Kudinov Mikhail

mishel.kudinov@gmail.com
mishel-kudinov@mail.ru
+31619876096
+79165754166
Telegram: @error024

WORK EXPERIENCE

RUSSIAN QUANTUM CENTER, *Research fellow* Oct 2018 - March 2022

My duties included research in the area of cryptography, especially post-quantum cryptography; consulting for the development team; preparation of conference talks and publications; give conference talks.

EINDHOVEN UNIVERSITY OF TECHNOLOGY, *PhD student* Jul 2021 - present

I am doing research in post-quantum cryptography, provable security. The aim of my current project is to give a proper proof of SPHINCS+ - post-quantum signature algorithm. The supervisor is Andreas Hülsing.

EDUCATION

SPECIALIST IN COMPUTER SECURITY Sep 2015 - Jul 2021

Bauman Moscow state technical university

The specialist degree is considered equivalent to a Masters degree with regard to the admission to PhD programs in Russia. The topic of the final thesis - "Development of an encryption algorithm based on attributes using pseudorandom functions". The supervisor is Chilikov Alexey.

HONORS AND AWARDS

2017 - MIEM Start CTF	Prize-Winner
2019 - International Olympiad in Cryptography, NSUCRYPTO	First place in the individual stage. First place in the group stage.
2020 - International Olympiad in Cryptography, NSUCRYPTO	Second place in the individual stage. First place in the group stage.
2021 - International Olympiad in Cryptography, NSUCRYPTO	First place in the group stage.

PUBLICATIONS

1. E.O. Kiktenko, **M.A. Kudinov** , A.K. Fedorov. Detecting Brute-Force Attacks on Cryptocurrency Wallets. Business Information Systems Workshops. BIS 2019. Lecture Notes in Business Information Processing, vol 373 (2019). https://doi.org/10.1007/978-3-030-36691-9_20

2. **M.A. Kudinov** , A.A. Chilikov, E.O. Kiktenko, and A.K. Fedorov. Advanced attribute-based encryption protocol based on the modified secret sharing scheme. J Comput Virol Hack Tech 16, 333–341 (2020). https://doi.org/10.1007/s11416-020-00366-8

3. E.O. Kiktenko, **M.A. Kudinov**, A.A. Bulychev, A.K. Fedorov. Proof-of-forgery for hash-based signatures, Proceedings of the 18th International Conference on Security and Cryptography (2021). https://doi.org/10.5220/0010579603330342

4. **M.A. Kudinov**, E. O. Kiktenko, A. K. Fedorov. Security analysis of the W-OTS+ signature scheme: Updating security bounds (2020), Mat. Vopr. Kriptogr. 12, 129 (2021). https://doi.org/10.4213/mvk362

5. S.E. Yunakovsky, M. Kot, N. Pozhar, D. Nabokov, **M. Kudinov**, A. Guglya, E.O. Kiktenko, E. Kolycheva, A. Borisov and A. K. Fedorov, Towards security recommendations for public-key infrastructures for production environments in the post-quantum era (2021), EPJ Quantum Technol. (2021). https://doi.org/10.1140/epjqt/s40507-021-00104-z

PREPRINTS

1. A. Hülsing, **M. Kudinov**. Recovering the tight security proof of SPHINCS$^+$. Cryptology ePrint Archive, Paper 2022/346 (2022). https://eprint.iacr.org/2022/346

REVIEWS

1. Journal of Cryptology 2022 - Reviewer
2. PQCrypto 2022 - Subreviewer
3. SAC 2022 - Subreviewer

SKILLS

Native Speaker	SageMath experience.
Advanced level	Python experience.
Intermediate level	C/C++ experience.

AREAS OF INTEREST

- Post-quantum cryptography
- Provable Security
- Hash-based signatures
- Quantum computations
- Quantum Random Oracles
- Attribute based encryption
- Elliptic curves cryptography
- Blockchain
- Smart Contracts