- AtheCrypt 2014 Program -

Athens Cryptography Day

Tuesday, January 7th 2014

* The talks and coffee breaks will take place at the Multimedia Amphitheater of the Central Library of NTUA.

9:00 – 9:15	*Registration*
9:15 – 10:00	**Rational Protocol Design: Cryptography Against Incentive-driven Adversaries** Vassilis Zikas (*University of California, Los Angeles*)
10:00 – 10:05	*Break*
10:05 – 10:35	**A New Constant Round ID-based Group Key Agreement Protocol** Elisavet Konstantinou (*University of the Aegean*)
10:35 – 10:40	*Break*
10:40 – 11:25	**Efficient Verifiable Set Operations over Outsourced Databases** Dimitris Papadopoulos (*Boston University*)
11:25 – 11:40	*Break*
11:40 – 12:25	**Oblivious RAM: state of the art and new constructions** Panagiotis Rizomiliotis (*University of the Aegean*)
12:25 – 12:30	*Break*
12:30 – 13:15	**A Survey of Group-based Cryptography** Dimitris Panagopoulos (*University of Athens*)
13:15 – 13:20	*Break*
13:20 – 14:05	**Non-interactive zero-knowledge shuffle arguments** Bingsheng Zhang (*University of Tartu*)
14:05 – 15:10	*Lunch Break*
15:10 – 15:55	**Delegatable Pseudorandom Functions and Applications** Thomas Zacharias (*University of Athens*)
15:55 – 16:05	*Break*
16:05 – 16:50	**Code-Based Public-Key Cryptosystems: Constructions and Attacks** Nicholas Kolokotronis (*University of Peloponnese*)
16:50 – 17:05	*Break*
17:05 – 17:50	**Cryptographic properties of Boolean functions: recent developments and open problems** Konstantinos Limniotis (*University of Athens*)
17:50 – 17:55	*Break*
17:55 – 18:40	**Coin Flipping of Any Constant Bias Implies One-Way Functions** Aris Tentes (*New York University*)
18:40	*End*