Nikolas Melissaris

IRIF, Université Paris-Cité
Sophie Germain - Room: 4058
8 Pl. Aurélie Nemours
75013 Paris

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

Research Interests

Multiparty Computation, Privacy Preserving Machine Learning, Combinatorics, Theory of Computation

Employment History

IRIF, CNRS & Université Paris-Cité
Postdoctoral Researcher, *hosted by Geoffroy Couteau*

Education

Aarhus University
PhD, Computer Science
Thesis - Better, Faster, Stronger:
Improving Security, Efficiency, and Primitives for MPC
Advisors: Peter Scholl, Claudio Orlandi

Rutgers University
MSc, Information Technology

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

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 Machine 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

Awards and Fellowships

Stibofonden - $7k
2023
Summer Research Award, Rutgers University - $3k
2019, 2020

Community Service

Subreviewer (various years) for CRYPTO, EUROCRYPT, ASIACRYPT, TCC

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. Geoffroy Couteau, Alexandrer Koch, Nikolas Melissaris, Sacha Servan-Schreiber, and Peter Scholl. Compressing Pseudorandom Permutations.

1. Daniel Escudero, Nikolas Melissaris, Antigoni Polychroniadou, and Akira Takahashi. Zero Knowledge Proof of Training for Decision Trees.