

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: **430+**

h-index: **12**






Education & Titles

since 2022	Assistant Professor Tenure-Track (Forskarassistent)	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	



Recent Achievements (Grants & Awards)

2023	Co-PI in a seed funding awarded by Chalmers' Areas of Advance on the topic <i>Towards a Multi-Layer Security Vision for Transportation Systems in the 6G Era</i>	(0.5M SEK)
2023-2027	PI of the prestigious Starting Grant awarded by the Swedish Research Council (VR starting) on <i>Progressive Verification of Cryptographic Schemes</i>	(4M SEK)
2020-2022	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 recognize the best research papers published during the last two years]	


Supervision of PhD Students (= I am the main advisor, = I co-supervise together with)

2023 - now	Adrian Perez Keilty : <i>Progressive Verification of Cryptographic Schemes</i> ()	Chalmers (SE)
	Planned PhD Defense: 20 Aug 2028	
2023 - now	Hanna Ek : <i>Advanced Properties for Digital Signatures</i> ()	Chalmers (SE)
	Planned PhD Defense: 31 Dec 2027	
2019 - now	Ivan Oleynikov : <i>Privacy-Preserving Location Proximity Testing</i> ()	Chalmers (SE)
	Licentiate: 30 Sept 2022. Planned PhD Defense: December 2024	
2020 - now	Joakim Brorsson : <i>Privacy Enhancing Technologies</i> ( T. Johansson)	Lund University (SE)
	Planned PhD Defense: December 2024	
2022 - now	Arthur Nijdam : <i>Secure Machine Learning for the Medical Sector</i> ( P. Stankovski-Wagner)	Lund University (SE)
	Planned PhD Defense: September 2027	


Graduated Students




















2023.03.21	Martin Gunnarsson : <i>Securing IoT Systems</i> ( Prof. C. Gehrman)	Lund University (SE)
2023.02.28	Hadi Sehat : <i>Dual Deduplication in multi-client setting and its applications</i> ( Prof. D. Lucani)	Aarhus University (DK)

Selection of Professional Activities

31.01.2024	Referral to a new National law proposal on a Swedish electronic identification system <i>En säker och tillgänglig statlig e-legitimation</i> (SOU 2023:61)	
2021-now	Program Committee Member for: LatinCrypt23, ACNS23, SEC@SAC22, ACISP21.	
2022-now	Mentor in the WISE-WWACQT mentorship program	
11.10.2023	Seminar speaker at ICT Area of Advance full-day seminar on Navigating the Cybersecurity Landscape on <i>Fortifying the Digital Fortress: Provably Secure Cryptography</i>	Chalmers (SE)
2023	Invited Speaker at AI NORDIC POWWOW on "Cybersecurity and AI for Company Security"	Lund (SE)
2023	Seminar speaker at the BARC center on <i>Progressive Verification for Cryptographic Schemes</i>	KU Copenhagen (DK)
2022	Invited Speaker at the seminar series at <i>Protocol Labs: Extended Threshold Ring Signatures</i> 	(remote)

2022	Invited Speaker at the CRC seminar series at <i>TII Research Centers: Progressive and Efficient Verification</i> 	(remote)
2022	Invited Speaker at a National hearing of researchers on “Innovative Processes for Data Integrity and Data Sharing” organized by the Swedish Ministry for Integrity Protection (Integritetsskyddsmyndigheten - IMY)	Stockholm (SE)
2022	Invited Panelist on “Allyship and Inclusion” at CRYPTO22 	Santa Barbara (CA, USA)
2021	Invited Speaker at ELLIIT initiative on <i>Future-Oriented Research: “Enhancing Data Authentication”</i> 	Lund (SE)
2021	Participant in the <i>Researchers’ Grand Prix: Security and Privacy in the Digital Era</i> 	Helsingborg (SE)
2020	Invited Speaker at <i>Framtidsveckan: AI, digitalisering och integritet – vad får vi för vår hälsodata?</i> Presentation and Panel Discussion on “Contact tracing apps and their security dilemmas” 	Lund (SE)
2019	Examiner for the PhD Defence of <i>Ijlal Loutfi</i> on “Trusted Execution on Commodity Devices”	University of Oslo (NO)

Teaching Experience		
2015-now	Master's Theses: Supervisor of 9, Examiner for 1.	Chalmers, Università di Milano, Lund University
2022-now	Course Responsible for the Masters level course <i>Cryptography</i> (TDA352/DIT250, 7.5hp)	Chalmers (SE)
2022	Lecturer and Co-instructor for the Masters level course <i>Advanced Cryptography</i> (EITN85, 7.5hp)	Lund University (SE)
2020 - 2022	Lecturer and Course Responsible for the Masters 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) 	Lund University (SE)

Selected List of Publications	
SCN24 	Baum, David, Elena Pagnin , and Takahashi: “CaSCaDE:(Time-Based) Cryptography from Space Communications DE-lay”. In: <i>International Conference on Security and Cryptography for Networks</i> (2024).
EuroS&P24 	Nelson, Elena Pagnin , and Askarov: “Metadata Privacy Beyond Tunneling for Instant Messaging”. In: <i>IEEE EuroS&P</i> (2024).
CT-RSA23 	Brorsson, David, Gentile, Elena Pagnin , and Stankovski-Wagner: “PAPR: Publicly Auditable Privacy Revocation for Anonymous Credentials”. In: <i>The Cryptographers’ Track at RSA Conference</i> (2023).
ACNS22  , 	Boschini, Fiore, and Elena Pagnin : “Progressive and Efficient Verification for Digital Signatures”. In: <i>International Conference on Applied Cryptography and Network Security - ACNS</i> (2022).
CLOUD22 	Vestergaard, Elena Pagnin , Kundu, and Lucani: “Secure Cloud Storage with Joint Deduplication and Erasure Protection”. In: <i>International Conference on Cloud Computing - IEEE CLOUD</i> (2022).
PKC22  , 	Aranha, Hall-Andersen, Nitulescu, Elena Pagnin , and Yakoubov: “Count Me In! Extendability for Threshold Ring Signatures”. In: <i>International Conference on Practice and Theory of Public-Key Cryptography - PKC</i> (2022).
IEEE-ICC21 	Sehat, Elena Pagnin , and Lucani: “Yggdrasil: Privacy-Aware Dual Deduplication in Multi Client Settings”. In: <i>IEEE International Conference on Communications - ICC: SAC Cloud Computing, Networking and Storage Track</i> (2021).
SCN20  , 	Lucani, Nielsen, Orlandi, Elena Pagnin , and Vestergaard: “Secure Generalized Deduplication via Multi-Key Revealing Encryption”. In: <i>Security and Cryptography for Networks</i> (2020).
ESORICS20  , 	Oleynikov, Elena Pagnin , and Sabelfeld: “Where Are You Bob? Privacy-Preserving Proximity Testing with a Napping Party”. In: <i>European Symposium on Research in Computer Security – ESORICS</i> (2020).
PETs19 	Elena Pagnin , Gunnarsson, Talebi, Orlandi, and Sabelfeld: “TOPPool: Time-aware Optimized Privacy-Preserving Ridesharing”. In: <i>Proceedings on Privacy Enhancing Technologies</i> (2019).
EuroS&P19 	Blazy, Bossuat, Bultel, Fouque, Onete, and Elena Pagnin : “SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting”. In: <i>2019 IEEE European Symposium on Security and Privacy - EuroS&P</i> (2019).
SCN18  , 	Fiore and Elena Pagnin : “Matrioska: A Compiler for Multi-key Homomorphic Signatures”. In: <i>International Conference on Security and Cryptography for Networks - SCN</i> (2018).
AC16  , 	Fiore, Mitrokotsa, Nizzardo, and Elena Pagnin : “Multi-key Homomorphic Authenticators”. In: <i>Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT</i> (2016).