Giacomo Fenzi

Milan, Italy · giacomofenzi@outlook · +41 765985537 · GitHub (WizardOfMenlo)

About Me

PhD in cryptography and proof systems at EPFL, supervised by Alessandro Chiesa. My research interests are quite varied, spacing from (my main focus) interactive proof systems and their practical instantations to cryptanalysis of post quantum cryptographic primitives, methods for automatic discovery of bugs in cryptographic implementations and more.

Education

EPFL — Lausanne, Switzerland
PhD in Computer Science — September 2022 - Present

ETH Zürich - EPFL — Zürich and Lausanne, Switzerland
MSc in Cybersecurity — September 2020 - August 2022
Master Thesis - *Klondike: Finding Gold in SIKE*

University of St. Andrews — St. Andrews, United Kingdom
BSc (Hons) Mathematics and Computer Science — September 2016 - July 2020
First Class degree - **GPA** 18/20
Dean's list '17-'18-'19-'20
SH Project - *Zero Knowledge Proofs, Theory and Applications*

Experience

ETH Zürich — Zürich, Switzerland
Hilfsassistent, Zero Knowledge Proofs - Applied Cryptography — September 2021 - August 2022

Teaching Assistant for the Zero Knowledge Proofs, held by Dr. Jonathan Bootle, and Applied Cryptography, held by Prof. Dr. Paterson. Developed exercises and solutions for exercise sessions and labs, and supervised exercise sessions.

Twitter — London, United Kingdom
Summer Intern, Make Everything Searchable — June 2021 - September 2021

Within the Search Result Page (SRP), developed new modules to gauge user feedback, and integrated them so to be available to the Data Science team. Conducted experiments to determine how user experience is affected by different SRP configurations

University of St. Andrews — St. Andrews, United Kingdom
Undergraduate Summer Research Assistant — June 2020 - August 2020

Researched stabiliser chain computations in the context of group theory, and developed from scratch a Rust library to efficiently compute them, with an emphasis on usability and extensive benchmarking (peal.github.io)

Goldman Sachs — London, United Kingdom
Summer Intern, Merchant Banking Division — June 2019 - August 2019

Derived mathematical models to optimize leverage on investments, built indexing services for easy serialization and deserialization, and contributed to a full stack project for regulatory documents, integrated within the company workflow

Deloitte — Milan, Italy
Summer Intern, Advanced Analytics — June 2018 - July 2018

Used machine learning models and statistical techniques such as Tensorflow, Xgboost and ARIMA to forecast future workforce trends and designed a portfolio website for the division using D3.js

Goldman Sachs — London, United Kingdom
Spring Intern, Investment Management Division — April 2018

Designed a system using pre-existing data sources to expose companies' fundamental data via API to internal clients

TecGlass Digital — Lalín, Spain
Summer Intern — June 2017

Created applications using WPF and C# to assist both the marketing team and the R&D department in fulfilling their roles

Publications

Books

- *(Forth).* G. Fenzi, *Latin Diachronic Frequency Dictionary Vol. 2.* Propylaeum: Digital Classics Books. Heidelberg: Universitätsbibliothek Heidelberg, 2022.
- *(Forth).* G. Fenzi, J. Leslie, W. Short and T. Spinelli, *Latin Diachronic Frequency Dictionary Vol. 4.* Propylaeum: Digital Classics Books. Heidelberg: Universitätsbibliothek Heidelberg, 2022.

Digital Publications

- M. R. Albrecht, G. Fenzi, N.K. Nguyen, O. Lapiha, SLAP: Succinct Lattice-Based Polynomial Commitments from Standard Assumptions, 2023. Available: https://eprint.iacr.org/2023/1469
- G. Fenzi, H. Moghaddas, N.K. Nguyen, Lattice-Based Polynomial Commitments: Towards Asymptotic and Concrete Efficiency, 2023. Available: https://eprint.iacr.org/2023/846
- G. Fenzi, A. Michael and T. Spinelli, Latin Decoder, University of Manchester, 2021. Available: latindecoder.com
- G. Fenzi, K. Kolosowski and T. Spinelli, Handbook of Latin Phonetics App, Libreria Ateneo Salesiano, 2020. Available: com.kolosowski.latinhandbook
- G. Fenzi, K. Kolosowski, J. Rybojad and T. Spinelli, Dataset, Latin Phonetics Processor, University of St Andrews. Available: doi:10.17630/19ce37ba-2d35-4920-bd7f-6287977de369
- G. Fenzi, K. Kolosowski and T. Spinelli, Latin Near-Synonyms App, University of St Andrews. Available: com.apps.kolosowski.synonymum
- G. Fenzi, T. Spinelli, Latin Diachronic Database, University of St. Andrews. Available: doi:10.5281/zenodo.2562829
- G. Fenzi, T. Spinelli, Online Dictionary of Latin Near-Synonyms. University of St Andrews. Available: doi:10.17630/3cf644e6-86b8-44d0-a50a-b33c7ca86072

Presentations & Projects

All projects available at linktree.com/giacomo.fenzi and gfenzi.io

Presentations

- Elliptic Curves: a (not so) brief introduction — Zürich, Switzerland, 2021
- Lossy Trapdoor Functions and their Applications — Zürich, Switzerland, 2021
- An Introduction to Category Theory: Towards Haskell's Applicative — Milan, Italy, 2021
- Teach Me X: Quantum Computing — St. Andrews, United Kingdom, 2020
- Teach Me X: Rust and Safe Systems Programming — St. Andrews, United Kingdom, 2019

Projects

Chosen Paper Attack	Zürich, Switzerland
Latin Diachronic Database	St. Andrews, United Kingdom
Stabchain (within PEAL group)	St. Andrews, United Kingdom

Skills

Research Interests: Public Key Cryptography, Post Quantum Cryptography and Cryptanalysis, Elliptic Curves, Isogenies, Lattices, Zero Knowledge Proofs

Programming Languages: Rust, Go, Python, Java, C, C++

Languages: English and Italian