

Dimitris Kolonelos

Contact: dimitriskolonelos@gmail.com, dimitris.kolonelos@berkeley.edu

Website: <https://dimkolonelos.github.io/>

INTERESTS Cryptography, Privacy-Enhancing Technologies, Succinct Zero-Knowledge Proofs, Advanced Encryption Schemes, Blockchain Applications.

EXPERIENCE **Postdoc** *September 2024 - now*
UC Berkeley
Host: Sanjam Garg

Visiting Scholar *June 2023 - July 2023*
UC Berkeley
Host: Sanjam Garg
Work on: *SNARKs, Threshold Encryption.*

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

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

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

EDUCATION **PhD in Computer Science** *February 2019 - February 2024*
IMDEA Software Institute & Universidad Politécnica de Madrid, Spain
Advisor: Dario Fiore
Thesis: *Succinct Cryptographic Commitments with Fine-Grained Openings for Decentralized Environments.*

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

SHORT VISITS IMDEA Software Institute (September 2025)
Host: Dario Fiore

Bocconi University (August 2025)
Host: Giulio Malavolta

The Chinese University of Hong Kong, Hong Kong (December 2023)
Host: Sherman S. M. Chow

IRIF, Paris (November 2023)
Host: Geoffroy Couteau

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

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

AWARDS

UPM Extraordinary Doctoral Thesis Award 2023/2024.

Berkeley Center for Responsible, Decentralized Intelligence (RDI) Fellowship. (February 2025 - April 2025)

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

PUBLICATIONS **Note: All publication are ordered alphabetically.**

Lighthouse: Single-Server Secure Aggregation with $O(1)$ Server-Committee Communication at Scale

Sanjam Garg, Alireza Kavousi, Dimitris Kolonelos, Erkan Tairi, Zhipeng Wang
Preprint

BABE: Verifying Proofs on Bitcoin Made 1000x Cheaper

Sanjam Garg, Dimitris Kolonelos, Mikhail Sergeevitch, Srivatsan Sridhar, David Tse
ACM CCS 2026– Core A*

Jigsaw: Doubly Private Smart Contracts

Sanjam Garg, Aarushi Goel, Dimitris Kolonelos, Rohit Sinha
IEEE S&P 2026 – Core A*

A Framework for Witness Encryption from Linearly Verifiable SNARKs and Applications

Sanjam Garg, Mohammad Hajiabadi, Dimitris Kolonelos, Abhiram Kothapalli, Guru-Vamsi Policharla

CRYPTO 2025– Core A*

Split Prover Zero-Knowledge SNARKs

Sanjam Garg, Aarushi Goel, Dimitris Kolonelos, Sina Shiehian, Rohit Sinha

PKC 2025– Core B

Threshold Encryption with Silent Setup

Sanjam Garg, Dimitris Kolonelos, Guru-Vamsi Policharla, Mingyuan Wang

CRYPTO 2024– Core A*

Zero-Knowledge Proofs for Set Membership: Efficient, Succinct, Modular

Daniel Benarroch, Matteo Campanelli, Dario Fiore, Kobi Gurkan, Dimitris Kolonelos

Designs, Codes and Cryptography, Volume 91 – SJR Q1

Cuckoo Commitments: Registration-Based Encryption and Key-Value Map Commitments for Large Spaces

Dario Fiore, Dimitris Kolonelos, Paola de Perthuis

ASIACRYPT 2023– Core A

Distributed Broadcast Encryption from Bilinear Groups
Dimitris Kolonelos, Giulio Malavolta, Hoeteck Wee
ASIACRYPT 2023– Core A

Efficient Registration-Based Encryption
Noemi Glaeser, Dimitris Kolonelos, Giulio Malavolta, Ahmadreza Rahimi
ACM CCS 2023– Core A*

Efficient Laconic Cryptography from Learning With Errors
Nico Döttling, Dimitris Kolonelos, Russell W. F. Lai, Chuanwei Lin, Giulio Malavolta, Ahmadreza Rahimi
EUROCRYPT 2023– Core A*

Zero-Knowledge Arguments for Subverted RSA Groups
Dimitris Kolonelos, Mary Maller, Mikhail Volkhov
PKC 2023– Core B

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

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

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

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– Core A

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

TALKS

Jigsaw: Doubly Private Smart Contracts
IOG Seminar, Online, October 2025

Jigsaw: Doubly Private Smart Contracts
IMDEA Software Institute, Madrid, September 2025

Threshold Encryption with Silent Setu
Bocconi University, Milan, August 2025

Jigsaw: Doubly Private Smart Contracts
The Science of Blockchain Conference 2025 (SBC 2025), Berkeley, August 2025

Jigsaw: Doubly Private Smart Contracts
Lagrange Science Fair, Online, August 2025

Jigsaw: Doubly Private Smart Contracts
o1Labs Reading Group, Online, July 2025

Split Prover Zero-Knowledge SNARKs
Public Key Cryptography 2025, Roros, May 2025

Jigsaw: Doubly Private Smart Contracts
Workshop on Cryptographic Tools for Blockchains, Madrid, May 2025

Jigsaw: Doubly Private Smart Contracts
Bay Area Crypto Day, Sunnyvale, April 2025

Beyond Garbling: Efficient Advanced Encryption Schemes without Trusted Authority
Eurocrypt 2024 Workshops: Theory and Practice of Laconic Cryptography, Zurich, May 2024

Registration-Based Encryption: How to build it without garbling
The Chinese University of Hong Kong, Hong Kong, December 2023

Distributed Broadcast Encryption from Bilinear Groups
Asiacrypt 2023, Guangzhou, December 2023

Cuckoo Commitments: Registration-Based Encryption and Key-Value Map Commitments for Large Spaces
Asiacrypt 2023, Guangzhou, December 2023

Efficient Registration-Based Encryption
ACM CCS 2023, Copenhagen, November 2023

Registration-Based Encryption: How to build it without garbling
IRIF Crypto Reading Group, Paris, November 2023

Distributed Broadcast Encryption from Bilinear Groups
Stanford Security Seminar, Palo Alto, August 2023

Distributed Broadcast Encryption from Bilinear Groups
UC Berkeley Cryptography Seminars, Berkeley, June 2023

Zero-Knowledge Arguments for Subverted RSA Groups
Public Key Cryptography 2023, Atlanta, May 2023

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 Decentralized 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

Program Committees: ACM CCS 2026, Usenix Security 2026, IEEE S&P 2026, ACM CCS 2025

External Reviews: CRYPTO 2026, EUROCRYPT 2026, TCC 2025, CRYPTO 2025, EUROCRYPT 2025, TCC 2024, ASIACRYPT 2024, CRYPTO 2024, EUROCRYPT 2024, TCC 2023, ASIACRYPT 2023, EUROCRYPT 2023, ACNS 2023, CRYPTO 2022, PKC 2021, ASIACRYPT 2021, EUROCRYPT 2021, FC 2021, ACM CCS 2020, PKC 2020

LANGUAGES

Greek (native), English (Proficiency), Spanish