

List of projects

Fall 2014/15

Name	Topic	Supervisor	Presentation date	Prelim. report	Peer reviews	Final report
Märt Bakhoff	EMV (chip & PIN) protocol	Arnis Parsovs	10 Nov.	24 Nov.	8 Dec.	15 Dec.
Riivo Talviste	Attack-tree based risk analysis of i-voting	Sven Heiberg & Jan Willemsen	10 Nov.	24 Nov.	8 Dec.	15 Dec.
Annabell Kuldmaa	Biclique	Faruk Göloğlu	17 Nov.	24 Nov.	8 Dec.	15 Dec.
Ivo Kubjas	Discrete logarithm problem	Faruk Göloğlu	17 Nov.	24 Nov.	8 Dec.	15 Dec.
Kristiina Rahkema	Quantum position verification in the random oracle model	Dominique Unruh	24 Nov.	24 Nov.	8 Dec.	15 Dec.
Francesco Di Ciccio	Comparison of security measures against identity theft in various countries	Vitaly Skachek	24 Nov.	24 Nov.	8 Dec.	15 Dec.
Sander Siim	Implementation of PRAM algorithms on Sharemind	Peeter Laud	1 Dec.	24 Nov.	8 Dec.	15 Dec.
Sushanta Paudyal	Study of code locality	Vitaly Skachek	1 Dec.	24 Nov.	8 Dec.	15 Dec.
Prastudy Fauzi	Indistinguishability obfuscation, part I	Dominique Unruh	8 Dec.	24 Nov.	8 Dec.	15 Dec.
Pille Pullonen	Indistinguishability obfuscation, part II	Dominique Unruh	8 Dec.	24 Nov.	8 Dec.	15 Dec.
Dmitri Gabbasov	From simple keylogger to advanced logging	Rafik Chaabouni	15 Dec	24 Nov.	8 Dec.	15 Dec.
Kristjan Krips	Security of symmetric encryption against mass surveillance	Dominique Unruh	15 Dec.	24 Nov.	8 Dec.	15 Dec.