**National Research Nuclear University MEPhI**

**(Moscow Engineering Physics Institute)**

**Department of Cryptology and Cybersecurity**

**(№ 42)**

**LIST OF PAPERS**

|  |
| --- |
| **Name: V.A. Afonin** |
|  |
| **English Teacher: E.V. Aleshinskaya** |

**Moscow**

**2024**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Author(s). Title. Source, year of publication** | **Amount of characters** | **Form of assessment** | **Mark** | **Signature** |
| 1. | Shafi Goldwasser et al. The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, 1989 | 78000 | Retelling (with Elements of Analysis) |  |  |
| 2. | Ariel Gabizon et al. PLONK: Permutations over Lagrange-bases for Oecumenical Noninteractive arguments of Knowledge. *Cryptology ePrint Archive*, 2019 | 67000 |
| 3. | Tomer Ashur and Al Kindi. Arithmetization Oriented Encryption. *Cryptology ePrint Archive*, 2023 | 12000 | Vocabulary Study |  |  |
| 4. | Mingjie Chen et al. Malleable Commitments from Group Actions and Zero-Knowledge Proofs for Circuits based on Isogenies. *Cryptology ePrint Archive*, 2023 | 71000 |
| 5. | Alessandro Chiesa et al. On Parallel Repetition of PCPs. *Cryptology ePrint Archive*, 2023 | 128000 |
| 6. | Claudia Bartoli and Ignacio Cascudo. On Sigma-Protocols and (packed) Black-Box Secret Sharing Schemes. *Cryptology ePrint Archive*, 2023 | 103000 |
| 7. | Yuncong Zhang et al. Polynomial IOPs for Memory Consistency Checks in Zero-Knowledge Virtual Machines. *Cryptology ePrint Archive*, 2023 | 111000 |
| 8. | Michael Rosenberg et al. zk-creds: Flexible Anonymous Credentials from zkSNARKs and Existing Identity Infrastructure. *Cryptology ePrint Archive*, 2022 | 141000 | Grammar Study |  |  |
| 9. | **(same as 5)** Alessandro Chiesa et al. On Parallel Repetition of PCPs. Cryptology ePrint Archive, 2023 | 128000 |
| 10. | Sanjam Garg et al. How to Prove Statements Obliviously? Cryptology ePrint Archive, 2023 | 169000 |
| 11. | Alex Evans. Succinct Proofs and Linear Algebra. Cryptology ePrint Archive, 2023 | 95000 |
| 12. | Benedikt Bunz. Protostar: Generic Efficient Accumulation/Folding for Special-sound Protocols. Cryptology ePrint Archive, 2023 | 116000 |
| 13. | Xing Z. et al. Zero-knowledge Proof Meets Machine Learning in Verifiability: A Survey. *arXiv preprint arXiv:2310.14848*, 2023 | 136000 | Literature Review |  |  |
| 14. | Goldwasser S. et al. Delegating Computation: Interactive Proofs for Muggles. *ACM Symposium on Theory of Computing, 113–122*, 2008 | 61000 |
| 15. | Thaler J. A Note on the GKR Protocol. URL: <https://people.cs.georgetown.edu/jthaler/GKRNote.pdf>, 2015 | 14000 |
| 16. | Valiant P. Incrementally Verifiable Computation or Proofs of Knowledge Imply Time/Space Efficiency. *Canetti, R. (eds) Theory of Cryptography, TCC 2008, Lecture Notes in Computer Science, vol 4948, 1–18*, 2008 | 48000 |
| 17. | Chisea A. & Tromer E. Proof-Carrying Data and Hearsay Arguments from Signature Cards. *Proceedings of the Symposium on Innovations in Computer Science, 310–331*, 2010 | 100000 |
| 18. | Ghodsi Z. et al. SafetyNets: verifiable execution of deep neural networks on an untrusted cloud. *NIPS'17: Proceedings of the 31st International Conference on Neural Information Processing Systems, 4675–4684*, 2017 | 37000 |
| 19. | Kang D. et al. Scaling up Trustless DNN Inference with Zero-Knowledge Proofs. *arXiv preprint arXiv:2210.08674*, 2024 | 54000 |
| 20. | Hengrui J. et al. Proof-of-Learning: Definitions and Practice. *2021 IEEE Symposium on Security and Privacy (SP), 1039–1056*, 2021 | 106000 |
| 21. | Abbaszadeh K. et al. Zero-Knowledge Proofs of Training for Deep Neural Networks. *Cryptology ePrint Archive*, 2024 | 127000 |
| 22. | Lingchen Zhao et al. VeriML: Enabling Integrity Assurances and Fair Payments for Machine Learning as a Service. *IEEE Transactions on Parallel and Distributed Systems, Vol. 32, No. 10, 2524–2540*, 2021 | 100000 | Introduction |  |  |
| 23. | Sanjam Garg et al. Experimenting with Zero-Knowledge Proofs of Training. *In Proceedings of the CCS '23: ACM SIGSAC Conference on Computer and Communications Security, 1880–1894*, 2023 | 143000 |
| 24. | Jiaheng Zhang et al. Zero Knowledge Proofs for Decision Tree Predictions and Accuracy. *In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS ’20). 2039–2053*, 2020 | 87000 |
| 25. |  |  | Presentation |  |  |
| 26. |  |  |

**Total: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ characters**

**Tests: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Academic Essay: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Conference Abstract: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Bonus points: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Overall Mark: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Signature: \_\_\_\_\_\_\_\_\_\_\_\_/Aleshinskaya E.V./**