

MTAT.07.022: Research Seminar in Cryptography

List of projects

Fall 2019-2020

Name	Supervisor	Topic	Present- ation	Prelim. report	Peer reviews	Final report
Abasi-Amefon Obot Affia	Danielle Morgan	Assessing the unlock mechanism of Tartu Bike Share	29 Nov	29 Nov	9 Dec	20 Dec
Shiting Long	Vitaly Skachek	Security of authentication protocols in 5G	6 Dec	29 Nov	9 Dec	20 Dec
Eric Cornelissen	Sven Laur	Formal verification of attack simplification lemmas	6 Dec	29 Nov	9 Dec	20 Dec
Mattias Lass	Danielle Morgan	Security of WiFi networks	13 Dec	29 Nov	9 Dec	20 Dec
Valeh Fazaliev	Vitaly Skachek	NIST quantum competition - second round	13 Dec	29 Nov	9 Dec	20 Dec
Risto Pärnapuu	Ahto Truu	Survey of homomorphic properties of secret sharing schemes	20 Dec	29 Nov	9 Dec	20 Dec
Kristiina Konno	Ahto Truu	Unlinkable attribute-based credentials	20 Dec	29 Nov	9 Dec	20 Dec