

ELENA PAGNIN

Assistant Professor at Chalmers
University of Technology

Personal Info

Nationality: Italian, Swedish

E-mail: elenap@chalmers.se

Webpage: epagnin.github.io

Profiles: Google Scholar, LinkedIn
Scopus

ORCID: 0000-0002-7804-6696

Impact [\(Google Scholar\)](#)

No. publications: **20+**

No. citations: **286**

h-index: **9**

Languages



Italian: Mother tongue (C2)

English: Fluent (C1)

Spanish: Fluent (B2)

Swedish: Intermediate (B1)

Education & Titles

since 2022	Assistant Professor Tenure-Track (Biträdande Professor)	Chalmers (SE)
2020 - 2022	Associate Senior Lecturer (Biträdande Universitetslektor)	Lund University (SE)
2019 - 2020	Post-Doctoral Researcher in Cryptography	Aarhus University (DK)
Feb - Mar 2014 - 2019	Ph.D. in Computer Science (Cryptography)	Chalmers (SE)
May - Jan	Thesis Title: <i>"Be more and be merry: enhancing data and user authentication in collaborative settings"</i> 	
	Supervisor: A. Sabelfeld	
2016	Licentiate Degree of Engineering	Chalmers (SE)
Aug 25th	Thesis Title: <i>"Authentication under Constraints"</i> 	
	Supervisor: A. Mitrokotsa	
2012 - 2013	Project Officer (paid Researcher Assistant position)	Nanyang TU (SG)
Aug - Feb	Master thesis project under Prof. F. Oggier supervision	
2011-2013	Master's in Applied Mathematics	University of Trento (IT)
	Thesis Title: <i>"Homomorphic Authentication Codes for Linear Network Coding"</i> Score: 110 / 110, cum laude	
2008-2011	Bachelor's in Pure Mathematics	University of Padova (IT)
	Thesis Title: <i>"Surfaces, Maps and Projections. A Teaching Experience"</i> Score: 102/110	

Upcoming Events

2022-23	CoSupervisor of Master Theses: Hanna Jonson <i>Practical evaluation of chain-like MPC protocols</i> (2023), Luca Torrisetti <i>Probing the practicality of efficient and progressive verification</i> (2022)	Lund University & Università di Milano (IT)
---------	---	---

Works Accepted for Publication in the Last Year

- *Bifrost: Secure, Scalable and Efficient File Sharing System Using Dual Deduplication* (**IEEE-CloudNet22**)
- *Count Me In! Extendability for Threshold Ring Signatures* (**PKC22**)
- *Progressive And Efficient Verification For Digital Signatures* (**ACNS22**)
- *Secure Cloud Storage with Joint Deduplication and Erasure Protection* (**IEEE-Cloud22**)
- *CatNap: Practical and Actively Secure Proximity Testing with a Napping Party based on Generic MPC Techniques* (**SECURITY22**)
- *Outsourcing MPC Precomputation for Location Privacy* (**LPW22**)

Selection of Achievements (Grants & Awards)

2020-2024	PI in a personal grant awarded to strategic research areas by the Excellence Center ELLIIT	(1.6M SEK)
2020	Best Paper Award for the full-version of <i>"Multi-Key Homomorphic Authenticators"</i> (extended abstract appeared in ASIACRYPT16) granted by the IET Information Security Journal. [This kind of Premium Award is given to recognise the best research papers published during the last two years]	
2015-2017	Four Short Term Scientific Missions (STSM) funded by e-COST Actions IC1306 and 1403	
2015	Japanese Society for Promotion of Science (JSPS) Summer Program Fellow at Prof. Tanaka lab	TokyoTech (JP) (500K YEN)
2014	"Premio di Merito" (award for merits) given to students who achieved stellar results in their masters (2.8K EUR)	University of Trento (IT)

Selection of Professional Activities

Supervision of PhD Students

2022 - now	Arthur Nijdam: <i>Secure Machine Learning for the Medical Sector</i> (main supervisor A. Aminifar)	Lund University (SE)
2022 - now	Martin Gunnarsson: <i>Securing IoT Systems</i> (main supervisor C. Gehrman)	Lund University (SE)
2020 - now	Joakim Brorsson: <i>Privacy Enhancing Technologies</i> (main supervisor M. Hell)	Lund University (SE)
2020 - now	Hadi Sehat: <i>Efficient & Private Cloud Storage Solutions</i> (main supervisor D. Lucani)	Aarhus University (DK)
2019 - now	Ivan Oleynikov: <i>Privacy-Preserving Location Proximity Testing</i> (main supervisor A. Sabelfeld)	Chalmers (SE)
	Licentiate: 30 Sept 2022. Planned PhD Defence: 31 Aug 2024	

Leading Roles

2022-now	Head of the Crypto Lab at the CSE Department	Chalmers (SE)
----------	---	---------------

2022	Scientific Leader at the EIT Department in Lund University for "SMARTY" SSF grant RIT17-0035	(22M SEK)
2019-2020	Board Member of ALICE (Alliance for women in It, Computing and Engineering at Aarhus University)	Aarhus University (DK)
2017-2018	Elected Member of the PhD Council at the Department of Computer Science and Engineering	Chalmers (SE)

Service in the Commuinity

09.09.2022	Invited Speaker at a National hearing of researchers on "Innovative Processes for Data Intergrity and Data Sharing" organized by the Swedish Ministry for Integrity Protection (Integritetsskyddsmyndigheten - IMY)	Stockholm (SE)
17.08.2022	Invited Panelist on "Allyship and Inclusion" at CRYPTO22	Santa Barbara (CA, USA)

Assessment of Others' Work

2021-2023	Program Committee Member for ACNS23, SEC@SAC22, ACISP21	
2019	Examiner for the PhD Defence of <i>Ijlal Loutfi</i> on "Trusted Execution on Commodity Devices"	University of Oslo (NO)
2015-2022	Subreviewer or Reviewer for <i>Journals</i> : Computer Journal, IET Information Security, IEEE Comm. Letters; <i>Conferences</i> : Crypto22, SEC@SAC22, ACISP21, TCHES21, SCN20, CCS19, AsiaCrypt19, POST18, iFM17, IndoCrypt16, ESORICS16, Infocom15.	

Research and Outreach Presentations

2022	Invited Speaker at the seminar series at <i>Protocol Labs</i> : Extended Threshold Ring Signatures	(remote)
	Invited Speaker at the CRC seminar series at <i>TII Research Centers</i> : Progressive and Efficient Verifications	(remote)
2021	Invited Speaker at ELLIIT initiative on <i>Future-Oriented Research</i> : "Enhancing Data Authentication"	Lund (SE)
	Invited Speaker at "Meet The Scientist" event organized by <i>ALICE</i> , Aarhus University	(remote)
2021	Participant in the <i>Researchers' Grand Prix</i> : Security and Privacy in the Digital Era	Helsinborg (SE)
2020	Invited Speaker at <i>Framtidsveckan</i> : AI, digitalisering och integritet – vad får vi för vår hälsodata? Popular Science Presentation and Panel Discussion on "Contact tracing apps and their security dilemmas"	Lund (SE)
2018	Invited Speaker at Göteborgs Vetenskapsfestivalen	Gothenburg (SE)

Teaching Experience

2022-now	Course Responsible for the Master level course <i>Cryptography</i> (TDA352/DIT250, 7.5hp)	Chalmers (SE)
2022	Lecturer and Co-instructor for the Master level course <i>Advanced Cryptography</i> (EITN85, 7.5hp)	Lund University (SE)
2020 - 2022	Lecturer and Instructor for the Master level course <i>Advanced Web Security</i> (EITN41, 7.5hp)	Lund University (SE)
2021	Course Responsible for the PhD level course <i>Frontiers in Security Research</i> (EIT190F, 7.5hp, 10 students)	Lund University (SE)
2015-2023	Supervisor of 6 Master Theses : Anton Jeppsson <i>Private set intersection via fully homomorphic encryption</i> (2020), Lamiya Yagublu <i>Explaining the Signal protocol</i> (2018), Anders Stigsson <i>Taxonomy of quantum algorithms</i> (2018), Emilie Widegren <i>FHE: a case of study</i> (2017), Elena Fuentes Bongenaar <i>Multi-key homomorphic encryption</i> (2016), Jing Liu <i>Verifiable delegation of computation in the setting of privacy-preserving biometric authentication</i> (2015)	Chalmers & Lund University

Selected List of Publications

ACNS22	Boschini, Fiore, and Elena Pagnin : " <i>Progressive and Efficient Verification for Digital Signatures</i> ". In <i>International Conference on Applied Cryptography and Network Security - ACNS</i> (2022).
PKC22	Aranha, Hall-Andersen, Nitulescu, Elena Pagnin , and Yakoubov: " <i>Count Me In! Extendability for Threshold Ring Signatures</i> ". In <i>International Conference on Practice and Theory of Public-Key Cryptography - PKC</i> (2022).
SCN20	Lucani, Nielsen, Orlandi, Elena Pagnin , and Vestergaard: " <i>Secure Generalized Deduplication via Multi-Key Revealing Encryption</i> ". In <i>Security and Cryptography for Networks</i> (2020).
PETs19	Elena Pagnin , Gunnarsson, Talebi, Orlandi, and Sabelfeld: " <i>TOPPool: Time-aware Optimized Privacy-Preserving Ridesharing</i> ". In <i>Proceedings on Privacy Enhancing Technologies</i> (2019).
AC16	Fiore, Mitrokotsa, Nizzardo, and Elena Pagnin : " <i>Multi-key Homomorphic Authenticators</i> ". In <i>Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT</i> (2016).