MTAT.07.022: Research Seminar in Cryptography **University of Tartu**

List of projects

Spring 2014

Name	Topic	Supervisor	Presentation date	Prelim. report	Peer reviews	Final report
Valdur Kadakas	Small-scale electronic elections	Jan Willemson	22 Apr.	22 Apr.	6 May	27 May
Ehsan Ebrahimi Targhi	Index coding	Vitaly Skachek	22 Apr.	22 Apr.	6 May	27 May
Riivo Talviste	Careful with composition: limitations of the indifferentiability framework	Dominique Unruh	29 Apr.	29 Apr.	13 May	27 May
Kairi Kangro	Efficient (quasi-adaptive) non-interactive zero knowledge	Helger Lipmaa	29 Apr.	29 Apr.	13 May	27 May
Ivo Kubjas	Computationally efficient mixnets for electronic voting	Helger Lipmaa	29 Apr.	29 Apr.	13 May	27 May
Mayuresh Anand	Batch codes	Vitaly Skachek	6 May	6 May	20 May	27 May
Tiit Pikma	Refinement types for secure implementations	Dominique Unruh	6 May	6 May	20 May	27 May
Pille Pullonen	Wiretap channel II	Vitaly Skachek	13 May	6 May	20 May	27 May
Reem Bayomi	Security measures against credit card frauds	Vitaly Skachek	13 May	6 May	20 May	27 May
Yauhen Yakimenka	Implementing transformations based on discrete logarithm for ProveIt	Kristjan Krips & Sven Laur	20 May	6 May	20 May	27 May
Siddharth Rao	How to make Bitcoin a better currency	Vitaly Skachek	20 May	6 May	20 May	27 May
Arnis Paršovs	Identity card key generation in the malicious card issuer model	Jan Willemson	27 May	6 May	20 May	27 May
Sushanta Paudyal	Everlasting multi-party computation	Dominique Unruh	27 May	6 May	20 May	27 May
Sevil Güler	Mobile app for secure multiparty computation	Riivo Talviste & Sven Laur	27 May	6 May	20 May	27 May