Nikolas Melissaris

Aarhus University
Bldg. 5335 - Room 278
Aabogade 34
DK-8200 Aarhus N

nikolasm@gmail.com
https://nikolasmelissaris.github.io/
Skype: nikolas.asteri
Phone: +45 42 45 35 93

Research Interests

Combinatorics, Secure Multiparty Computation,
Privacy preserving Machine Learning, and Foundational problems in Cryptography

Education

(Current) **Aarhus University**
PhD Student
Advisor: Peter Scholl
Co-advisor: Claudio Orlandi

Rutgers University
MSc, Information Technology
GPA: 3.97/4

School of Applied Mathematics and Physical Sciences,
National Technical University of Athens
BSc and MSc, Applied Mathematics
Majors: Computer Science, Probability/Statistics

Diploma Theses

"The concrete security of practical cryptographic constructions",
Advisor: Associate Professor Periklis Papakonstantinou, Rutgers University
Survey on the security of cryptographic constructions in the information theoretic setting.

"Mathematical Attacks on RSA"
Advisor: Assistant Professor Petros Stefaneas, NTUA
Implementation of attacks on the RSA cryptosystem.

Research

Institut de Recherche en Informatique Fondamentale, Paris
Research Visit, Spring 2024
Host: Geoffroy Couteau

JP Morgan - AlgoCRYPT group, New York City
Research Intern, Summer 2023
Advisors: Antigoni Polychroniadou and Daniel Escudero.
Privacy Preserving Vertical Federated Learning for Gradient Boosted Decision Trees.

Capital Fund Management, New York City
Research Intern, Summer 2021
Performance of clustering techniques on stock returns.

MadHive Inc, New York City
Research Assistant, Summer 2019
Using cryptography to ensure integrity and detect fraud in AdTech technologies.

Computer Security Lab, University of California at Santa Barbara
Research Assistant, Summer 2015
Advisors: Professors Christopher Kruegel and Giovanni Vigna.
Armoring Android mobile devices against fake location signals.

Teaching

Computer Science Dept., Aarhus University
Teaching Assistant, Cryptology, Fall 2023
Teaching Assistant, Computability and Logic, Spring 2023
Teaching Assistant, Cryptology, Fall 2022
Teaching Assistant, Optimization, Spring 2022

MSIS Dept., Rutgers University
Teaching Assistant, Information Security, Fall 2020, Spring 2021
Instructor, Management Information Science, Summer 2020
Teaching Assistant, Business Data Management, Spring 2020
Teaching Assistant, Fundamentals of Optimization (Graduate), 2019
Teaching Assistant, Statistics, 2019

School of Professional Studies, Columbia University.
Instructor, Introduction to Programming with C, Summer 2017

Mathematics Dept., NYC College of Technology
Instructor, Discrete Structures and Algorithms I, 2016
Instructor, Quantitative Reasoning, 2017

Computer Science Dept., Brooklyn College
Instructor, Intro to Computer Applications, 2016

Computer Science Dept., Borough of Manhattan Community College
Instructor, Principles in Information Science and Computing, 2016

Work Experience

Linux System Administrator
The Graduate Center, CUNY, New York, 2015-2016
Supervisors: Gary Kettner, Lihua Wang
Maintaining (patching, upgrading, monitoring, securing) all the Linux servers

of the school, migrations to newer technologies, in addition to threat response.

Software Engineer
Icehole Games, Athens, 2014-2015
Supervisor: Konstantinos Chatzopoulos
Building web crawlers and scrapers to collect 15 years of basketball statistics from leagues around the world for the critically acclaimed game "World Basketball Manager".

Awards and Fellowships

Summer Research Award
Rutgers University
2019, 2020

Languages and Skills

Greek (native), English (proficient), German (intermediate)
Python, R, JavaScript, MATLAB, LaTeX, Mathematica

Publications

4. Dung Bui, Geoffroy Couteau, and Nikolas Melissaris. Structured-Seed Local Pseudorandom Generators and their Applications. `https://eprint.iacr.org/2024/1027.pdf`
3. Carsten Baum, Nikolas Melissaris, Rahul Rachuri, and Peter Scholl. Cheater Identification on a Budget: MPC with Identifiable Abort from Pairwise MACs. CRYPTO 2024
2. Nikolas Melissaris, Divya Ravi, and Sophia Yakoubov. Threshold-optimal MPC with Friends and Foes. INDOCRYPT 2023
1. Pei Peng, Nikolas Melissaris, Emina Soljanin, Bill Lee, Anton Maliev, and Huafeng Fan. Straggling for covert message passing on complete graphs. Allerton 2019

Manuscripts

2. Daniel Escudero, Nikolas Melissaris, and Antigoni Polychroniadou. Privacy Preserving Vertical Federated Learning for Gradient Boosted Decision Trees.
1. Nikolas Melissaris and Antigoni Polychroniadou. Agreeing on the same Neural Network after compressing on different data.