

# Dimitris Kolonelos

---

dimitriskolonelos@gmail.com

**INTERESTS** Succinct Cryptographic Primitives, Zero-Knowledge Proofs, Authenticated Data Structures, Advanced Public-key Encryption, Blockchain Applications.

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

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

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

**PUBLICATIONS** *Threshold Encryption with Silent Setup*  
Sanjam Garg, Dimitris Kolonelos, Guru-Vamsi Policharla, Mingyuan Wang  
CRYPTO 2024

*Cuckoo Commitments: Registration-Based Encryption and Key-Value Map Commitments for Large Spaces*  
Dario Fiore, Dimitris Kolonelos, Paola de Perthuis  
ASIACRYPT 2023

*Distributed Broadcast Encryption from Bilinear Groups*  
Dimitris Kolonelos, Giulio Malavolta, Hoeteck Wee  
ASIACRYPT 2023

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

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

*Zero-Knowledge Arguments for Subverted RSA Groups*  
Dimitris Kolonelos, Mary Maller, Mikhail Volkhov  
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

*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**

**External Reviews:** 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