MIA FILIĆ

Doctorate student

@ mfilic@ethz.ch @ filicmia@gmail.com Zürich, Switzerland

EDUCATION

Doctorate student

Applied cryptography group, ETH Zürich

Sep 2019 – present | Zürich, Switzerland

- Research focus: probabilistic data structures under adversaries, partially funded by Microsoft Swiss Joint Research Center
- BSc and MSc thesis mentor: Daniel Patrick Frey, Filip Dobrosavljević, Philipp Engljähringer, Ella Kummer, Jonas Hofmann
- Teaching assistant: Linear algebra, Applied cryptography (coordinator)

Master of computer science and mathematics

University of Zagreb

Sep 2015 – Sep 2017 | Zagreb, Croatia

- Master thesis: Analysis of the position estimation procedure based on given GNSS pseudoranges in a GNSS SDR receiver
- Semester abroad: University of Ljubljana, Slovenia
- Prizes: 2019 URSI AP-RASC Student paper competition award, 2018 URSI Young researcher award, Sandoz Croatia scholarship for master's studies

Bachelor of mathematics

University of Zagreb

Sep 2012 – Sep 2015 | Zagreb, Croatia

- Prizes: Sandoz Croatia scholarship for undergraduate studies

RECENT PAPERS

Privacy implications of AMQ-based PQ TLS authentication

D. Francolla, M. Filić, S. Veitch | CoNEXT 2024; https://dl.acm.org/doi/10.1145/3680121.3697813

A Formal Treatment of Key Transparency Systems with Scalability Improvements

N. Brandt, M. Filić, S. A. Markelon | under submission

Probabilistic Data Structures in the Wild

M. Filić, J. Hofmann, S. A. Markelon, K. G. Paterson, A. Unnikrishnan | https://eprint.iacr.org/2024/1312

Deletions and Dishonesty: Probabilistic Data Structures in Adversarial Settings

M. Filić, K. Kocher, E. Kummer, A. Unnikrishnan | AsiaCrypt 2024; https://eprint.iacr.org/2024/1911

Compact Frequency Estimators in Adversarial Environments

S. A. Markelon, M. Filić, T. Shrimpton | ACM CCS 2023; https://eprint.iacr.org/2023/1366

Adversarial Correctness and Privacy for Probabilistic Data Structures

M. Filić, K. G. Paterson, A. Unnikrishnan, F. Virdia | ACM CCS 2022; https://eprint.iacr.org/2022/1186

TALKS & EVENTS

Deletions and Dishonesty: Probabilistic Data Structures in Adversarial Settings

Mia Filić

Dec 12th 2024 | Asiacrypt @ Kolkata, India

Cryptographic Vulnerabilities and How To Find Them

Kien Tuong Truong, Mia Filić

June 4th 2024 | RWC Summer School on real-world crypto and privacy 2024 @ Vodice, Croatia

Probabilistic Data Structures in Adversarial Settings

Mia Filić

Apr 10th 2024 | Swiss Joint Research Centre | Spring Workshop 2024 @ Zürich, CH

Compact Frequency Estimators in Adversarial Environments

Mia Filić

Mar 27th 2024 | RWC 2024 @ Toronto, CA

Compact Frequency Estimators in Adversarial Environments

Mia Filić

Feb 28th 2024 | FU Berlin Cybersecurity & AI seminar

Adversarial Correctness and Privacy for Probabilistic Data Structures

Mia Filić

Nov 9th 2022 — ACM CCS 2022 @ Los Angeles, USA

Adversarial Correctness and Privacy for Probabilistic Data Structures

Mia Filić, Anu Unnikrishnan

Nov 4th 2022 — Stanford Security Seminar

Understanding the Security of Probabilistic Data Structures under Adversarial Conditions

Mia Filić

Mar 29th 2022 — Swiss Joint Research Center | Workshop 2022 @ Lausanne, CH

EXPERIENCE

Cryptography intern

HP Inc.

Jul 2024 – Dec 2024 — Bristol, UK

Scientific Assistant/Doctorate student

Applied cryptography group, ETH Zürich

Sep 2022 – present — Zürich, CH

Scientific Assistant

Applied cryptography group, ETH Zürich

Sep 2019 – Aug 2022 — Zürich, CH

Research visit

Department of Computer and Information Science and Engineering, University of Florida

Sep 2022 – Jan 2023 — Gainesville, FL, USA

Independent and collaborative research in the area of secure probabilistic data structures: (i) exploration of new security notions, (ii) analysis of the security properties of existing data structures, and (iii) development of new structures that remain compact while providing better overall security guarantees. Collaborators: Dr. Thomas Shrimpton, Sam A. Markelon

Independent researcher

Remote

Aug 2016 – Sep 2019 — Remote

Project leader and participant in projects on: (i) analysis and extension of existing position estimation methods; (ii) mathematical methods for anomaly detection in weather-related degradation of GNSS positioning performance, and GNSS spoofing.

Teaching assistant

University of Ljubljana

Oct 2018 – Aug 2019 — Ljubljana, Slovenia

Research focus: Cryptography; TA for Web programming, Algorithms, Software engineering

Researcher

University of Zagreb

Mar 2018 – Sep 2018 — Zagreb, Croatia

Design of self-managing system for corn cultivation (Python)

Software developer

Armone (start-up)

Jul 2017 – Mar 2018 — Zagreb, Croatia

Design and implementation of communication process between robotic arm and raspberry pi (C/C++); voluntary work

External lecturer

University of Rijeka

Sep 2017 – Feb 2018 — Rijeka, Croatia

Research focus: Location Intelligence; Co-lecturer and TA for Location Intelligence/Location-Based Services course; Co-advisor for seminars and MSc thesis

Student assistant

Ericsson Nikola Tesla

Jul 2016 – Sep 2016 — Zagreb, Croatia

Spatial data analysis and modelling (R); Software development

SUMMER SCHOOLS

- RWC Summer School on real-world crypto and privacy 2019,2023,2024; Vodice, Croatia
- IACR Summer School in Post-Quantum Cryptography 2022, Budapest, Hungary
- IACR-CROSSING School on Combinatorial Techniques in Cryptography, 2022, Valletta, Malta

OTHER

- Languages: English (fluent), Croatian (native), German (intermediate)
- Selected publications prior 2019 (non-crypto and -security):
  - Anatomy of Origin-Destination Matrix derived from GNSS alternatives, R. Filjar, M. Filić, A. Lucić, K. Vidović, D. Šarić, Coordinates Oct 2018.
  - Modelling the Connection between GNSS Positioning Performance Degradation, and Space Weather and Ionospheric Conditions using RReliefF Features Selection, M. Filić, R. Filjar, ION GNSS+ 2018.
  - On development of the forecasting model of GNSS positioning performance degradation due to space weather and ionospheric conditions, M. Filić, URSI AT-RASC 2018.

  For the complete list of publications check Google Scholar.
- Sub-reviewer: CT-RSA 2020, CRYPTO 2020, CRYPTO 2020
- Coding: Python, R, C, Java, Javascript