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: **340+**
h-index: **10**

Languages

Italian: Mother tongue (C2)
English: Fluent (C1)
Spanish: Fluent (B2)
Swedish: Intermediate (B1)

Education & Titles

since 2022	**Assistant Professor** Tenure-Track (Forskarassistent)	Chalmers (SE)
2020 - 2022	**Associate Senior Lecturer** (Biträdande Universitetslektor)	Lund University (SE)
Apr-Aug		
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: "*Be more and be merry: enhancing data and user authentication in collaborative settings*" *Supervisor: A. Sabelfeld*	
2016	**Licentiate** Degree of Engineering	Chalmers (SE)
Aug 25th	Thesis Title: "*Authentication under Constraints*" *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** 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)

Selection of Achievements (Grants & Awards)

2023-2027	**PI** 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]	
2015-2017	Four **Short Term Scientific Missions (STSM)** funded by e-COST Actions IC1306 and 1403 [two at IMDEA (E), ETH (CH), Xlim/Limoges (F)]	
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	University of Trento (IT) (2.8K EUR)

Selection of Professional Activities

Supervision of PhD Students (= as main advisor, = in co-supervision with)

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: December 2025	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 (= in co-supervision with)

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)

Leading Roles

2022-now	**Head** of the CryptoTeam 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)

Assessment of Others' Work

2021-2023	**Program Committee Member** for: LatinCrypt23, ACNS23, SEC@SAC22, ACISP21	
2019	**Examiner** for the PhD Defence of *Ijlal Loutfi* on "Trusted Execution on Commodity Devices"	University of Oslo (NO)

2015-2023 **Subreviewer** or **Reviewer** for *Journals:* PETs, Computer Journal, IET Information Security, IEEE Comm. Letters. *Conferences:* LatinCrypt23, ACNS23, Crypto22, SEC@SAC22, ACISP21, TCHES21, SCN20, CCS19, AsiaCrypt19, POST18, iFM17, IndoCrypt16, ESORICS16, Infocom15.

Industrial Collaborations

2022-ongonig **Volvo AB Innovation Arena** (C. Carlsson and K. Lindström): "Autgoraph"

2020-2023 **Chocolate Cloud** (D. Lucani): "Secure Cloud-Aided Storage Solutions"
Publications in: IEEE-Cloud22, IEEE-ICC21, SCN20

2021-2022 **Protocol Labs** (A. Nitulescu): "Extendability for Threshold Ring Signatures"
Publication in: PKC22

Recent Research Presentations

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)
Invited Speaker at the CRC seminar series at *TII Research Centers*: Progressive and Efficient Verification — (remote)

Service in the Community

2022-now **Mentor** in the WISE-WWACQT mentorship program

09.09.2022 **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)

17.08.2022 **Invited Panelist** on "Allyship and Inclusion" at CRYPTO22 — Santa Barbara (CA, USA)

Outreach Presentations

2022 Popular science video on "Cybersecurity" (3mins)

2021 **Invited Speaker** at ELLIIT initiative on *Future-Oriented Research*: "Enhancing Data Authentication" — Lund (SE)
Invited Speaker at "Meet The Scientist" event organized by ALICE, Aarhus University — (remote)

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?* Popular Science Presentation and Panel Discussion on "Contact tracing apps and their security dilemmas" — Lund (SE)

2018 **Invited Speaker** at Göteborgs Vetenskapsfestivalen — Gothenburg (SE)

Formal Qualifications & Training

2022 **Swedish for University Staff (SFU)**, level 4 (out of 5), completed with grade 82/100 (VG) — Lund University (SE)

2021 **Readership Course (Docentkurs)**, 3 weeks = 4.5hp (GB_S91) — Lund University (SE)

2018 **Reflecting on Leadership Perspectives and Contexts** 5.0hp (GFOK090) — Chalmers (SE)

2015 **Advanced communication and Popular presentation** 1.5hp (GFOK045) — Chalmers (SE)
Teaching, Learning and Evaluation 3.0 hp (GFOK020)
Creating and Managing Effective Teams 1.5 hp (GFOK050)

2014 **Career Planning Your Personal Leadership** 1.5 hp (GFOK010) — Chalmers (SE)

Teaching Experience

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)

2015-2023 **Supervisor of Masters Theses**: Hanna Jonson *Practical evaluation of chain-like MPC protocols* (2023), Luca Torrisetti *Probing the practicality of efficient and progressive verification* (2022), Anton Jeppsson *Private set intersection via fully homomorphic encryption* (2020), Lamiya Yagublu *Explaining the Signal protocol* (2018), Anders Stigsson *Taxonomy of quantum algorithms* (2018), Emilie Widegren *FHE: a case of study* (2017), Elena Fuentes Bongenaar *Multi-key homomorphic encryption* (2016), Jing Liu *Verifable delegation of computation in the setting of privacy-preserving biometric authentication* (2015) — Chalmers, Università di Milano, Lund University

Selected List of Publications

CT-RSA23
Brorsson, David, Gentile, **Elena Pagnin**, and 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).

IndoC14
Elena Pagnin, Dimitrakakis, Abidin, and Mitrokotsa: *"On the Leakage of Information in Biometric Authentication"*. In: *International Conference on Cryptology in India - INDOCRYPT* (2014).