Pielikums Nr.1
SIA „whiteCryption" pētniecības darbu stipendijai

**SIA „whiteCryption" pētniecības darbu stipendiju konkursa pieteikuma darba tēmu virzieni saskaņā ar stipendiju konkursa kārtību**

1. ARM TrustZone izmantošana datorprogrammu pretkopēšanas aizsardzībai;
   1.1. 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);
   2.1. http://www.whiteboxcrypto.com/
3. Pilnībā homomorfiskas šifrēšanas implementācija ar piemēriem;
   3.1. https://en.wikipedia.org/wiki/Homomorphic_encryption
   3.2. https://crypto.stanford.edu/craig/easy-fhe.pdf
   3.3. https://crypto.stanford.edu/craig/craig-thesis.pdf
   3.4. https://eprint.iacr.org/2015/1192.pdf
4. Pētījums par specializēto Intel procesora instrukciju izmantošanu kriptogrāfisko algoritmu paātrināšanai;
   4.1. https://en.wikipedia.org/wiki/CLMUL_instruction_set
   4.2. http://www.intel.co.kr/content/dam/www/public/us/en/documents/white-papers/polynomial-multiplication-instructions-paper.pdf
   4.3. https://eprint.iacr.org/2011/589.pdf
5. Pētījums par uz režģiem balstītām kriptosistēmām;
   5.1. https://en.wikipedia.org/wiki/Lattice-based_cryptography
6. Pētījums par jaunākajiem bloku algoritmu šifrēšanas režīmiem uz diska glabātu datu aizsardzībai;
   6.1. https://en.wikipedia.org/wiki/Disk_encryption_theory
7. Uz TPM (Trusted Platform Module) balstīta platformas apstiprināšana un droša sāknēšana;
   7.1. http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/
8. Koda integritātes nodrošināšana JavaScript programmās;
9. Koda integritātes pārbaude, kas pieļauj Intel PIN rīku lietošanu;
10. Kriptogrāfisku atslēgu aizsardzība TLS bibliotēkā;
    10.1. https://tools.ietf.org/html/rfc5246
11. WEB Cryptography API realizācijas prototips;
    11.1. https://www.w3.org/TR/WebCryptoAPI/
12. Pārskats par pieejamo aparatūras atbalstu drošai skaitļošanai (ARM TrustZone, TPM, Rambus CryptoManager, Intel TXT/SGX/AMT u.c.);
    12.1. https://www.arm.com/products/security-on-arm/trustzone
    12.2. http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/

12.3. https://www.rambus.com/security/cryptomanager-platform/
12.4. https://software.intel.com/en-us/articles/intel-trusted-execution-technology-a-primer
12.5. https://en.wikipedia.org/wiki/Intel_Active_Management_Technology

13. Mašīnu apmācības (https://en.wikipedia.org/wiki/Machine_learning) pielietojums programmu obfuskācijai - https://en.wikipedia.org/wiki/Obfuscation(software))
14. Mašīnu apmācības pielietojums programmu deobfuskācijai - (deobfuscation) un deobfuskācijas grūtības novērtēšanai.
15. Cita konkrēta, ar SIA whiteCryption saskaņota pētniecības tēma, kas iekļaujas kādā no zemāk minētajiem tematiem:
    15.1. Klasiskā kriptogrāfija (simetriskās un publiskās atslēgas algoritmi, kopīgas atslēgas izveidošanas protokoli, digitālie paraksti, utml.);
    15.2. "Baltās kastes" (white box) kriptogrāfija;
    15.3. Programmas koda un datu integritātes pārbaude un nodrošināšana;
    15.4. Programmas koda obfuskācija (obfuscation);
    15.5. Pretkopēšanas aizsardzība;
    15.6. Nodevēju izsekošana (traitor tracing);
    15.7. Digitālā satura tiesību pārvaldība (digital rights management).