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:	**380+**
h-index:	**10**

Education & Titles

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

Recent Achievements (Grants & Awards)

2023	**Co-PI** in a seed funding awarded by Chalmers' Areas of Advance on the topic *Towards a Multi-Layer Security Vision for Transportation Systems in the 6G Era*	**(0.5M SEK)**
2023-2027	**PI** of the prestigious Starting Grant awarded by the Swedish Research Council (VR starting) on *Progressive Verification of Cryptographic Schemes*	**(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 "*Multi-Key Homomorphic Authenticators*" (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**: *Progressive Verification of Cryptographic Schemes* (👤) Planned PhD Defense: 20 Aug 2028	Chalmers (SE)
2023 - now	**Hanna Ek**: *Advanced Properties for Digital Signatures* (👤) Planned PhD Defense: 31 Dec 2027	Chalmers (SE)
2019 - now	**Ivan Oleynikov**: *Privacy-Preserving Location Proximity Testing* (👤) Licentiate: 30 Sept 2022. Planned PhD Defense: 31 Aug 2024	Chalmers (SE)
2020 - now	**Joakim Brorsson**: *Privacy Enhancing Technologies* (👥 T. Johansson) Planned PhD Defense: April 2024	Lund University (SE)
2022 - now	**Arthur Nijdam**: *Secure Machine Learning for the Medical Sector* (👥 A. Aminifar) Planned PhD Defense: September 2027	Lund University (SE)

Graduated Students

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

Selection of Professional Activities

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 *Fortifying the Digital Fortress: Provably Secure Cryptography*	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 *Progressive Verification for Cryptographic Schemes*	KU Copenhagen (DK)
2022	**Invited Speaker** at the seminar series at *Protocol Labs*: Extended Threshold Ring Signatures 📄	(remote)
2022	**Invited Speaker** at the CRC seminar series at *TII Research Centers*: Progressive and Efficient Verification 📄	(remote)

2022	**Invited Speaker** at a National hearing of researchers on "Innovative Processes for Data Intergrity and Data Sharing" organized by the Swedish Ministery 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 *Future-Oriented Research*: "Enhancing Data Authentication" 🎥	Lund (SE)
2021	**Participant** in the *Researchers' Grand Prix*: Security and Privacy in the Digital Era 🎥	Helsinborg (SE)
2020	**Invited Speaker** at *Framtidsveckan: AI, digitalisering och integritet – vad får vi för vår hälsodata?* Presentation and Panel Discussion on "Contact tracing apps and their security dilemmas" 🎥	Lund (SE)
2019	**Examiner** for the PhD Defence of *Ijlal Loutfi* 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 *Cryptography* (TDA352/DIT250, 7.5hp)	Chalmers (SE)
2022	**Lecturer and Co-instructor** for the Masters level course *Advanced Cryptography* (EITN85, 7.5hp)	Lund University (SE)
2020 - 2022	**Lecturer and Course Responsible** for the Masters course *Advanced Web Security* (EITN41, 7.5hp)	Lund University (SE)
2021	**Course Responsible** for the PhD level course *Frontiers in Security Research* (EIT190F, 7.5hp) 📄	Lund University (SE)

Selected List of Publications

CT-RSA23 📄	Brorsson, David, Gentile, **Elena Pagnin**, and Stankovski-Wagner: *"PAPR: Publicly Auditable Privacy Revocation for Anonymous Credentials"*. In: *The Cryptographers' Track at RSA Conference* (2023).
ACNS22 🎥, 📄	Boschini, Fiore, and **Elena Pagnin**: *"Progressive and Efficient Verification for Digital Signatures"*. In: *International Conference on Applied Cryptography and Network Security - ACNS* (2022).
CLOUD22 📄	Vestergaard, **Elena Pagnin**, Kundu, and Lucani: *"Secure Cloud Storage with Joint Deduplication and Erasure Protection"*. In: *International Conference on Cloud Computing - IEEE CLOUD* (2022).
PKC22 🎥, 📄	Aranha, Hall-Andersen, Nitulescu, **Elena Pagnin**, and Yakoubov: *"Count Me In! Extendability for Threshold Ring Signatures"*. In: *International Conference on Practice and Theory of Public-Key Cryptography - PKC* (2022).
IEEE-ICC21 📄	Sehat, **Elena Pagnin**, and Lucani: *"Yggdrasil: Privacy-Aware Dual Deduplication in Multi Client Settings"*. In: *IEEE International Conference on Communications - ICC: SAC Cloud Computing, Networking and Storage Track* (2021).
SCN20 🎥, 📄	Lucani, Nielsen, Orlandi, **Elena Pagnin**, and Vestergaard: *"Secure Generalized Deduplication via Multi-Key Revealing Encryption"*. In: *Security and Cryptography for Networks* (2020).
ESORICS20 🎥, 📄	Oleynikov, **Elena Pagnin**, and Sabelfeld: *"Where Are You Bob? Privacy-Preserving Proximity Testing with a Napping Party"*. In: *European Symposium on Research in Computer Security – ESORICS* (2020).
PETs19 📄	**Elena Pagnin**, Gunnarsson, Talebi, Orlandi, and Sabelfeld: *"TOPPool: Time-aware Optimized Privacy-Preserving Ridesharing"*. In: *Proceedings on Privacy Enhancing Technologies* (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: *2019 IEEE European Symposium on Security and Privacy - EuroS&P* (2019).
SCN18 🎥, 📄	Fiore and **Elena Pagnin**: *"Matrioska: A Compiler for Multi-key Homomorphic Signatures"*. In: *International Conference on Security and Cryptography for Networks - SCN* (2018).
AC16 🎥, 📄	Fiore, Mitrokotsa, Nizzardo, and **Elena Pagnin**: *"Multi-key Homomorphic Authenticators"*. In: *Annual International Conference on the Theory and Application of Cryptology and Information Security - ASIACRYPT* (2016).