

## Personal information

Name / Surname **Brunetta Carlo**  
Personal Email brunocarletta@gmail.com  
Home page <https://charlietrip.neocities.org>  
Nationality Italian  
Date of birth 28 May 1992  
Gender Male



## Summary

**Myself** I love solving problems, learning and expanding my knowledge. I love to share, discuss and tackle challenges with other people. I like working in diverse teams where sharing expertise is mandatory for succeeding. I believe that Respect is the fundamental ingredient for any good team/relationship.

**Seeking** Problem-solving job, preferably in areas of Cryptography or Mathematics.

**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

## 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

<p><b>Personal Skills</b></p> <p>Languages</p> <p>Management</p> <p>Technical Skills</p> <p>Teaching and Supervision</p>	<p>Italian (mother tongue), English (professional level)</p> <p>Several courses (during PhD and Postdoc) on Teaching and Supervision  Courses on Project Management, Efficient Team Management, Information Retrieval and Utilization, Personal Efficiency, Scientific Divulgateion, Leadership Organization and management of volunteers for a local folk/music festival.  Public relations for several musical bands.</p> <p>Advanced algorithmic analysis (academic research level)  Code-capable, i.e. rapid learning of new programming languages based on the task's needs. <i>Examples:</i> Python, Java, L<sup>A</sup>T<sub>E</sub>X, C, C++, MatLab, VBA, Visual Basic, HTML, CSS, JavaScript, Ruby, Magma  Intermediate knowledge of hardware and network configurations.</p> <p>Teaching Assistant for several courses between 2016-2019. Supervision of 3× MSc Thesis and 3× BSc Thesis (6 students group).</p>
<p><b>Academic Experience</b></p> <p>Date (from-to)</p> <p>Name of the institute</p> <p>Research topic/interest</p> <p>Date (from-to)</p> <p>Name of the institute</p> <p>Thesis</p> <p>Research topic/interest</p> <p>Date (from-to)</p> <p>Name of the institute</p> <p>Thesis</p> <p>Date (from-to)</p> <p>Name of the institute</p> <p>Thesis</p>	<p>October 2021 - September 2023 (on going)  Simula UiB  <b>Postdoctoral Researcher - Cryptography</b>  Theoretical Cryptography, Side-Channel Attacks, Block Ciphers, Mathematics</p> <p>September 2016 - August 2021  Chalmers University of Technology , Dep. of Computer Science and Engineering  <b>Doctor of Philosophy - Cryptography</b>  <i>"Cryptographic Tools for Privacy Preservation"</i>  Theoretical Cryptography, Privacy Applications, Differential Privacy, Homomorphic Encryption, Security in Wearable Devices, Mathematics</p> <p>September 2014 - July 2016  University of Trento – Department of Mathematics  <b>Master degree in Mathematics - Curriculum Coding Theory and Cryptography</b>  <i>"Algorithms and bounds for hidden sums in cryptographic trapdoors"</i></p> <p>September 2011 - September 2014  University of Trento – Department of Mathematics  <b>Bachelor Degree in Mathematics</b>  <i>"Attribute Based Encryption"</i></p>
<p><b>Publication</b></p> <p>Google Scholar</p> <p>ORCID</p> <p>Title</p> <p>Authors</p> <p>Date - Venue</p> <p>Title</p>	<p><a href="https://scholar.google.com/citations?user=RcS01mUAAAAJ">https://scholar.google.com/citations?user=RcS01mUAAAAJ</a></p> <p><a href="https://orcid.org/0000-0001-9363-7585">https://orcid.org/0000-0001-9363-7585</a></p> <p><b>Leakage Certification Made Simple</b>  A. Chowdhury, A. Roy, C. Brunetta, E. Oswald  <i>(To Appear) August 2024 - Crypto 2024</i></p> <p><b>A Scheme for Distributed Vehicle Authentication and Revocation in Decentralized VANETs</b></p>

Authors	S. Naskar, C. Brunetta, G. Hancke, T. Zhang, M. Gidlund
Date - Venue	May 2024 - IEEE Early Access
Title	<b>SoK: Public Key Encryption with Openings</b>
Authors	C. Brunetta, H. Heum, M. Stam
Date - Venue	April 2024 - PKC 2024
Title	<b>Multi-Instance Secure Public-Key Encryption</b>
Authors	C. Brunetta, H. Heum, M. Stam
Date - Venue	May 2023 - PKC 2023
Title	<b>Modelling Cryptographic Distinguishers Using Machine Learning</b>
Authors	C. Brunetta, P. Picazo
Date - Venue	Jun 2022 - Journal of Cryptographic Engineering
Title	<b>Turn Based Communication Channel</b>
Authors	C. Brunetta, M. Larangiera, B. Liang, A. Mitrokotsa, K. Tanaka
Date - Venue	Dec 2021 - PROVSEC 2021
Title	<b>Non-Interactive, Secure Verifiable Aggregation for Decentralized, Privacy-Preserving Learning</b>
Authors	C. Brunetta, G. Tsaloli, B. Liang, G. Banegas, A. Mitrokotsa
Date - Venue	Dec 2021 - ACISP 2021
Title	<b>DEVA: Decentralized, Verifiable Secure Aggregation for Privacy-preserving Learning</b>
Authors	G. Tsaloli, B. Liang, C. Brunetta, G. Banegas, A. Mitrokotsa
Venue	Nov 2021 - ISC 2021
Title	<b>Code-Based Zero Knowledge PRF Arguments</b>
Authors	C. Brunetta, B. Liang, A. Mitrokotsa
Date - Venue	Sep 2019 - ISC 2019
Title	<b>A Lattice-Based Commitment Scheme with Applications to Simulatable VRFs</b>
Authors	C. Brunetta, B. Liang, A. Mitrokotsa
Date - Venue	Nov 2018 - ProvSec 2018 (Workshop) - Journal ver. JISIS 2018
Title	<b>HIKE: Walking the Privacy Trail</b>
Authors	E. Pagnin, C. Brunetta, P. Picazo
Date - Venue	Sep 2018 - CANS 2018
Title	<b>A Differentially Private Encryption Scheme</b>
Authors	C. Brunetta, B. Liang, C. Dimitrakakis, A. Mitrokotsa
Date - Venue	Nov 2017 - ISC 2017
Title	<b>On hidden sums compatible with a given block cipher diffusion layer</b>
Authors	C. Brunetta, M. Calderini, M. Sala
Date - Venue	Feb 2019 - WCC 2017 - Extended Journal ver. "Discrete Mathematics" 342-2
Title	<b>Towards the verification of image integrity in online news</b>
Authors	C. Brunetta, A. F. Vinci, G. Boato, C. Pasquini, V. Conotter
Date - Venue	Jun 2015 - Multimedia & Expo Workshop

---

## Academic Roles

Role	Program Committee
------	-------------------

Venue	21st International Conference on Applied Cryptography and Network Security (ACNS 2023: <a href="https://sulab-sever.u-aizu.ac.jp/ACNS2023/index.html">https://sulab-sever.u-aizu.ac.jp/ACNS2023/index.html</a> )
Venue	The 38th ACM/SIGAPP Symposium On Applied Computing (SAC 2023: <a href="http://www.sigapp.org/sac/sac2023/index.html">http://www.sigapp.org/sac/sac2023/index.html</a> )
Role	Reviewer
Venue	CCS, CSF, NORDSEC, Euro S&P, ACISP, Journal IET, WISEC, MDPI Entropy, MDPI Computer, SAC, ACNS
Role	Organization Committee
Venue	23rd International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2021: <a href="https://www.cse.chalmers.se/~elad/SSS2021/index.html">https://www.cse.chalmers.se/~elad/SSS2021/index.html</a> )
Role	Supervision <i>"Framework for Hidden Sum Attacks on Blockciphers: Constructing and Launching Hidden Sum Attacks Against Block-ciphers"</i> , Ludvig Blomkvist, MSc Thesis (2022) <i>"Virtual Outsourcing of Verifiable Computation with Function Hiding"</i> , Christian Ross, MSc Thesis (2021) <i>"A Decentralized Voting System"</i> , 6 students, BSc Thesis (2020) <i>"A Decentralised Polling Application: Utilising the Ethereum Platform"</i> , 6 students, BSc Thesis (2020) <i>"The Signal Protocol for non-Cryptographers"</i> , Lamiya Yagublu, MSc Thesis (2019) <i>"A Decentralized Voting System"</i> , 6 students, BSc Thesis (2019)
Role	Teaching Teaching Assistant for <i>"Computer Security"</i> , <i>"Network Security"</i> and <i>"Cryptography"</i> at Chalmers each year between 2016-2019

---

## 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.
Date (from-to)	February - May 2015
Name and address	Siemens Transformers S.p.A. - Spini di Gardolo (Italy)
Sector	Producer of mid/low-voltage transformer
Contract	Project contract as a consultant in the ENG department
Tasks	Tasks automation, research and optimization of the internal data flow
Date (from-to)	June - December 2013
Name and address	Siemens Transformers S.p.A. - Spini di Gardolo (Italy)
Sector	Producer of mid/low-voltage transformer
Contract	Stage in the ENG and R&D department
Tasks	Tasks automation, research and optimization of the internal data flow, optimization on the construction price of a transformer

---