

Elena Pagnin

Associate Senior Lecturer
at Lund University

Personal Info

Birthday: 15.05.1989
Nationality: Italian, Swedish
E-mail: elena.pagnin@eit.lth.se
Webpage: epagnin.github.io

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

No. publications: **21**
No. citations: **252**
h-index: **8**

Languages

Italian:Mother tongue (C2)
English:Fluent (C1)
Spanish:Fluent (B2)
Swedish:Intermediate (B1)
German:Basic (A2)

Education & Titles

2020 - now	Associate Senior Lecturer (Biträdande Universitetslektor)	Lund University (SE)
start: Apr		
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> 📄 (degree received on 12-Nov-2018) Supervisor: A. Sabelfeld	
2016	Licentiate Degree of Engineering	Chalmers (SE)
Aug 25th	Thesis Title: <i>"Authentication under Constraints"</i> 📄 Supervisor: A. Mitrokovtsa	
2012 - 2013	Project Officer (paid researcher assistant position)	Nanyang Tech. Univ. (SG)
Aug - Feb	master thesis abroad under the supervision of F. Oggier	
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	

Achievements, Grants & Awards

2022-2024	Scientific leader at the EIT Department for the SSF "SMARTY" grant RIT17-0035 (22M SEK)	Lund University (SE)
2020-2022	Strategic research area ELLIIT personal grant (1.6M SEK)	Lund University (SE)
2020	Best Paper Award for <i>Multi-Key Homomorphic Authenticators</i> (full-version)	IET Information Security Journal
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 (500K YEN)	TokyoTech (JP)
2014	"Premio di Merito" (award for merits) given to students who achieved stellar results in their masters (2.8K EUR)	University of Trento (IT)

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).
LatinC21 📄 , 📄	Aranha, Elena Pagnin , and Rodríguez-Henríquez: <i>"LOVE a pairing"</i> . In <i>Progress in Cryptology - LATINCRYPT 2021</i> (2021).
IEEE-ICC21 📄	Sehat, Elena Pagnin , and Lucani: <i>"Yggdrasil: Privacy-Aware Dual Deduplication in Multi Client Settings"</i> . 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: <i>"Secure Generalized Deduplication via Multi-Key Revealing Encryption"</i> . In <i>Security and Cryptography for Networks</i> (2020).
ESORICS20 📄 , 📄	Oleynikov, Elena Pagnin , and Sabelfeld: <i>"Where Are You Bob? Privacy-Preserving Proximity Testing with a Napping Party"</i> . In <i>European Symposium on Research in Computer Security - ESORICS</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 - PETS</i> (2019).
EuroS&P19 📄	Blazy, Bossuat, Bultel, Fouque, Onete, and Elena Pagnin : <i>"SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting"</i> . In <i>2019 IEEE European Symposium on Security and Privacy - EuroS&P</i> (2019).
SCN18 📄 , 📄	Fiore and Elena Pagnin : <i>"Matrioska: A Compiler for Multi-key Homomorphic Signatures"</i> . In <i>International Conference on Security and Cryptography for Networks - SCN</i> (2018).

Professional Activities


Highlights

- 2022 **Invited Speaker** at the seminar series at *Protocol Labs*: Extended Threshold Ring Signatures 
Invited Speaker at the CRC seminar series at *TII Research Centers*: Progressive and Efficient Verifications 
- 2021-2022 **Program Committee Member** at SEC@SAC22, ACISP21
- 2019 **Examiner** for the PhD Defence of *Ijlal Loutfi* on "Trusted Execution on Commodity Devices" University of Oslo (NO)
- Journals **Subreviewer or Reviewer** for: Computer Journal, IET Information Security, IEEE Comm. Letters
- Conferences **Subreviewer or Reviewer** for: SEC@SAC22, ACISP21, TCHES21, SCN20, CCS19, AsiaCrypt19, POST18, iFM17, IndoCrypt16, ESORICS16, Infocom15.
- 2021 **Invited Speaker** at
 - ELLIIT initiative on digital seminars around *Future-Oriented Research*: "Enhancing Data Authentication" Lund (SE)
 - 'Meet The Scientist' event organized by ALICE (Alliance for women In Computer science and Engineering at 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?*, Contact tracing apps and their security dilemmas  Lund (SE)
- 2019-2020 **Board Member of ALICE** (Alliance for women in It, Computing and Engineering at Aarhus University) Aarhus University (DK)
- 2018 Member of the **Local and Organising Committee** of CANS 2018 Naples (IT)
- 2018 **Invited Speaker** at Göteborgs Vetenskapsfestivalen Gothenburg (SE)
- 2017-2018 **Elected Member of the PhD Council** at the Department of Computer Science and Engineering Chalmers (SE)

Supervision of PhD Students

- 2020 - 2023 **Joakim Brorsson** topic: *Privacy Enhancing Technologies* (main supervisor M. Hell) Lund University (SE)
- 2020 - 2022 **Hadi Sehat** topic: *Efficient & Private Cloud Storage Solutions* (main supervisor D. Lucani) Aarhus University (DK)
- 2020 - 2022 **Rohon Kundu** topic: *Fully Homomorphic Encryption from Number Theoretic Assumptions* (M. Hell) Lund University (SE)
- 2019 - 2024 **Ivan Oleynikov** topic: *Privacy-Preserving Location Proximity Testing* (main supervisor A. Sabelfeld) Chalmers (SE)

Teaching Experience

- 2022 **Supervisor** of Luca Torresetti's **Master Project** on *Progressive signature verification for IoT devices* in cooperation with Milano University under the 'research and study stay' framework and stipend Lund University (SE)
- Mar-Jun
- since 2022 **Lecturer and Co-instructor** for the Master level course *Advanced Cryptography*, in collaboration with T. Johansson and Q. Guo (ETIN85, 7.5hp, ~ 20 students) Lund University (SE)
- since 2020 **Lecturer and Instructor** for the Master level course *Advanced Web Security* (EITN41, 7.5hp, ~ 30 students) Lund University (SE)
- 2021 **Course Responsible** for the PhD level course *Frontiers in Security Research* (EIT190F, 7.5hp, 10 students)  Lund University (SE)
- 2020 **Supervisor of Master Theses Projects**: Anton Jeppsson *Private Set Intersection via Fully Homomorphic Encryption* Lund University (SE)
- 2014-2018 **Supervisor of 5 Master Theses**: 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 *Verifiable delegation of computation in the setting of privacy-preserving biometric authentication* (2015) Chalmers (SE)
- 2016-2017 **Lecturer and Instructor** for the Master level course *Cryptography* (TDA352/DIT250, 7.5hp, ~ 130 students) Chalmers (SE)
- 2014-2018 **Teaching Assistant** *Cryptography, Algorithms, Design and development of embedded systems, Technical writing, Programutveckling* Chalmers (SE)
- 2013-2014 **Teaching Assistant** for the courses *Geometry I* (Bsc Mathematics) and *Mathematics* (Bsc Chemistry) University of Padova (IT)