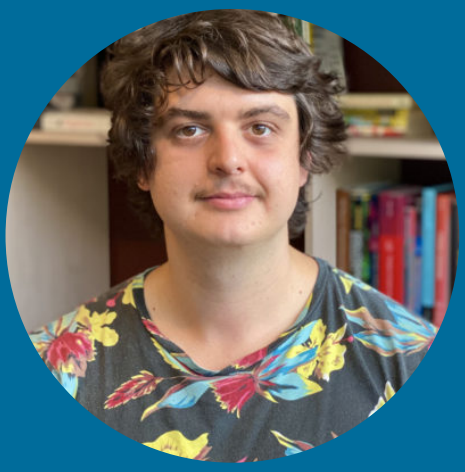
Carlo Brunetta

Independent Consultant &
Researcher in Math & Cryptology



I love learning and solving any challenge by sharing my experience with others.

Italian, Europe

Links

charlietrip.neocities.org
brunocarletta@gmail.com
Google Scholar
/carlo-brunetta
/CharlieTrip
/Charlie_Trip

Short Summary

- PhD: **Crypto**, MSc/BSc: **Math**
- ~20 peer-rev. & publ. papers
- Teamwork, Team Management, Leadership Experience
- Fast Learner
- Respectful, Open-Minded
- Teaching + Supervision exp.

Research Interests

- Cryptanalysis
- Privacy-Preserving Crypto
- Multi-Party Computations
- Side-Channel Attacks
- Alg. Optimization

Currently, I work as a...

Independent Consultant in Cryptology

Paris (France) Jan 2024 – (on going) **EU VAT ID :** FR04 933 961 070

I collaborate with prof. Massimiliano Sala on applied cryptology projects for/together with international clients and startups.

The projects involves tasks such as:

- design of novel solution for securely expand the application-oriented features of *Multi-Party Signature Scheme*
- development of *Threshold Signature Scheme* prototypes in *Golang* and efficiency evaluation
- design of distributed protocol for novel *blockchain-application*
- technical writing of white-paper for future product
- academic writing in the domain of applied cryptography

Selected Publications

Credential Loss Problem for Cryptowallet Custodians (Short Paper)
M. Battagliola, *C. Brunetta* **FCIR 2025**

SoK: Modelling Data Storage and Availability
C. Brunetta, M. Sala **Financial Crypto – WTSC 2025**

Leakage Certification Made Simple
A. Chowdhury, A. Roy, *C. Brunetta*, E. Oswald **Crypto 2024**

Modelling Cryptographic Distinguishers Using Machine Learning
C. Brunetta, P. Picazo **Journal of Cryptographic Engineering**

Non-Interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning
C. Brunetta, G. Tsaloli, B. Liang, G. Banegas, A, Mitrokotsa **ACISP 2021**

Professional Experience

Independent Consultant in Cryptology

Paris (France) Jan 2024 – (on going)

EU VAT Number: FR04 933 961 070

Research Area: Applied Cryptography, Threshold Signature Scheme, Secure Multi Party Protocols, Computational Optimization, Cryptanalysis

Postdoctoral Researcher

Simula UiB (Bergen, Norway) Oct 2021 – Sep 2023

Research Area: Theoretical Cryptology, Information Theory, Design of Block Cipher, Side-Channel Attacks, Cryptanalysis, Mass-Surveillance Security, Computational Optimization

Doctor of Philosophy - Cryptography

Chalmers University of Technology (Göteborg, Sweden) Sep 2016 – Aug 2021

Thesis: *"Cryptographic Tools for Privacy Preservation"*

Research Area: Theoretical Cryptology, Privacy Applications, Security in Wearable Devices, Differential Privacy, Homomorphic Encryption, Mathematics

MSc - Mathematics
Curriculum: *Coding Theory and Cryptography*

University of Trento (Trento, Italy) Sep 2014 – Jul 2016

Thesis: *"Algorithms and bounds for hidden sums in crypto. trapdoors"*

BSc - Mathematics

University of Trento (Trento, Italy) Sep 2011 – Sep 2014

Thesis: *"Attribute Based Encryption"*

Academic Citizenship

Supervision

- *"Sudoku and Security (Sudokurity!)"*, Håvard Skjetne Lilleheie & Johanne Krogholm Sand, Summer Internship at Simula UiB (2023)
- *"Framework for Hidden Sum Attacks on Blockciphers: Constructing and Launching Hidden Sum Attacks Against Block-ciphers"*, Ludvig Blomkvist, MSc (2022)
- *"Virtual Outsourcing of Verifiable Computation with Function Hiding"*, Christian Ross, MSc (2021)
- *"A Decentralized Voting System"*, 6 students, BSc (2020)
- *"A Decentralised Polling Application: Utilising the Ethereum Platform"*, 6 students, BSc Thesis (2020)
- *"The Signal Protocol for non-Cryptographers"*, Lamiya Yagublu, MSc (2019)
- *"A Decentralized Voting System"*, 6 students, BSc (2019)

Conference

- 1st International Conference: Financial Cryptography in Rome (FCiR 2025) (as Editor)
- 21st International Conference on Applied Cryptography and Network Security (ACNS 2023) (as Program Committee)
- The 38th ACM/SIGAPP Symposium On Applied Computing (SAC 2023) (as Program Committee)

Reviewer

JCM, CCS, CSF, NORDSEC, Euro S&P, ACISP, Journal IET, WISEC, MDPI Entropy, MDPI Computer, SAC, ACNS, GLOBECOM

Teaching

Teaching Assistant for *"Computer Security"*, *"Network Security"* and *"Cryptography"* at Chalmers each year between 2016-2019

Language Fluency

- Italian
- English
- French

- Python
- LaTeX
- Java
- Rust
- Golang
- C,C++
- General WebDev

General Skills

- Fast Learner
- Problem Solving
- Communication

- Leadership
- Management
- Mentoring
- Networking

- Divulgation
- Research
- Supervision
- Teaching

Self-evaluation scale using the mantra: *"To completely master a skill, one must know that there is nothing else to learn."*

Minimal Able Knowledgable Professional Master

Academic Publications

Credential Loss Problem for Cryptowallet Custodians (Short Paper)
M. Battagliola, *C. Brunetta* — **FCIR 2025**

Authentication Framework with Enhanced Privacy and Batch Verifiable Message Sharing in VANETs
S. Naskar, *C. Brunetta*, G. Hancke, T. Zhang, M. Gidlund — **IEEE TVT 2025**

Influence of Faulty Signatures in Batch Verification in VANET
S. Naskar, *C. Brunetta*, G. Hancke, T. Zhang, M. Gidlund — **ICPS 2025**

SoK: Modelling Data Storage and Availability
C. Brunetta, M. Sala — **Financial Crypto – WTSC 2025**

Leakage Certification Made Simple
A. Chowdhury, A. Roy, *C. Brunetta*, E. Oswald — **Crypto 2024**

A Scheme for Distributed Vehicle Authentication and Revocation in Decentralized VANETs
S. Naskar, *C. Brunetta*, G. Hancke, T. Zhang, M. Gidlund — **IEEE Early Access**

SoK: Public Key Encryption with Openings
C. Brunetta, H. Heum, M. Stam — **PKC 2024**

Multi-Instance Secure Public-Key Encryption
C. Brunetta, H. Heum, M. Stam — **PKC 2023**

Modelling Cryptographic Distinguishers Using Machine Learning
C. Brunetta, P. Picazo — **Journal of Cryptographic Engineering**

Turn Based Communication Channel
C. Brunetta, M. Larangiera, B. Liang, A, Mitrokotsa, K. Tanaka — **PROVSEC 2021**

Non-Interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning
C. Brunetta, G. Tsaloli, B. Liang, G. Banegas, A, Mitrokotsa — **ACISP 2021**

DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-preserving Learning
G. Tsaloli, B. Liang, *C. Brunetta*, G. Banegas, A, Mitrokotsa — **ISC 2021**

Code-Based Zero Knowledge PRF Arguments
C. Brunetta, B. Liang , A. Mitrokotsa — **ISC 2019**

A Lattice-Based Commitment Scheme with Applications to Simulatable VRFs
C. Brunetta, B. Liang , A. Mitrokotsa — **ProvSec 2018** (Workshop)
Journal ver. **JISIS 2018**

HIKE: Walking the Privacy Trail
E. Pagnin, *C. Brunetta*, P. Picazo — **CANS 2018**

A Differentially Private Encryption Scheme
C. Brunetta, B. Liang , C. Dimitrakakis , A. Mitrokotsa — **ISC 2017**

On hidden sums compatible with a given block cipher diffusion layer
C. Brunetta, M. Calderini, M. Sala — **WCC 2017**
Extended ver. Journal **Discrete Mathematics**

Towards the verification of image integrity in online news
C. Brunetta, A. F. Vinci, G.Boato, C. Pasquini, V. Conotter — **Multimedia & Expo Workshop 2015**

Crypto & Math Knowledge

- Computational Algebra
- Cryptanalysis
- Elliptic Curve
- Formal Proving
- Formal Verification
- Homomorphic Encryption
- Linear Algebra
- Multi Party Computation
- Post-Quantum Crypto
- Privacy
- Secure Impl. Hardware
- Secure Impl. Software
- Side-Channel
- Standard Primitives
- Verifiable Computation
- Web 3
- Zero-Knowledge

Self-evaluation scale using the mantra: *"To completely master a skill, one must know that there is nothing else to learn."*

Minimal — Able — Knowledgable — Professional — Master