Pielikums Nr.1
pie kārtības Nr. 1-2021/RTUAF-2021/15
whiteCryption SIA noslēguma darbu stipendiju piešķiršanai

whiteCryption SIA noslēguma darba stipendiju konkursa pieteikuma darba tēmas

Nr.p.k.	Temats
1.	ARM TrustZone izmantošana datorprogrammu pretkopēšanas aizsardzībai https://www.arm.com/products/security-on-arm/trustzone
2.	Datu un ar tiem veicamo operāciju maskēšana (aizsardzība pret novērošanu un analīzi) pilnīgi atklātā programmas izpildīšanās vidē (white-box environment) http://www.whiteboxcrypto.com/
3.	Pilnībā homomorfiskas šifrēšanas implementācija ar piemēriem https://en.wikipedia.org/wiki/Homomorphic_encryption https://crypto.stanford.edu/craig/easy-fhe.pdf https://crypto.stanford.edu/craig/craig-thesis.pdf https://eprint.iacr.org/2015/1192.pdf https://tfhe.github.io/tfhe/ https://github.com/google/fully-homomorphic-encryption
4.	Pētījums par specializēto Intel procesora instrukciju izmantošanu kriptogrāfisko algoritmu paātrināšanai https://en.wikipedia.org/wiki/CLMUL_instruction_set http://www.intel.co.kr/content/dam/www/public/us/en/documents/whitepapers/polynomial-multiplication-instructions-paper.pdf https://eprint.iacr.org/2011/589.pdf
5.	Pētījums par uz režģiem balstītām kriptosistēmām https://en.wikipedia.org/wiki/Lattice-based_cryptography
6.	Pētījums par jaunākajiem bloku algoritmu šifrēšanas režīmiem uz diska glabātu datu aizsardzībai https://en.wikipedia.org/wiki/Disk_encryption_theory
7.	Uz TPM (Trusted Platform Module) balstīta platformas apstiprināšana un droša sāknēšana http://www.trustedcomputinggroup.org/trusted-platform-module-tpmsummary/
8.	Koda integritātes nodrošināšana JavaScript programmās
9.	Koda integritātes pārbaude, kas pieļauj Intel PIN rīku lietošanu
10.	Pārskats par pieejamo aparatūras atbalstu drošai skaitļošanai (ARM TrustZone, TPM, Rambus CryptoManager, Intel TXT/SGX/AMT u.c.) https://www.arm.com/products/security-on-arm/trustzone http://www.trustedcomputinggroup.org/trusted-platform-module-tpmsummary https://www.rambus.com/security/cryptomanager-platform https://software.intel.com/en-us/articles/intel-trusted-execution-technology-aprimer_ https://en.wikipedia.org/wiki/Intel_Active_Management_Technology
11.	Cita konkrēta, ar SIA „whiteCryption" saskaņota pētniecības tēma, kas iekļaujas kādā no zemāk minētajiem tematiem: 1. Klasiskā kriptogrāfija (simetriskās un publiskās atslēgas algoritmi, kopīgas atslēgas izveidošanas protokoli, digitālie paraksti, utml.); 2. "Baltās kastes" (white-box) kriptogrāfija; 3. Programmas koda un datu integritātes pārbaude un nodrošināšana; 4. Programmas koda obfuskācija (obfuscation); 5. Pretkopēšanas aizsardzība; 6. Nodevēju izsekošana (traitor tracing); 7. Digitālā satura tiesību pārvaldība (digital rights management); 8. Būla ķēžu obfuskācija; 9. Cita ar datu vai programmatūras drošību saistīta tēma.