Elena Pagnin

Associate Senior Lecturer at Lund University

Personal Info

Birthday: 15.05.1989
Nationality: Italian
Driving: B
E-mail: elena.pagnin@eit.lth.se
Profiles: Google Scholar, LinkedIn

Impact

No. publications: **16**
No. citations: **163** (Google Scholar)
h-index: **7** (Google Scholar)

Languages

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

Hobbies

Martial arts, traveling, hiking, cooking, photography, theater, music, sailing.

Education & Titles

2020 - now	**Associate Senior Lecturer** (Biträdande Universtietslektor)	Lund University (SE)
2019 - 2020	**Post-Doctoral Researcher** in Cryptography	Aarhus University (DK)
2014 - 2019 (early defence on 07.09.2018)	**Ph.D.** in Computer Science (Cryptography) *Supervisors: A. Sabelfeld & D. Fiore (IMDEA)*	Chalmers University of Technology, Gothenburg (SE)
25.08.2016	**Licentiate** Degree of Engineering *Supervisors: A. Mitrokotsa & D. Fiore (IMDEA)*	Chalmers (SE)
2012-2013	**Project Officer** (paid researcher assistant position)	Nanyang Tech. Univ. (SG)
2011-2013	**Masters in Applied Mathematics** Score: **110** / 110**, cum laude**	University of Trento (IT)
2008-2011	**Bachelor Degree in Pure Mathematics**	University of Padova (IT)

Achievements, Grants & Awards

2020	**Best Paper Award** for *Multi-Key Homomorphic Authenticators* (Fiore, Mitrokotsa, Nizzardo, Pagnin)	IET Information Security Journal
2020-2022	Strategic research area **ELLIIT personal grant** (1.6M SEK)	Lund University (SE)
2015-2017	Four **Short Term Scientific Missions (STSM)** funded by e-COST Actions IC1306 and 1403	IMDEA, ETH, Xlim/Limoges
2015	Japanese Society for Promotion of Science **(JSPS) Summer Program Fellow** at Prof. Tanaka lab	TokyoTech (JP)
2014	"**Premio di Merito**" award for merits given to students who achieved stellar results in their masters	University of Trento (IT)

Professional Activities

Assignments as public examiner/opponent/evaluator

2019 **Examiner** for the PhD Defence of *Ijlal Loutfi* on "Trusted Execution on Commodity Devices" — University of Oslo (NO)

Board Member of University Associations

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)

Popular Science Presentations

2020 **Invited Speaker** at 'AI, digitalisering och integritet – vad får vi för vår hälsodata?' — Lund (SE)
2018 **Invited Speaker** at Göteborgs Vetenskapsfestivalen — Gothenburg (SE)

Conference - Workshop Organisation

2021 Member of the **Program Committee** of ACISP-2021 — Perth (AU)
2018 Member of the **Local and Organising Committee** of CANS-2018 — Naples (IT)

(Sub)Reviewer

Journals: Computer Journal, IET Information Security, IEEE Comm. Letters.
Conferences: SCN20, CCS19, AsiaCrypt19, POST18, iFM17, IndoCrypt16, ESORICS16, Infocom15.

Supervision of PhD Students

2020 - 2022 **Joakim Brorsson** topic: *Privacy Enhancing Technologies* (main supervisor M. Hell) — Lund University (SE)
2020 - 2025 **Rohon Kundu** topic: *Fully Homomorphic Encryption from Number Theoretic Assumptions* (M. Hell) — Lund University (SE)
2020 - 2022 **Hadi Sehat** topic: *Efficient & Private Cloud Storage Solutions* (D. Lucani) — Aarhus University (DK)
2019 - 2024 **Ivan Oleynikov** topic: *Privacy-Preserving Location Proximity Testing* (A. Sabelfeld) — Chalmers (SE)

Main, Recent Publications

IEEE ICC	Sehat, Lucani, and Pagnin, *"Yggdrasil: Privacy-Aware Dual Deduplication in Multi Client Settings"*, 2021.
SCN	Lucani, Nielsen, Orlandi, Pagnin, and Vestergaard, *"Secure Generalized Deduplication via Multi-Key Revealing Encryption"*, 2020.
ESORICS	Oleynikov, Pagnin, and Sabelfeld, *"Where Are You Bob? Privacy-Preserving Proximity Testing with a Napping Party"*, 2020.
IET IS	Fiore, Mitrokotsa, Nizzardo, and Pagnin, *"Multi-key Homomorphic Authenticators"*, 2019.
LatinCrypt	Aranha and Pagnin, *"The Simplest Multi-key Linearly Homomorphic Signature Scheme"*, 2019.
EuroS&P	Blazy, Bossuat, Bultel, Fouque, Onete, and Pagnin, *"SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting"*, 2019.
SCN	Fiore and Pagnin, *"Matrioska: A Compiler for Multi-key Homomorphic Signatures"*, 2018.

Teaching Experience

2016-2017	**Lecturer and Instructor** for the Master level course *Advanced Web Security* (EITN41, 7.5hp)	Lund University (SE)
2020-*now*	**Supervisor of Master Theses Projects** Anton Jeppsson *Private Set Intersection via Fully Homorphic 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 *Verifable 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)	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)