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

List of projects

Fall 2015-2016

Name	Topic	Supervisor	Presentation date	Prelim. report	Peer reviews	Final report
Ehsan Ebrahimi Targhi	Information-theoretic PIR with low storage overhead	Helger Lipmaa & Vitaly Skachek	24 Nov.	24 Nov.	8 Dec.	15 Dec.
Sander Siim	The simplest protocol for oblivious transfer	Pille Pullonen	24 Nov.	24 Nov.	8 Dec.	15 Dec.
Sergio Andrés Figueroa Santos	Incoercible e-voting	Helger Lipmaa	1 Dec.	24 Nov.	8 Dec.	15 Dec.
Janno Siim	Efficient shuffle arguments	Helger Lipmaa	1 Dec.	24 Nov.	8 Dec.	15 Dec.
Dmitri Gabbasov	Password-based encryption in ZIP files	Arnis Parsovs	8 Dec.	24 Nov.	8 Dec.	15 Dec.
Yauhen Yakimenka	Password-based encryption in PDF files	Arnis Parsovs	8 Dec.	24 Nov.	8 Dec.	15 Dec.
Suela Kodra	Protocol verification with Proverif	Dominique Unruh	15 Dec.	24 Nov.	8 Dec.	15 Dec.
Annabell Kuldmaa	Comparison of quantum-proof anonymous key exchange protocols	Ahto Truu	15 Dec.	24 Nov.	8 Dec.	15 Dec.
Cesar Pereida Garcia	Literature overview about active security in garbled circuits	Pille Pullonen	15 Dec.	24 Nov.	8 Dec.	15 Dec.