Cryptanalyst **Jun. 2022 - Present**
Technology Innovation Institute *Abu Dhabi, UAE*
The following publications were obtained as a result of research:

- *Karenin, A., Kirshanova, E.* (2024, July). Finding dense submodules with algebraic lattice reduction. In International Conference on Cryptology in Africa (pp. 403-427). Cham: Springer Nature Switzerland. Available at https://eprint.iacr.org/2024/844.pdf
- *Hanyecz, O., Karenin, A., Kirshanova, E., Kutas, P., Schaeffler, S.* (2025). Constant time lattice reduction in dimension 4 with application to SQIsign. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(2), 511-534. Available at https://eprint.iacr.org/2025/027.pdf
- *Karenin, A., Kirshanova, E., May, A., Nowakowski, J.* Fast Slicer for Batch-CVP: Making Lattice Hybrid Attacks Practical. To appear in Proceedings of the 2025 Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2025).

Talks
- Finding Dense Submodules with Algebraic Lattice Reduction (Jul. 2024). AFRICACRYPT 2024, Douala, Cameroon.
- Finding Dense Submodules with Algebraic Lattice Reduction (2024). CHARM Web Seminar. Slides available at https://github.com/alexgit256/personal_talks_kas/blob/main/CHARM/CHARM_2024_talk.pdf
- Constant time lattice reduction in dimension 4 with application to SQIsign. (Sep. 2025). CHES 2025, Kuala Lumpur, Malaysia. Slides available at https://iacr.org/submit/files/slides/2025/tches/tches2025/2_72/2_72_slides.pdf