

# - AtheCrypt 2016 Program -

*Athens Cryptography Day*

Monday, January 11<sup>th</sup> 2016

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

9:30 – 10:00	<i>Registration - Opening</i>
10:00 – 10:45	<b>Online Template Attacks on Elliptic Curves</b> Louiza Papachristodoulou, <i>iCIS, RU Nijmegen</i>
10:45 – 11:30	<b>Non-malleable codes in the split-state model</b> Yiannis Tselekounis, <i>University of Athens</i>
11:30 – 12:00	<i>Break</i>
12:00 – 12:45	<b>The importance of the human factor in the security of voting protocols</b> Thomas Zacharias, <i>University of Athens</i>
12:45 – 14:00	<i>Lunch Break</i>
14:00 – 15:00	<b>Fair and Robust Multi-Party Computation using a Global Transaction Ledger</b> Aggelos Kiayias, <i>University of Athens</i>
15:00 – 15:10	<i>Break</i>
15:10 – 15:55	<b>Monero: An untraceable unlinkable bitcoin alternative</b> Dionysis Zindros, <i>National Technical University of Athens</i>
15:55 – 16:05	<i>Break</i>
16:05 – 17:00	<b>Probabilistic attacks against compressed encrypted protocols</b> Dimitris Karakostas, <i>National Technical University of Athens</i>
17:10	<i>End</i>