Katerina Sotiraki

sotiraki.com
aikaterini.sotiraki@yale.edu

Research Interests

My research interests lie mainly in the area of theoretical computer science. In particular, I am interested in cryptography, post-quantum cryptography, complexity theory, and secure computation.

Employment

2023–present **Assistant Professor**, *Yale University, CS*

2020–2023 **Postdoctoral Researcher**, *UC Berkeley, EECS*
- Supervisors: Alessandro Chiesa and Raluca Ada Popa

Education

2016–2020 **PhD**, *Massachusetts Institute of Technology, CSAIL*
- Thesis: New hardness results for total search problems and non-interactive lattice-based protocols
- Supervisor: Vinod Vaikuntanathan

2013–2016 **Master of Science**, *Massachusetts Institute of Technology*
- Thesis: Authentication Protocols using Trapdoored Matrices
- Supervisor: Ronald L. Rivest

2008–2013 **Diploma degree**, *National Technical University of Athens (NTUA)*
- Department: School of Applied Mathematics and Physics
- Major: Applied Mathematics
- GPA: 9.73/10 (Graduation Rank: 2nd)

Publications

The authors in all publications, except those marked with $*$, are ordered alphabetically.

Lattice-Based Succinct Arguments for NP with Polylogarithmic-Time Verification
Jonathan Bootle, Alessandro Chiesa, and Katerina Sotiraki
CRYPTO 2023 (Annual International Cryptology Conference)

HOLMES: Efficient Distribution Testing for Secure Collaborative Learning
$*$ *Ian Chang, Katerina Sotiraki, Weikeng Chen, Murat Kantarcioglu, and Raluca Ada Popa*
USENIX Security 2023 (USENIX Security Symposium)

Sumcheck Arguments and their Applications
Jonathan Bootle, Alessandro Chiesa, and Katerina Sotiraki
CRYPTO 2021 (Annual International Cryptology Conference)

A Topological Characterization of Modulo-p Arguments
Aris Filos-Ratsikas, Alexandros Hollender, Katerina Sotiraki, and Manolis Zampetakis
SODA 2021 (ACM-SIAM Symposium on Discrete Algorithms)

Consensus-Halving: Does it Ever Get Easier?
Aris Filos-Ratsikas, Alexandros Hollender, Katerina Sotiraki, and Manolis Zampetakis
EC 2020 (ACM Conference on Economics and Computation)

On the Complexity of Modulo-q Arguments
Mika Göös, Pritish Kamath, Katerina Sotiraki, and Manolis Zampetakis
CCC 2020 (Computational Complexity Conference)

Limits on the Efficiency of (Ring) LWE-Based Non-interactive Key Exchange
Siyao Guo, Pritish Kamath, Alon Rosen, and Katerina Sotiraki
PKC 2020 (Conference on Practice and Theory of Public Key Cryptography)
invited to the Journal of Cryptology

Privately Computing Set-Maximal Matches In Genomic Data
∗ *Katerina Sotiraki, Esha Ghosh, and Hao Chen*
BMC Medical Genomics 2020
winning solution of iDASH competition 2018

Towards Non-Interactive Zero-Knowledge from LWE
Ron Rothblum, Adam Sealfon, and Katerina Sotiraki
PKC 2019 (Conference on Practice and Theory of Public Key Cryptography)
invited to the Journal of Cryptology

PPP-completeness with Connections to Cryptography
Katerina Sotiraki, Manolis Zampetakis, and Giorgos Zirdelis
FOCS 2018 (Annual IEEE Symposium on Foundations of Computer Science)

Agreement in Partitioned Dynamic Networks
Adam Sealfon and Katerina Sotiraki
DISC 2014 (International Symposium on Distributed Computing)

Occupational fraud detection through visualization
Evmorfia N. Argyriou, Katerina Sotiraki, and Antonios Symvonis
ISI 2013 (IEEE Intelligence and Security Informatics)

Implementation Projects

HOLMES: Efficient Distribution Testing for Secure Collaborative Learning
Weikeng Chen, Katerina Sotiraki, Ian Chang, Murat Kantarcioglu, and Raluca Popa
github: `https://github.com/holmes-inputcheck/`

Privately Training Classifiers for Genomic Data
Schuyler Rosefield, Katerina Sotiraki, Emily Chen, Noah Luther, and Vinod Vaikuntanathan
among top-performing solutions of iDASH competition 2019

Privately Computing Set-Maximal Matches In Genomic Data
Katerina Sotiraki, Esha Ghosh, and Hao Chen
winning solution of iDASH competition 2018

Program Committees

- TCC'22
- PPML at CRYPTO'23

Teaching Experience

I was a teaching assistant in the following courses.

Fall 2018 **6.852 Distributed Algorithms**, *Instructor: Nancy Lynch*
TA Evaluation: 7.0/7.0 (median)

Spring 2016 **6.064 Introduction to Algorithms**, *Instructors: Constantinos Daskalakis, Stefanie Jegelka, Vinod Vaikuntanathan*
TA Evaluation: 6.0/7.0 (median)

Fall 2015 **6.852 Distributed Algorithms**, *Instructor: Nancy Lynch*
TA Evaluation: 7.0/7.0 (median)

Spring 2015 **6.857 Computer and Network Security**, *Instructor: Ronald L. Rivest*
TA Evaluation: 5.0/7.0 (median)