Haetham AL ASWAD

PHD student in cryptography

Personal Information

- Birth : 1996 in Deraa, Syria
- Citizenship : French, Syrian
- Email : haetham.al-aswad@inria.fr
- Webpage : `https://members.loria.fr/HAlAswad/`

PhD Thesis

Oct 2021 - continues **Discrete Logarithm in Finite Fields**, *INRIA Nancy*, France
under the supervision of Emmanuel Thomé and Cécile Pierrot. I focus on studying the Discrete Logarithm problem, specifically in non-prime finite fields (with extension degree greater than one). My research contributes to improving the Number Field Sieve algorithm and its variants in both theoretical and practical aspects.

Education

2020 - 2021 **Master 2 in Applied algebra**, *University of Versailles*, France

2020 **Degree of agrégation in Mathematics**, *France*

2019 - 2020 **Master 2 preparation of the agrégation in Mathematics**, *University of Saclay*, France

2018 - 2019 **Master 1 in fundamental Mathematics**, *University of Saclay*, France

2017 - 2018 **Bachelor's degree in fundamental and applied Mathematics**, *University of Saclay*, France

Publications and ongoing work

Al Aswad, Pierrot **Individual Discrete Logarithm with Sublattice Reduction**, *Designs, Codes and Cryptography*, 2023

Unpublished work

Al Aswad, Pierrot, Thomé **Discrete Logarithm Factory**
eprint : `https://eprint.iacr.org/2023/834`, under submission to Crypto.

Ongoing work

I currently work with Cécile Pierrot and Emmanuel Thomé on using Galois automorphisms in the Tower Number Field Sieve. We have exciting results that lead to significant accelerations in the linear algebra step. These accelerations allow significant and practical improvements in attacks against pairings. The work will be made public soon.

Internships, Projects, and Fellowships

May 2022 - June 2022 **Research stay at the University of California as part of the thesis**, *UCSD*, San Diego
under the supervision of Nadia Heninger and Emmanuel Thomé. I Worked on my Phd and discussed lattice related problems with Nadia Heninger and Phd's students Adam Suhl and Keegan Rayan. This tenure was sponsored by the program *Dream* of University of Lorraine

Internships

March 2021 - Sept 2021 **The individual Logarithm step in NFS**, *INRIA Nancy*, France
under the supervision of Cécile Pierrot

2019, 40h **Teaching in high school**, *lycée des loges Evry*, France

2019 **Study of group representation's theory and an application to random walks on finite groups**, *University of Saclay*, France
under the supervision of Amaury Freslon

August 2018 **Study of the quality of digital hand signatures using fractal dimensions**, *Institute of Mines Télécom Evry*, France
under the supervision of Nesma Houmani

Summer Schools

Nov 2022 - Dec 2022 **REDOCS : Constructing an authentication protocol**, *CIRM*, France
under the supervision of Chloé Hébant. Development of an authentication protocol designed to address a real-world challenge presented by the company *Cosmian*. This is a co-work with four other Phd-students

August 2019 **MathInFoly**, *Insa Lyon*, France
Introduction to cryptography and proofs with Coq

Implementations

Nov 2023 **Implementation in Sage of the Tower Number Field Sieve**, *INRIA*, France
Co-project with Cécile Pieroot and Emmanuel Thomé

Dec 2020 - Feb 2021 **Implementation in C of the Hellman-Reyneri algorithm for the discrete logarithm in small characteristics**, *University of Versailles*, France
Co-project with Hadrien Notarantonio

Fellowships

Oct-2021 - Sep 2024 **INRIA fellowship for PhD**

Oct-2021 - Sep 2024 **French Ministry of Army fellowship for PhD**

May-2022 - June 2024 **Mobility fellowship Dream**, *University of Lorraine*, France
Two months stay at the University of California San Diego

Other

2016 **Co-author of the comic book Haytham une jeunesse syrienne**, *edition Dargaud*
Comic book co-written with the writer Nicolas Hénin and the cartoonist Kuyng Park

Teaching

Lectures

Nov 2023 - Dec 2023 **Graph theory : shortest path problem (Master 1)**, *6h*, École des mines Nancy, France

Study of three algorithms, Bellman-Ford, Dijkstra, and A*, with a focus on correctness and optimality proofs. The notes are available on my webpage

Exercise sessions

2021 -2024 **Exercise sessions in the following courses for three years**, *64h per year*, École des mines Nancy, France

- Programming in Python and Data Structure (Bachelor 3).
- Advanced Algorithms and Complexities (Bachelor 3).
- Operations Research (Bachelor 3).
- Introduction to Machine Learning (Master 1).
- Programming Languages : JavaScript and Go (Master 1).

2019 - 2021 **Mathematics (Bachelor 1)**, *2h per week*, Blaise Pascal Orsay, France

2017 - 2018 **Preparation for Science at University**, *20h*, University of Saclay, France

Supervision of students

Jan 2022 **Studying primality tests : ”Observation Internship” for a ninth grader**, *35h*, INRIA Nancy, France

Languages

Arabic and French (bilingual)

English (fluent)

Other interests

Politics. I am implicated in anti-discrimination political movements. I believe that doing research is a political act with profound societal consequences. Therefore, I view reflections on these consequences as equally crucial to the research process itself.

Teaching. I continuously try to improve my teaching skills. I consider teaching as an inseparable part of research. I love the enthusiastic interactions with students, usually about their projects.

Chess. I love playing chess and I participate in amateur-level tournaments. In my childhood, I won the chess championship of the city of Deraa in Syria in the children category.