AtheCrypt 2013 – National Technical University of Athens

Athens Cryptography Day

– Program –

The talks and coffee breaks will take place at the Multimedia Amphitheater of the Central Library of National Technical University of Athens.

Monday, January 7	
08:30 – 09:00	Registration
08:55	Opening and Welcome
09:15 – 10:15	Secure Multiparty Computation via Hidden Subsets Aggelos Kiayias (University of Athens, University of Connecticut)
10:15 – 11:00	Pseudorandom Knapsacks and the Sample Complexity of LWE Search-to-Decision Reductions Petros Mol (University of California, San Diego)
11:00 – 11:15	Coffee Break
11:15 – 12:00	Secure Broadcast in generic and wireless networks Dimitris Sakavalas (National Technical University of Athens)
12:00 – 12:45	The Learning Parity with Noise assumption and applications Aris Tentes (New York University)
12:45 – 13:00	Coffee Break
13:00 – 13:45	Super-Efficient and Parallelizable Authenticated Pattern Matching and XML Search Dimitris Papadopoulos (Boston University)
13:45 – 15:30	Lunch Break
15:30 – 16:15	Proofs of Secure Erasure Nikos Karvelas (Darmstadt University of Technology)
16:15 – 17:00	Anonymous Credentials Light Foteini Baldimtsi (Brown University)
17:00 – 17:05	Coffee Break
17:05 – 17:50	Universally Composable Synchronous Computation Vassilis Zikas (University of California, Los Angeles)