Agha Aghayev

aghayevagha.github.io | aghayevagha | LinkedIn | email| scholar

Experience

Research Assistant *May 2025 – Present*
Azerbaijan Technical University, Baku, Azerbaijan
Supervisor: Dr. Yadigar Imamverdiyev

- Assisting in research projects focused on cryptography.

Adjunct Instructor *September 2025 – Present*
Baku Higher Oil school, Baku, Azerbaijan
Courses

- Advanced Cryptography and Data Protection (graduate level)
- Discrete Mathematics (undergraduate level)

Junior Machine Learning Engineer *Dec 2023 – July 2024*
PRODATA

- Smart agriculture solutions for satellite imagery using machine learning.
- Implemented algorithms for water detection and volume estimation.

Publications

1. **Agha Aghayev**. Implementation of Lattice Trapdoors for Quantum-proof Identity-based Encryption, (accepted to PCI 2025 conference).
2. **Agha Aghayev** and Yadigar Imamverdiyev. Privacy-preserving Shape Matching with Leveled Homomorphic Encryption (Preprint)
3. **Agha Aghayev** and Nour-eddine Rahmani. Cryptanalysis of a Post-Quantum Signature Scheme Based on Number-Theoretic Assumptions (Preprint)

Projects

Lattice-based trapdoor sampling

- Implementation of Discrete Gaussian sampling for the GPV scheme with full-rank bases and Gadget-based trapdoors (with 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

Grobner basis attacks on multiple-key NTRU problem(ongoing)

- Arora-Ge modeling for converting NTRU learning instances to error-free multi-variable polynomial system of equations
- Solving system with Grobner basis computation and investigating speed-ups

Education

MS in Computer Science and Data Analytics (Diploma of Honors)
GWU, Washington DC, United States (3.79 / 4) / ADAU, Baku, Azerbaijan (3.81 / 4).
Sep. 2023 – Jun. 2025
Thesis: *Lattice-based Identity-based encryption: Foundations, Constructions, and Implementation* under supervision of Prof. Arkady Yerukhimovich

BS in Computer Science (Diploma of Honors) - GPA : 92.83/100
ASOIU, Baku, Azerbaijan.
Sep. 2019 – Jul. 2023

Technical Skills

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