Personal information

Name / Surname	**Brunetta Carlo**
Telephone	+46 736964104
Personal Email	brunocarletta@gmail.com
Home page	https://charlietrip.neocities.org
Nationality	Italian
Date of birth	28 May 1992
	Google Scholar Profile
ORCID	0000-0001-9363-7585

Summary

Myself	I love to share, discuss and tackle challenges with other people. I believe that Respect is the fundamental ingredient for any good team/relationship.
Interests	Cryptography and Security: designing of new protocols and primitives, optimization of attacks and algorithms. Formal proving of security guarantees. Application of Mathematics in Computer Science or Engineering environment. Using formal argument for modelling, optimizing and solving concrete challenges.
Skills	Formal/critical argumentation, research, teamwork and team management. Extended mathematical, coding/algorithmic and engineering knowledge.
Achievements	16 peer-reviewed and published papers, reviewer and program committee for several international conferences, teaching and supervision experience. Experiences in leadership and management of teams.

Last Occupation

Date (from-to)	October 2021 - September 2023
Name of the institute	Simula UiB
	Postdoctoral Researcher - Cryptography
Research topic/interest	Theoretical Cryptography, Side-Channel Attacks, Block Ciphers, Mathematics, Automotive Authentication Protocol, Zero-Knowledge
Additional Responsibilities	Planning, organizing and developing social/team building activities (member of the social committee of Simula UiB), actively collaborating with HR for the well-being of PhD students.

Last Education

Date (from-to)	September 2016 - August 2021
Name of the institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
	Doctor of Philosophy - Cryptography
Thesis	*"Cryptographic Tools for Privacy Preservation"*
Research topic/interest	Theoretical Cryptography, Privacy Applications, Differential Privacy, Homomorphic Encryption, Security in Wearable Devices, Zero-Knowledge, Mathematics
Additional Responsibilities	Student representative for the CSE PhD Council (2017-2021), management of the webpage for CSE Network and Systems ex-division, member of a CSE cross-departmental music band

Academic Experience

Date (from-to)	October 2021 - September 2023
Name of the institute	Simula UiB
	Postdoctoral Researcher - Cryptography
Research topic/interest	Theoretical Cryptography, Side-Channel Attacks, Block Ciphers, Mathematics, Automotive Authentication Protocol, Zero-Knowledge
Additional Responsibilities	Planning, organizing and developing social/team building activities (member of the social committee of Simula UiB), actively collaborating with HR for the well-being of PhD students.
Date (from-to)	September 2016 - August 2021
Name of the institute	Chalmers University of Technology , Dep. of Computer Science and Engineering
	Doctor of Philosophy - Cryptography
Thesis	*"Cryptographic Tools for Privacy Preservation"*
Supervision	*Supervisor:* Aikaterini Mitrokotsa, *cosupervisor:* Bei Liang
	Further information on the defence can be found at this link
Research topic/interest	Theoretical Cryptography, Privacy Applications, Differential Privacy, Homomorphic Encryption, Security in Wearable Devices, Mathematics
Additional Responsibilities	Student representative for the CSE PhD Council (2017-2021), management of the webpage for CSE Network and Systems ex-division, member of a CSE cross-departmental music band, organization of a PhD level self-study course
Date (from-to)	September 2014 - July 2016
Name of the institute	University of Trento – Department of Mathematics
	Master degree in Mathematics - Curriculum *Coding Theory and Cryptography*
Thesis	*"Algorithms and bounds for hidden sums in cryptographic trapdoors"*
Supervision	*Supervisor:* Massimiliano Sala, *cosupervisor:* Marco Calderini
Additional Responsibilities	Student representative for the Mathematical department (2014-2016), management of advanced mathematical talks for students, organization of departmental events
Date (from-to)	September 2011 - September 2014
Name of the institute	University of Trento – Department of Mathematics
	Bachelor Degree in Mathematics
Thesis	*"Attribute Based Encryption"*
Supervision	*Supervisor:* Andrea Caranti
Additional Responsibilities	Student representative for the Mathematical department (2012-2014), management of advanced mathematical talks for students, organization of departmental events

Industrial Experience

Date (from-to)	September 2015 - March 2016
Name and address	Argentea Srl - Trento (Italy)
Sector	Payment processor and terminal POS manager
Contract	Project with the University of Trento to develop new Mobile Payment using Bitcoin and PagoBancomat (the Italian payment circuit)
Tasks	Study the PagoBancomat standard, EMV technical manual and created a document that analyses the security contained in these protocols. Development of some ideas on the possible integration of payment using Bitcoin and PagoBancomat into an Argentea product.

Teaching Experience

Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Course	**TDA352 – Cryptography** (2016 – 2019)
Role	Leading Teaching Assistant (TA), frontal lecture with exercise sessions and addendum to the course content
Students	Master level, $\sim$200 students
Additional Responsibilities	Re-design all the students weekly exercises and team assessments, handling students' communications, managing course webpage/Canvas page, exam co-design, management of the exam correction
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Course	**EDA263 – Computer Security** (2017 – 2020)
Role	Teaching Assistant, laboratory exercise sessions
Students	Master level, $\sim$130 students
Additional Responsibilities	Exam correction, verifying exercises correctness
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Course	**EDA491 – Network Security** (2017 – 2020)
Role	Teaching Assistant, laboratory exercise sessions
Students	Master level, $\sim$130 students
Additional Responsibilities	Exam correction, verifying exercises correctness

Supervision Experience

Institute	Simula UiB
PhD Students	Hans Heum, Sigurd Jordal – during 2021-2023
Role	Co-supervision of the PhD (main supervisor: Martijn Stam)
Institute	Mid Sweden University
PhD Students	Sujash Naskar – during 2023-2024
Role	Mentoring and research collaboration
Institute	Simula UiB
Project	*"Sudoku and Security (Sudokurity!)"* – Summer Internship 2023
Students	Håvard Skjetne Lilleheie (master), Johanne Krogholm Sand (bachelor)
Role	Main responsible for the internal proposal (for funds) and project, interns co-supervised with Maiara Bollauf (PostDoc @ Simula UiB), handling the administrative required steps and interview co-management with HR
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Thesis	*"Framework for Hidden Sum Attacks on Blockciphers: Constructing and Launching Hidden Sum Attacks Against Block-ciphers"* – MSc 2022
Student	Ludvig Blomkvist
Role	Supervisor following Chalmers guidelines
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Thesis	*"Virtual Outsourcing of Verifiable Computation with Function Hiding"* – MSc 2021
Student	Christian Ross
Role	Supervisor following Chalmers guidelines
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Thesis	*"A Decentralized Voting System"* – BSc 2020
Students	6 students team
Thesis	*"A Decentralised Polling Application: Utilising the Ethereum Platform"* – BSc 2020

Students	6 students team
Role	Team-management and supervision following Chalmers guidelines, second and third iteration of this bachelor thesis project
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Thesis	*"The Signal Protocol for non-Cryptographers"* – MSc 2021
Student	Lamiya Yagublu
Role	Co-supervision
Institute	Chalmers University of Technology, Dep. of Computer Science and Engineering
Thesis	*"A Decentralized Voting System"* – BSc 2019
Students	6 students team
Role	Team-management and supervision following Chalmers guidelines, first iteration of this thesis project

Academic Citizenship

Role	Reviewer
Venue	CCS, CSF, NORDSEC, Euro S&P, ACISP, Journal IET, WISEC, MDPI Entropy, MDPI Computer, SAC, ACNS, ICDCN, internal reviews for students
Role	Program Committee
Venue	21st International Conference on Applied Cryptography and Network Security (ACNS 2023: https://sulab-sever.u-aizu.ac.jp/ACNS2023/index.html)
Venue	The 38th ACM/SIGAPP Symposium On Applied Computing (SAC 2023: http://www.sigapp.org/sac/sac2023/index.html)
Role	Organization Committee
Venue	23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2021: https://www.cse.chalmers.se/~elad/SSS2021/index.html)
Role	Social Activities Committee
Institute	Simula UiB (2022-2023)
Responsibilities	Organizing social activities, designing anonymous feedback system for scheduling activities that facilitate diversity and inclusion
Role	Student Representative – PhD Council
University	Chalmers – CSE Department – PhD Council (2017-2021)
Responsibilities	Representation of students' needs at the departmental meetings, development of a common communication infrastructure, organization of formal (and non) events, collaboration with extra-departmental representation groups, investigations and reporting on PhD stress, work-life balance and supervision issues to the CSE Research School and department (reports *"50 Shades of Supervision/Stress"*)
Role	Student Representative
University	Università di Trento – Mathematics Department (2012-2016)
Responsibilities	Representation of students' needs at the departmental meetings, development of a common communication infrastructure, organization of formal (and non) events, collaboration with extra-departmental representation groups

Publication

Google Scholar	https://scholar.google.com/citations?user=RcS01mUAAAAJ
ORCID	https://orcid.org/0000-0001-9363-7585
Statistics	*h-index:* 7, *i10-index:* 4 (source Google Scholar)

Highlighted Papers

Title	**Modelling Cryptographic Distinguishers Using Machine Learning**
Authors	*C. Brunetta*, P. Picazo
Date - Venue	*Jun 2022* - Journal of Cryptographic Engineering
Paper	Personal copy link, journal link
Role	Main responsible for the paper's idea, organization and development. Designer of the theoretical framework, co-design of the experiments and data analysis and responsible for the formal verification of the theorems.
Importance	The paper formalizes the idea that machine learning (or similar artificial intelligence methods) can effectively be used for cryptanalysis and other type of crypto-oriented attacks. Differently from other papers in the area, this paper's novelty resides in providing evidence that both formal guarantees and general frameworks can and should be achieved when combining machine learning and cryptanalysis in, for example, side-channel security analysis.

Title	**Non-Interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning**
Authors	*C. Brunetta*, G. Tsaloli, B. Liang, G. Banegas, A, Mitrokotsa
Date - Venue	*Dec 2021* - ACISP 2021
Paper	Personal copy link, proceedings link
Role	Responsible for the paper's solution and team organization and development. Designer of the theoretical framework, experiments and data analysis and responsible for the formal verification of the theorems and debugging of the code.
Importance	The paper provides a non-interactive version of a known protocol created by Google and designed for federated learning, i.e. a delegated machine learning paradigm with higher privacy guarantees. Differently from other papers in the area, this paper provides theoretical and empirical proofs that a simpler and more efficient approach to the problem (e.g. non-interactivity and simpler mathematical structures) is possible.

Title	**SoK: Public Key Encryption with Openings**
Authors	*C. Brunetta*, H. Heum, M. Stam
Date - Venue	*April 2024* - PKC 2024
Paper	Personal copy link, conference link (proceedings not yet published), preprint link
Role	Co-designer of the taxonomy framework, literature classification and analysis.
Importance	The paper provides a modular and comprehensive taxonomy of over 30 years of security notions for public key encryption schemes with different opening/corruption oracles able to model an immense variety of real/realistic attack scenarios. The biggest contribution is providing a guideline for developers to identify the security notion required by an application depending on the accepted security risk.

Title	**Turn Based Communication Channel**
Authors	*C. Brunetta*, M. Larangiera, B. Liang, A, Mitrokotsa, K. Tanaka
Date - Venue	*Dec 2021* - PROVSEC 2021
Paper	Personal copy link, proceedings link
Role	Main responsible for the paper's idea, team organization and development. Designer of the theoretical framework and co-responsible for the formal verification of the theorems.

Importance	The paper provides a general framework for building a secure and consistent communication channel using a model commonly used in the Blockchain domain. Differently from other papers, the paper opens the opportunity to the definition of publicly-fair protocol which are of current interest in the Web3 domain.
Title	**Towards the verification of image integrity in online news**
Authors	*C. Brunetta,* A. F. Vinci, G.Boato, C. Pasquini, V. Conotter
Date - Venue	*Jun 2015* - Multimedia & Expo Workshop
Paper	Personal copy link, proceedings link
Role	Co-responsible for the paper's idea, experiment and code development. Designer of the data analysis and experimental framework.
Importance	The paper provides a methodology and framework for how web-crawlers and image-comparison algorithms can create metadata-based timelines where a forensic investigator can spot if news contains fake images. This paper precedes the modern machine learning/artificial intelligence usage and application and was pioneering the requirement of tools for media analysis aided with automatic technologies, e.g. web-crawlers and searching engines.

Peer-Reviewed Conference

Title	**Leakage Certification Made Simple**
Authors	A. Chowdhury, A. Roy, *C. Brunetta*, E. Oswald
Date - Venue	*(To Appear) August 2024* - Crypto 2024
Title	**A Scheme for Distributed Vehicle Authentication and Revocation in Decentralized VANETs**
Authors	S. Naskar, *C. Brunetta*, G. Hancke, T. Zhang, M. Gidlund
Date - Venue	*May 2024* - IEEE Early Access
Title	**SoK: Public Key Encryption with Openings**
Authors	*C. Brunetta*, H. Heum, M. Stam
Date - Venue	*April 2024* - PKC 2024
Title	**Multi-Instance Secure Public-Key Encryption**
Authors	*C. Brunetta*, H. Heum, M. Stam
Date - Venue	*May 2023* - PKC 2023
Title	**Modelling Cryptographic Distinguishers Using Machine Learning**
Authors	*C. Brunetta*, P. Picazo
Date - Venue	*Jun 2022* - Journal of Cryptographic Engineering
Title	**Turn Based Communication Channel**
Authors	*C. Brunetta*, M. Larangiera, B. Liang, A, Mitrokotsa, K. Tanaka
Date - Venue	*Dec 2021* - PROVSEC 2021
Title	**Non-Interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning**
Authors	*C. Brunetta*, G. Tsaloli, B. Liang, G. Banegas, A, Mitrokotsa
Date - Venue	*Dec 2021* - ACISP 2021
Title	**DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-preserving Learning**
Authors	G. Tsaloli, B. Liang, *C. Brunetta*, G. Banegas, A, Mitrokotsa
Venue	*Nov 2021* - ISC 2021
Title	**Code-Based Zero Knowledge PRF Arguments**

Authors	*C. Brunetta*, B. Liang , A. Mitrokotsa
Date - Venue	*Sep 2019* - ISC 2019
Title	**A Lattice-Based Commitment Scheme with Applications to Simulatable VRFs**
Authors	*C. Brunetta*, B. Liang , A. Mitrokotsa
Date - Venue	*Nov 2018* - ProvSec 2018 (Workshop)
Title	**HIKE: Walking the Privacy Trail**
Authors	E. Pagnin, *C. Brunetta*, P. Picazo
Date - Venue	*Sep 2018* - CANS 2018
Title	**A Differentially Private Encryption Scheme**
Authors	*C. Brunetta*, B. Liang , C. Dimitrakakis , A. Mitrokotsa
Date - Venue	*Nov 2017* - ISC 2017
Title	**On hidden sums compatible with a given block cipher diffusion layer**
Authors	*C. Brunetta*, M. Calderini, M. Sala
Date - Venue	*Feb 2019* - WCC 2017
Title	**Towards the verification of image integrity in online news**
Authors	*C. Brunetta,* A. F. Vinci, G.Boato, C. Pasquini, V. Conotter
Date - Venue	*Jun 2015* - Multimedia & Expo Workshop

Peer-Reviewed Journal

Title	**A Lattice-Based Commitment Scheme with Applications to Simulatable VRFs**
Authors	*C. Brunetta*, B. Liang , A. Mitrokotsa
Date - Venue	*Nov 2018* - Journal ver. JISIS 2018
Title	**On hidden sums compatible with a given block cipher diffusion layer**
Authors	*C. Brunetta*, M. Calderini, M. Sala
Date - Venue	Extended Journal ver. “Discrete Mathematics” 342-2

Preprint, Under Submission

Title	**Efficient Zero-Knowledge Distributed Vehicle Authentication in Decentralized VANETs**
Authors	S. Naskar, *C. Brunetta*, G. Hancke, T. Zhang, M. Gidlun
Date - Venue	Under submission (journal)

Additional Info

Presentation	All the published conference papers Additional presentation during research visits: Harvard (2016), Tokyo Tech (2019), Lund University (2020), IT University of Copenhagen (ITU) (2020)
Courses	During PhD (General Transferable Skill (GTS) courses) and Postdoc on Teaching, Ethics, Supervision, (Team) Management and Efficiency Courses on Project Management, Efficient Team Management, Information Retrieval and Utilization, Personal Efficiency, Scientific Divulgation, Leadership
Technical Skills	Advanced algorithmic analysis (academic research level) Code-capable, i.e. rapid learning of new programming languages based on the task's needs. *Examples:* Rust, Python, Java, LaTeX, C, C++, MatLab, VBA, Visual Basic, HTML, CSS, JavaScript, Ruby, Magma Currently re-implementing several research project in Rust and publishing code and explanation on my personal webpage Intermediate knowledge of hardware and network configurations
Volunteering	Local folkloristic festival organization, design of questions and supervision at the Simula UiB IMO 2022 (local phase for the International Mathematical Olympics 2022)
Languages	Italian (mother tongue), English (professional), Swedish and Norwegian (beginner)

Trieste, May 29, 2024
Carlo Brunetta