Dimitris Kolonelos

dimitris.kolonelos@imdea.org

INTERESTS

Various cryptographic topics: Succinct Primitives, Zero-Knowledge Proofs, Lattice-based Cryptography, Blockchain Applications, Public-key Cryptography.

EDUCATION

PhD in Computer Science *February 2019 - present*
IMDEA Software Institute & Universidad Politecnica de Madrid, Spain
Advisor: Dario Fiore
Work on: *Succinct & Verifiable Cryptographic Primitives for large-scale applications.*

MEng Electrical and Computer Engineering (5-year) *Sept 2011 - Jul 2018*
National Technical University of Athens (NTUA), Greece

- GPA: 8.12/10.00
- Thesis: ”Anonymous Digital Survey Systems and Cryptographic Ring Signatures”
  Advisor: Aris Pagourtzis

RESEARCH EXPERIENCE

Research intern *April 2021 - August 2021*
Ethereum Foundation
Advisor: Mary Maller
Work on: *Zero-Knowledge Proofs over highly untrusted settings (subverted RSA groups).*

Research intern *September 2018 - February 2019*
IMDEA Software Institute
Advisor: Dario Fiore
Work on: *Efficient Zero-Knowledge Proofs for privacy-preserving applications.*

Undergraduate Research Assistant *September 2017 - July 2018*
NTUA Computation and Reasoning labatory (Corelab)
Advisor: Aris Pagourtzis
Work on: *Anonymous Survey Systems through cryptographic techniques. Improving privacy of 'Anonize', an existing anonymous survey system.*

SHORT VISITS

Max Planck Institute for Security and Privacy (MPI-SP), Bochum (February 2022)
Host: Giulio Malavolta

Microsoft Research, Redmond (November 2022)
Host: Melissa Chase & Esha Ghosh

AWARDS

Protocol Labs research gift: award of one-year PhD funding (September 2019 - August 2020)

PUBLICATIONS

Efficient Registration-Based Encryption
Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, Ahmadreza Rahimi
Preprint

Efficient Laconic Cryptography from Learning With Errors
Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta,

Ahmadreza Rahimi
To appear at EUROCRYPT 2023

Zero-Knowledge Arguments for Subverted RSA Groups
Dimitris Kolonelos, Mary Maller, Mikhail Volkhov
To appear at PKC 2023

Succinct Zero-Knowledge Batch Proofs for RSA Accumulators
Matteo Campanelli, Dario Fiore, Semin Han, Jihye Kim, Dimitris Kolonelos, Hyunok Oh
ACM CCS 2022

Ring Signatures with User-Controlled Linkability
Dario Fiore, Lydia Garms, Dimitris Kolonelos, Claudio Soriente, Ida Tucker
ESORICS 2022

Inner Product Functional Commitments with Constant-Size Public Parameters and Openings
Hien Chu, Dario Fiore, Dimitris Kolonelos, Dominique Schröder
SCN 2022

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan, Dimitris Kolonelos
Financial Cryptography and Data Security 2021

Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage
Matteo Campanelli, Dario Fiore, Nicola Greco, Dimitris Kolonelos, Luca Nizzardo
ASIACRYPT 2020

TALKS

Succinct Zero-Knowledge Batch Proofs for RSA Accumulators
Microsoft Research, Redmond, November 2022

Succinct Zero-Knowledge Batch Proofs for RSA Accumulators
Crypto Economics Security Conference (CESC) 2022, Berkeley, October 2022

Succinct Cryptographic primitives with applications to the Blockchain
Cybersecurity Research Network meeting, Lleida, March 2022

SoK - Vector Commitments
Ethereum Foundation, Online, June 2021

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
Financial Cryptography and Data Security 2021, Online, March 2021

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
Monash Cybersecurity Seminars, Online, February 2021

Incrementally Aggregatable Vector Commitments and Applications to Verifiable De-

centralized Storage
Asiacrypt 2020, Online, December 2020

Incrementally Aggregatable Vector Commitments and Applications to Verifiable Decentralized Storage
Protocol Labs Research Seminar Series, Online, November 2020

Vector Commitment Techniques and Applications to Verifiable Decentralized Storage
Theory and Practice of Blockchains (TPBC) 2020, Online, July 2020

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
Theory and Practice of Blockchains (TPBC) 2020, Online, June 2020

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular
Crypto Economics Security Conference (CESC) 2019, Berkeley, October 2019

SERVICE

External Reviews: EUROCRYPT 2023, CRYPTO 2022, PKC 2021, ASIACRYPT 2021, EUROCRYPT 2021, Financial Cryptography 2021, ACM CCS 2020, PKC 2020

SCHOOLS ATTENDED

Lattices: Algorithms, Complexity, and Cryptography Boot Camp
Simons Institute for the Theory of Computing, Berkeley, January 2020

COMPUTING SKILLS

Programming Languages: C/C++, Java, ML, MySQL
Tools: Matlab, Latex, Git
Operating Systems: MacOS, Linux, Windows

LANGUAGES

Greek (native), English (Proficiency), Spanish