Parsa Tasbihgou

Email: parsa.tasbihgou@epfl.ch
Phone: +41 767895180

Education

- **Ecole Polytechnique Federale de Lausanne (EPFL)** — Lausanne, Switzerland
  MSc - Computer Science; GPA:5.3/6 — *September 2023 - Now*
- **University of Tehran** — Tehran, Iran
  BSc - Computer Science; GPA:18.3/20 — *September 2019 - August 2023*

Research Interests

- **Cryptography, Isogeny-based cryptography, Lattice-based cryptography**
- **Probabilistic proofs, Zero-knowledge proofs**
- **Algebra, Number theory**
- **Graph theory, Combinatorics**

Selected Courses

- **Master @ EPFL**
  - **Foundations of Probabilistic Proofs - Chiesa**
  - **Cryptography and security - Vaudenay**
  - **Advanced cryptography - Vaudenay**
  - **Integer optimization - Eisenbrand**
  - **Number theory in cryptography - Jetchev**
- **Bachelor @ University Of Tehran**
  - **Topics in Cryptology**
  - **Introduciton to Cryptography**
  - **Number Theory**
  - **Algebra I**
  - **Algorithm Design and Analysis**

Research Experience

- **Internship at COSIC, KU Leuven**
  Supervisor: Dr. Wouter Castryck — *July-September 2024*

I visited the isogeny group at the COSIC lab in KU Leuven and I was hosted by Wouter Castryck. During my stay there I studied a variety of problems including: Finding isogenies between ordinary elliptic curves with large prime conductor gap, more generally walking up in a volcano (ordinary or oriented supersingular). Using more efficient orientations to construct class group actions similar to ScallopHD. Quantum secure VDFs. Quantum complexity of finding large prime degree isogenies between oriented elliptic curves. Structure of the isogeny graph of non-simple ordinary abelian surfaces. I am working on a note covering my activities in Leuven. It will be published once its ready.

Selected Projects

- **Isogeny-based time-release cryptography**
  Supervisor: Dr. Boris Fouotsa — *June 2024*

In this project I studied time-release cryptographic primitives and instantiations based on isogeny of supersingular elliptic curves. I looked at the verifiable delay function proposed by De Feo et al. based on chains of low degree isogenies and pairings and delay encryption introduced by De Feo and Burdges based on the same VDF. I also looked at two quantum-secure VDFs, one based on high degree rational isogenies and Kani's criterion, the other based on the CGL hash function and SNARGs.
To further my view on this field I also looked at some constructions based on squaring in groups of unknown order.

- **Supersingular Elliptic Curves in Cryptography** — Bachelor project
  Superviser: Prof. Shahram Khazaei — *2023*

In this project I studied the elliptic curves and their isogenies and how these are used in cryptography. I studied the SIDH protocol as a basic key exchange protocol based on isogenies. Additionaly I looked at some of the attacks on SIDH and how they leverage the knowledge of torsion points. I also looked at a zero-knowledge proofs for the weak-SIDH relation and observed how the attacks on SIDH don't apply because no torsion information is revealed.

Awards and Honors

- **Third prize in the International Mathematics Competition (IMC) - 2022**
- **Bronze medal in the National Mathematics Competition for university students - 2022**
- **Top 10 teams in University Of Tehran's ICPC - 2019 & 2022**
- **University of Tehran's representative in national ACM-ICPC - 2019**
- **Participation in National Olympiads in Informatics - 2017**

Presentations

- **IOPP for algebraic geometry codes**: This presentation was a part of the project for the course "Foundations of Probabilistic proofs" by Alessandro Chiesa. We studied and presented a paper with the same title by Bordage, Lhotel, Nardi and Randriam. This paper extends the ideas from the FRI protocol for the Reed-Solomon codes to create a proof of proximity to AG codes. In addition to preseting some parts of the paper, we also gave a brief background on the algebraic geometry knowledge required to understand the paper.
- **A tour in modern cryptography**: This presentaion was a two-part lecture that aimed to introduce students to the main goals and definitions of cryptographic primitives, also introduce the main ideas in classical and quantum-secure cryptography.
- **Introduction to Spectral Graph Theory**: A quick introduction to spectral graph theory and important theorems building up to Kirchhof's Matrix-Tree theorem. In this presentation we used spectral graph theory to talk about chromatic number, graph structure and graph polynamials.
- **Spectral Clustering**: I used my previous experience in spectral graph theory to present a brief introduction to a data mining class. This project made me familiar with graph embedding and topology in data scientific applications.

Other Projects

- **Study the structure of z_n^* group and applications in cryptography**: Answering the question: "For which $n \in N$ the multiplicative group of integers modulo n is cyclic?", proving the "Primitive root theorem", analysing the computational complexity of discrete logarithm problem and proposed sub-exponential algorithms, introducing the "Diffie-Hellman key exchange method".
- **A survey on heuristic approches for the Set Covering Problem**: I presented heuristic algorithms for SCP using PSO, ACO and Genetic Algorithm, and further developed a better algorithm by combining ACO and GA, that matched the current best known results.
- **Google's PageRank algorithm**: Introducing the Web graph and the random surfer model, eigenvalue centerality, Google PageRank algorithm and search result prioritizing.
  I implemented the PageRank algorithm in Pyhton.
- **Image Segmentation using heuristic search**: I used histogram analysis and Particle Swarm Optimization (PSO) to create an image clustering algorithm. I tested this algorithm on "ALL IDB" dataset for acute lymphoblastic leukemia detection.
- **COOL compiler**: I created a compiler for COOL programming language. This compiler includes Lexer, Parser and Semantical analyzer.

Teaching Experience

- **University Of Tehran**
  Student Assistant
  - **Data Structures and Algorithms**
  - **Combinatorics**
  - **Graph Theory**
  - **Computation Theory**
  - **Artificial Inteligence**
- **EPFL**
  Student Assistant
  - **Algorithms I** Prof. Svenson