Agha Aghayev

GitHub | LinkedIn | Email
Mobile:+994555231317

Research Experience

Master's Thesis – *Lattice-based Identity-based encryption: Foundations, Constructions, and Implementation* under supervision of Prof. Arkady Yerukhimovich
George Washington University, Washington DC
Sep. 2024 – Apr. 2025

- Adressing key authenticity problem via Identity-based encryption (IBE)
- Exploring quantum-proof cryptographic tools: the foundations of lattice problems, hardness assumptions, reductions, and lattice-based cryptographic schemes
- Building secure Gadget-based and traditional lattice-trapdoors for preimage sampling of identity vectors
- Developing prototype tools for lattice-based IBE systems

Publications

1. Agha Aghayev. Implementation of Lattice Trapdoors for Quantum-proof Identity-based Encryption, PCI 2025.
2. Agha Aghayev and Yadigar Imamverdiyev. Privacy-preserving Shape Matching with Leveled Homomorphic encryption (Submitted to AICT 2025, under review)
3. (Ongoing work) Agha Aghayev and Nour-eddine Rahmani. Cryptanalysis of a Post-Quantum Signature Scheme Based on Number-Theoretic Assumptions (**Manuscript in preparation**)

Projects

Lattice-based trapdoor sampling

- Working as a part of my master's thesis, I am developing tools for secure trapdoor sampling functions
- Implementation of Discrete Gaussian sampling for the GPV scheme with full-rank bases
- Implementation of Gadget-based trapdoor sampling with offline perturbation sampling
- Built quantum-resistant public key encryption, such as Dual-Regev scheme.

Privacy-Preserving Shape matching with OpenFHE

- Utilized leveled CKKS scheme for secure shape matching
- Approximation of non-linear functions with Chebyshev's interpolation method

Protocols and attacks on Lattice-Based Cryptography

- Implemented LLL basis reduction attacks to attack classic cryptographic systems such as knapsack and GGH cryptosystems
- Developed cryptographic protocols based on lattice-based hard problems such as LWE, enabling post-quantum security

Education

Master of Science in Computer Science and Data Analytics
GWU, Washington DC, United States (3.79 / 4) / ADAU, Baku, Azerbaijan (3.81 / 4)
Sep. 2023 – Jun. 2025
Relevant Course: Cryptography by Prof. Yerukhimovich
Bachelors Degree in Computer Science (Diploma of Honours) - GPA : 92.83/100
ASOIU, Baku, Azerbaijan
Sep. 2019 – Jul. 2023

Industry Experience

Junior Machine Learning Engineer – Development and Research Team
Baku, Azerbaijan
Feb. 2023 – Jul. 2024

- Researched and implemented machine learning techniques for satellite imagery analysis, with a focus on applications in smart agriculture
- Developed and trained models for satellite imagery data using PyTorch, focusing on water detection, quality assessment, and volume estimation

Technical Skills

Languages: C++, Python, Java, Haskell, LaTeX, HTML and CSS (basic)
Developer Tools: Git, Linux, Docker
Frameworks: OpenFHE, SageMath(basic), Tenseal, PyTorch, Spring