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	10-ish published papers, reviewer and program committee for several international conferences, teaching and supervision experience. Experiences in team-working and management.

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, Mathematics

Personal Skills

Languages	Italian (mother tongue), English (professional level)
Management	Several courses (during PhD and Postdoc) on Teaching and Supervision Courses on Project Management, Efficient Team Management, Information Retrieval and Utilization, Personal Efficiency, Scientific Divulgation, Leadership Organization and management of volunteers for a local folk/music festival. Public relations for several musical bands.
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:* Python, Java, LaTeX, C, C++, MatLab, VBA, Visual Basic, HTML, CSS, JavaScript, Ruby, Magma Intermediate knowledge of hardware and network configurations.
Teaching and Supervision	Teaching Assistant for several courses between 2016-2019. Supervision of 3× MSc Thesis and 3× BSc Thesis (6 students group).

Academic Experience

Date (from-to)	October 2021 - September 2023 (on going)
Name of the institute	Simula UiB
	Postdoctoral Researcher - Cryptography
Research topic/interest	Theoretical Cryptography, Side-Channel Attacks, Block Ciphers, Mathematics
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, Mathematics
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"*
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"*

Publication

Google Scholar	https://scholar.google.com/citations?user=RcS01mUAAAAJ
ORCID	https://orcid.org/0000-0001-9363-7585
Title	**SoK: Public Key Encryption with Openings**
Authors	*C. Brunetta*, H. Heum, M. Stam
Date - Venue	*(To appear) 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	**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) - Journal ver. JISIS 2018
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 - Extended Journal ver. “Discrete Mathematics” 342-2
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

Academic Roles

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	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: https://www.cse.chalmers.se/~elad/SSS2021/index.html)
Role	Supervision

	“Framework for Hidden Sum Attacks on Blockciphers: Constructing and Launching Hidden Sum Attacks Against Block-ciphers”, Ludvig Blomkvist, MSc Thesis (2022) *“Virtual Outsourcing of Verifiable Computation with Function Hiding”*, Christian Ross, MSc Thesis (2021) *“A Decentralized Voting System”*, 6 students, BSc Thesis (2020) *“A Decentralised Polling Application: Utilising the Ethereum Platform”*, 6 students, BSc Thesis (2020) *“The Signal Protocol for non-Cryptographers”*, Lamiya Yagublu, MSc Thesis (2019) *“A Decentralized Voting System”*, 6 students, BSc Thesis (2019)
Role	Teaching Teaching Assistant for *“Computer Security”*, *“Network Security”* and *“Cryptography”* 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

Trieste, January 16, 2024
Carlo Brunetta