.

Distinctions:

- European Research Council, Starting grant. IDEAS program 2011-2016.
- Marie Curie Reintegration Grant 2011-2014.
- Public-Service Award by the Secretary of the State of Connecticut 2008.
- Outstanding faculty of the year 2006, U. of Connecticut SoE.
- NSF CAREER Award 2005.
- Fulbright Fellowship 1998-2002.
- University of Athens fellowship 1995-1996.

Other Activities:

- Program Chair CT-RSA 2011.
- Co-program chair RL-CPS 2010, ACM-DRM 2007, ACM-DRM 2004.
- Steering Committee ACM-DRM Workshop 2004-2011.
- 13 R&D projects
- Proposal evaluation for National Science Foundation, Microsoft Ph.D. scholarships, Hong-Kong Research Grants Council, MITACS - Canada, ANR France, Binational Israel US Foundation.
- Security consultant, OPAP, INTRALOT, State of Connecticut. State of New York Nassau County.
- More than 50 program committees