Giacomo Santato

Ph.D. Student in Cryptography – FHE | MPC | Cryptanalysis
santato.giacomo@gmail.com | Linkedin | Personal Website |

Education

Ph.D. student in Cryptography — Saarbrücken, Germany
CISPA Helmholtz Center for Information Security — *May 2022 - Present*

- Main focus on Fully Homomorphic Encryption and Multi-Party Computation.
- PhD advisor: Antoine Joux.
- Expected completion date: Mid 2026.

Double Master of Science cum laude (Mathematics) — The Netherlands/Italy
Leiden University and Padova University — *Sep 2019 - Jul 2021*

- Graduated cum laude from both universities with a 4.0 GPA.

Bachelor of Science cum laude (Mathematics) — Padova, Italy
Padova University — *Sep 2016 - Sep 2019*

Publications

Fherret: Proof of FHE Honest Evaluation with Circuit Privacy from MPCitH
J. Huth, A. Joux, G. Santato; IACR ePrint Archive — *Apr 2025*

- Developed proof systems securing FHE against reaction-based attacks using MPC-in-the-Head paradigms.
- Proof-of-concept implementation in C++ using OpenFHE.

On Circuit Private, Multikey and Threshold Approximate Homomorphic Encryption
K. Kluczniak, G. Santato; IACR Communications in Cryptology (CiC) — *Apr 2025*

- Conducted in-depth analysis of circuit privacy and multiparty security in approximate FHE schemes.

Dimensional eROSion: Improving the ROS Attack with Decomposition in Higher Bases
A. Joux, J. Loss, G. Santato; IACR ePrint Archive — *Feb 2025*

- Improved the ROS cryptanalysis by reducing attack complexity through lattice reduction.
- Sagemath implementation of the attack against Schnorr Blind Signatures (Github).

Other Experience

Applied Cryptography & Competitions

- Active member of about:blankets CTF team (2023–present).
- Fully solved Cryptohack: challenge-based cryptanalysis platform.

Scholarships

- ALGANT scholarship for talented master students in Algebra, Cryptography, and Number Theory.
- INdAM scholarship for talented bachelor mathematics students in Italy.

Skills

Languages

- English: C1 level, TOEFL iBT with a 110/120 score.
- Italian: Mother tongue.

Programming

- Python 3 (SageMath 10, PyCryptodome library).
- C++ (OpenFHE library).