Nikolas Melissaris

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

✉ nikolasm@gmail.com
🔗 nikolasmelissaris.github.io
📱 Phone: +33 7 75 75 53 83

Employment

IRIF, CNRS & Université Paris-Cité · *Paris, France* 2025–Present
Postdoctoral Researcher, *hosted by Geoffroy Couteau*

Education

Aarhus University · *Aarhus, Denmark* 2021–2025
PhD in Computer Science
Thesis: Better, Faster, Stronger: Improving Security, Efficiency, and Primitives for MPC [pdf]
Advisors: Peter Scholl, Claudio Orlandi

Rutgers – The State University of New Jersey · *New Jersey, USA* 2017–2021
MSc in Information Technology

National Technical University of Athens · *Athens, Greece* 2009–2015
BSc & MSc in Applied Mathematics
Majors: Discrete Mathematics, Probability and Statistics

Note: Between 2004-2009 I pursued a career in professional basketball which ended abruptly. Between 2015-2017 I worked as a lecturer in various universities in New York City (see Teaching section). In 2017 I started my PhD at Rutgers University but had to eventually quit after a switch in research interests.

Research Experience

Institut de Recherche en Informatique Fondamentale · *Paris, France* Spring '24
Research Visit, *hosted by Geoffroy Couteau*

JP Morgan, AlgoCRYPT Group · *New York City, USA* Summer '23
Research Intern – Privacy-preserving ML

Capital Fund Management · *New York City, USA* Summer '21
Research Intern – Clustering methods for financial time series

MadHive Inc. · *New York City, USA* Summer '19
Research Assistant – Cryptographic integrity for AdTech

UC Santa Barbara, Computer Security Lab · *Santa Barbara, USA* Summer '15
Research Assistant – Android GPS spoofing defense

Teaching

Instructor

Institution	Term	Hours	Course · Students
ESILV Paris	Fall '25	8	Zero-Knowledge Proofs [link] · 12
Rutgers University	Summer '20	40	Management Information Systems · 30
Columbia University	Summer '17	55	Introduction to Programming with C · 25
Borough of Manhattan Community College	Spring '17	38	Principles in Information Science and Computing [link] · 20
NYC College of Technology	Spring '17	38	Quantitative Reasoning [link] · 25
	Fall '16	50	Discrete Structures and Algorithms I [link] · 20
Brooklyn College	Fall '16	38	Intro to Computer Applications [link] · 30
	Spring '17	38	

Teaching Assistant

Institution	Term	Hours	Course · Students
Aarhus University	Fall '23	15	Cryptology · 25
	Fall '22	15	
	Spring '23	5	Computability and Logic · 18
	Spring '22	40	Optimization · 9
Rutgers University	Spring '21	15	Information Security · 30
	Fall '20	15	
	Fall '18	15	Database Systems · 60
	Spring '18	15	Business Data Management [link] · 120
	Spring '19	15	
	Fall '17	10	Optimization · 30
	Fall '17	10	Statistics · 30

Note: The distinction between the two tables lies in the level of responsibility. As an instructor I was solely responsible for the course, from setting the curriculum, to teaching, to office hours, to grading. As a teaching assistant the workload revolved around exercise sessions, office hours, and grading. The hours mentioned are only in-class hours, per semester, either lecturing or for exercise sessions, and do not include preparation and grading. The number of students mentioned is per semester and it refers to the group of students that I was responsible for, not (always) the whole class. I've linked to course materials where I still have them and they're mine to share. Some are lost to time and others are stuck behind institutional access I no longer have.

Academic Service

Subreviewer

CRYPTO	(2021, 2025)
EUROCRYPT	(2022, 2024, 2025, 2026)
ASIACRYPT	(2024, 2025)
TCC	(2019, 2023)
PKC	(2026)

Papers

Published

4. *Benny Applebaum, Dung Bui, Geoffroy Couteau, and Nikolas Melissaris.* Structured-Seed Local Pseudorandom Generators and their Applications. **APPROX/RANDOM 2025** [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** [pdf]

2. *Nikolas Melissaris, Divya Ravi, and Sophia Yakoubov.* Threshold-optimal MPC with Friends and Foes. **INDOCRYPT 2023** [pdf]

1. *Pei Peng, Nikolas Melissaris, Emina Soljanin, Bill Lee, Anton Maliev, and Huafeng Fan.* Straggling for Covert Message Passing on Complete Graphs. **Allerton 2019** [pdf]*

Manuscripts

4. *Diego F. Aranha and Nikolas Melissaris.* Scanning the Social Contract: Freedom, Fear, and the Limits of Technological Obedience. In Submission [pdf]

3. *Diego F. Aranha and Nikolas Melissaris.* What is Cryptography Hiding from Itself?. Cryptology ePrint Archive [pdf]

2. *Geoffroy Couteau, Alexandrer Koch, Nikolas Melissaris, Sacha Servan-Schreiber, Peter Scholl, and Xiaxi Ye.* On Compressing Non-Additive Correlations. In Submission [pdf]

1. *Nikolas Melissaris, Antigoni Polychroniadou, Akira Takahashi, Chenkai Weng, and Jiayi Xu.* ZKBoost: Zero-Knowledge Verifiable Training for XGBoost. In Submission [pdf]

Note: In cryptography (and theoretical computer science in general) the author list is alphabetical. Research in this field tends to happen in small groups of people. It becomes hard to say whose idea contributed more to what. Alphabetical ordering is a clean way to acknowledge that and default to "we all contributed," which typically reflects reality reasonably well. All publications above follow this convention, except the ones marked with an asterisk, which are published in different venues where contribution-based ordering is standard. While my research is generally made publicly available (usually via the Cryptology ePrint Archive), some manuscripts currently listed as "in submission" contain material that is sensitive with respect to the review process. For this reason, their PDFs have not yet been posted publicly, but have been made available to the committee through a private repository.

Talks

Conferences & Workshops

March 2026	Undone Computer Science · *Luxembourg, Luxembourg*
March 2026	Real World Crypto · *Taipei, Taiwan*
August 2024	CRYPTO [video] · *Santa Barbara, USA*
June 2024	Theory and Practice of MPC [video] · *Darmstadt, Germany*

Invited Talks

December 2025	Séminaire Algorithmique GREYC · [slides] · [page] · *Caen, France*
December 2025	Crypto Seminar CAPSULE · [slides] · [page] · *Rennes, France*
November 2025	Seminar INSPIRE · [slides] · *Saclay, France*
October 2025	Crypto Seminar LIRMM · [slides] · [page] · *Montpellier, France*
February 2024	AlgoComp Seminar IRIF · [slides] · [page] · *Paris, France*
September 2023	AI Research JP Morgan [slides] · *New York City, USA*
December 2022	AlgoCRYPT Seminar JP Morgan · *New York City, USA*
June 2022	Crypto Summer Day [slides] · *Aarhus, Denmark*

Science Outreach

March 2022	AU Hack [slides] · *Aarhus, Denmark*

Note: Where available, links to videos and slides are included. For invited talks, some research groups maintain public seminar pages with speaker announcements, which I've linked. Others don't publicize their seminars online or the pages are no longer available.

Awards and Honors

Stibofonden · 50,000 dkk · 2024
Rutgers Summer Research · 3,000 usd · 2019, 2020

Note: The Stibofonden grant is awarded to PhD students for extended research visits abroad. The Rutgers Summer Research Scholarship is a merit-based award granted on the basis of a submitted research proposal.