# Marco Marchesin

Email: marco37marchesin@gmail.com Website: marcomarchesin.it

## Education

Sep 2022 – Mar 2025 M.S. in Mathematics, curricula in Cryptography, Univesity of Trento, Italy.
Thesis: Classification of Planar Functions in Characteristic Five.
Supervisor: Prof. Irene Villa.

Sep 2017 – Sep 2020 B.S. in Computer Science, Univerisity of Padua, Italy.
Thesis: Study and implementation of SSI in the context of IAM.
Supervisor: Prof. Francesco Ranzato.

### Skills

Languages: Italian, mothertongue; English, C1 attested by Univesity of Trento; French, basic.
Soft: Organisation and planning. Leadership and diplomatic. Adaptability and proactive.
Computers: Office suite; *development and management of UNIX-like system, network and database*; forensics and reverse engineering; programming: Scheme, miniKanren, Magma, ANSI C/C++, Python.
These programming languages are my preferences or what we are currently using. Putting the whole list would be useless.

### Publications

Nov 2025 G. Gelpi, —, *A Practical Encrypted Cloud for Financial Data*, FCIR25. Presented Oct 1, 2025.

### Extracurricular Activities

2022 – today Volunteer of De Componendis Cifris.
Automated generation of DOI and website pages for Koine volumes.

2018 – today Member of mHackeroni and others.
Capture the flag teams solving security challenges.

### Awards

Jan 2024 Cyprus Tech Odyssey 2024, University of Nicosia & XRPL Commons
First place with a PoC for a whistleblowing service.

Oct 2020 CryptoWars2020, with Flying Pwnycorn, 4th place.

## Employment history

Feb 2026 – today Fixed-term Researcher, University of Bari, Remote.
Research on Algebraic Methods in Cryptanalysis, supervised by Prof. Roberto La Scala. The goal of this project is to develop efficient methods of cryptanalysis on modern ciphers by modelling them as multivariate polynomials systems over finite fields.

Apr 2025 – May 2025 Cryptography Consulting, Prof. Roberto La Scala and Ing. Gianandrea Gelpi, Trento, Italy.
Development, experimentation and simulation of proof-of-concept for Functional Encryption protocols based on Multivariate cryptography (UOV Scheme) in Magma for its application in some common use cases (Inner Product Functional Encryption). Characterization of the protocol and related parameters to guarantee Multivariate Functional Encryption with reasonable security levels. Study of practicality of the choosen protocols in terms of key size and efficiency of algorithms for encryption and decryption.

Feb 2025 – Mar 2025 Cryptography Consulting, Ing. Gianandrea Gelpi, Trento, Italy.
Prototype for Multi-party Computation Threshold ECDSA Signatures (DKLS 2023) in Go.

Mar 2024 – Sep 2024 Internship as payment integration developer, Argentea S.R.L., Trento, Italy.
Android Development for PAX payment terminal, payment integrations, extending exisiting protocols, query design for complex database, planning non-disruptive updates.

Nov 2020 – Sep 2022 Full-stack Software Engineer, Monokee S.R.L., Padua, Italy.
SCIM implementation and integration; Unit Test; quality management systems (ISO 9001:2008); SonarQube; Azure DevOps Pipelines; improved Quality of Work with an internal documentation system and reproducible builds using Docker.

Dec 2021 – Mar 2022 Software Engineer, Accenture P.L.C., Remote.
Hashicorp Vault Plugins written in Go for password rotation automation; Salesforce and Splunk integration; verifier application for policy automation.

Jul 2020 – Aug 2020 Internship as Software Engineer, Athesys S.R.L., Padua, Italy.
Self-sovereing Identity (SSI) in Identity and Access Management (IAM).

Oct 2018 – Feb 2019 Internship as Trainee, Friso Computer S.R.L., Padua, Italy
Computer repair; Data recovery; UNIX sysadmin; Network management.

Aug 2016 – Sep 2018 Internship as DevSecOps, Entelligo B.V., Amsterdam, The Netherlands.
Opinionated SaaS.

## Portfolio

2020 – ongoing Alchemy. An extensible computer algebra library written in Scheme.

Dec 2020 HITCON 2020 Write up, 100 pins

Oct 2020 mHackeCTF 2020, Organized an Attack and defence Capture The Flag, https://ctftime.org/event/1053

Feb 2020 Haskell solution to Google hash code 2020, Ask for repository link.

2014 – 2021 *TramPadova*, iOS and Web Application with Go backend to show trams in Padua.

2012 – 2017 *Score Arco*, iOS Application for keeping score of archery matches.

Autorizzo il trattamento dei dati personali presenti nel CV ai sensi del D.Lgs. 2018/101 e del GDPR (Regolamento UE 2016/679).
Last updated: March 9, 2026