Dimitrios Papadopoulos

Associate Professor
Department of Computer Science & Engineering
Hong Kong University of Science & Technology
e-mail: dipapado@cse.ust.hk webpage: https://www.cse.ust.hk/~dipapado/

A. Education

09/2011 – 06/2016	PhD in Computer Science Department of Computer Science, Boston University, USA *Thesis: Function-specific schemes for Verifiable Computation* *Thesis Advisor: Nikos Triandopoulos*
09/2003 – 09/2010	Diploma in Applied Mathematics School of Applied Mathematics and Natural Sciences, National Technical University of Athens, Greece

B. Employment

07/2023 – Present	Associate Professor Department of Computer Science & Engineering, HKUST
02/2017 – 06/2023	Assistant Professor Department of Computer Science & Engineering, HKUST
06/2024 – Present	Senior Research Scientist (Consultancy) Lagrange Labs Inc.
07/2016 – 01/2017	Post-Doctoral Researcher University of Maryland Institute for Advanced Computer Studies

C. Funded Projects

1. *PI:* Zero-Knowledge Proofs with Offline/Online Provers: Applications to Efficient Zero-Knowledge Dictionaries and Beyond. *Hong Kong RGC General Research Fund* 16200721 (HK$838,393; 2022-2024)
2. *PI:* Private Smart Contracts Evaluation using Efficient Zero-knowledge Proofs. *Hong Kong RGC Early Career Scheme* 26208318 (HK$800,000; 2019-2021)
3. *PI:* Efficient zkDEX – Perpetuals based on new zero-knowledge techniques. OKX Exchange (HK$780,000; 2024-2025)
4. *PI:* Honest Maximum Extractable Value for Ethereum Block Builders. Ethereum Foundation (HK$227,284; 2024-2026)
5. *PI:* Verifiable Time-lock puzzles and their Applications in Blockchains. SUI Foundation Research Award (HK$194,592; 2025-2029)
6. *PI:* AUTI: A Verifiable and Privacy-Preserving Auditing Platform. *HKUST-Kaisa Joint Research Institute Seed Fund* (HK$627,000; 2021-2022)
7. *PI:* Developing Blockchain-friendly Cryptographic Tools for Private Verifiable Queries. *HUAWEI Innovation Research Program OPEN 2018* (HK$390,000; 2019-2020)
8. *Co-PI:* Security-minded CDE for Building Data Management Using Distributed Ledger Technology. *ITC Innovation and Technology Fund* (HKD$7,799,471.71; 2021-2023)
9. *Co-PI:* Federated Learning at Scale: Systems, Security and Applications. *WeBank-HKUST Joint Lab Project* (HK$2,243,107; 2019-2021)
10. *CI:* Adaptive VCBF and Applications to Proof of Space. *Protocol Labs Research Donation* (US$50,000, 2022)

D. Publications (Convention: graduate advisees are underlined; interns and visiting student advisees are in italics; (*) denotes authors are in alphabetical order; my PhD advisor is marked with †)

Referred Papers in Conferences

1. Christodoulos Pappas, **Dimitrios Papadopoulos**: Hobbit: Space-Efficient zkSNARK with Optimal Prover Time, *USENIX Security Symposium 2025*
2. Christodoulos Pappas, **Dimitrios Papadopoulos**, Charalampos Papamanthou: HydraProofs: Optimally Computing All Proofs in a Vector Commitment (with applications to efficient zkSNARKs over data from multiple users), *IEEE Symposium on Security and Privacy (Oakland) 2025*
3. Jiajun Xin, **Dimitrios Papadopoulos**: “Check-Before-you-Solve”: Verifiable Time-lock Puzzles, *IEEE Symposium on Security and Privacy (Oakland) 2025*
4. Apostolos Mavrogiannakis, Xian Wang, Ioannis Demertzis, **Dimitrios Papadopoulos**, Minos N. Garofalakis: OBLIVIATOR: Oblivious Parallel Joins and other Operators in Shared Memory Environments. *USENIX Security Symposium 2025*
5. Christodoulos Pappas, **Dimitrios Papadopoulos**: Sparrow: Space-Efficient zkSNARK for Data-Parallel Circuits and Applications to Zero-Knowledge Decision Trees, *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2024*
6. Kasra Abbaszadeh, Christodoulos Pappas, **Dimitrios Papadopoulos**, Jonathan Katz: Zero-Knowledge Proofs of Training for Deep Neural Networks, *2024 ACM SIGSAC Conference on Computer and Communications Security (CCS) 2024*
7. Jiajun Xin, Arman Haghighi, Xiangan Tian, **Dimitrios Papadopoulos**: Notus: Dynamic Proofs of Liabilities from Zero-knowledge RSA Accumulators, *USENIX Security Symposium 2024*
8. Priyanka Mondal, Javad Ghareh Chamani, Ioannis Demertzis, **Dimitrios Papadopoulos**: I/O-Efficient Dynamic Searchable Encryption meets Forward & Backward Privacy. USENIX Security Symposium 2024
9. Nicholas Ngai, Ioannis Demertzis, Javad Ghareh Chamani, **Dimitrios Papadopoulos**: Distributed & Scalable Oblivious Sorting and Shuffling, *IEEE Symposium on Security and Privacy (Oakland) 2024*
10. Vlasis Koutsos, Xiangan Tian, **Dimitrios Papadopoulos**, Dimitris Chatzopoulos: Cross Ledger Transaction Consistency for Financial Auditing. Advances in Financial Technologies, AFT 2024: 4:1-4:25
11. Javad Ghareh Chamani, *Ioannis Demertzis*, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Rasool Jalili: “GraphOS: Towards Oblivious Graph Processing”, in *Proceedings of the VLDB Endowment (VLDB)*, 16(13): 4324-4338 (2023)
12. Vlasis Koutsos, **Dimitrios Papadopoulos**, “Publicly Auditable Functional Encryption”, in *Applied Cryptography and Network Security: 21st International Conference (ACNS 2023)*: 396-425 (2023)
13. Giuseppe Ateniese, Long Chen, Danilo Francati, **Dimitrios Papadopoulos**, Qiang Tang: “Verifiable Capacity-Bound Functions: A New Primitive from Kolmogorov Complexity - (Revisiting Space-Based Security in the Adaptive Setting),” in *Public Key Cryptography (PKC)* 2023, 2: 63-93 (2023)
14. Xiangan Tian, Vlasis Koutsos, *Lijia Wu, Yijian Wu*, **Dimitrios Papadopoulos**, "Demo: VaxPass -- A Scalable and Verifiable Platform for COVID-19 Records," in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22)*, November 2022
15. Javad Ghareh Chamani, **Dimitrios Papadopoulos**, Mohammadamin Karbasforushan, Ioannis Demertzis, “Dynamic Searchable Encryption with Optimal Search in the Presence of Deletions,” in *USENIX Security Symposium 2022*, August 2022
16. Christodoulos Pappas, **Dimitrios Papadopoulos**, Dimitris Chatzopoulos, Eleni Panagou, Spyros Lalis, Manolis Vavalis, “Towards Efficient Decentralized Federated Learning,” in *IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW) 2022*, July 2022
17. Yun Wang, **Dimitrios Papadopoulos**, “Multi-User Collusion-Resistant Searchable Encryption with Optimal Search Time,” in *Asia Conference on Computer and Communications Security (AsiaCCS) 2021*, pp. 252-264, June 2021
18. Xianrui Meng, **Dimitrios Papadopoulos**, Alina Oprea, Nikos Triandopoulos†, “Private Hierarchical Clustering and Efficient Approximation,” in *Cloud Computing Security Workshop CCSW@CCS 2021*, pp. 3-20, November 2021 (***Best Paper Award Runner-Up***)
19. *Ioannis Demertzis*, Javad Ghareh Chamani, **Dimitrios Papadopoulos**, Charalampos Papamanthou, “Dynamic Searchable Encryption with Small Client Storage,” in *Network and Distributed System Security Symposium (NDSS) 2020*, February 2020
20. *Ioannis Demertzis*, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Saurabh Shintre, “SEAL: Attack Mitigation for Encrypted Databases via Adjustable Leakage,” in *USENIX Security Symposium 2020*, pp. 2433-2450, August 2020
21. Ahmed Kosba, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Dawn Song, “MIRAGE: Succinct Arguments for Randomized Algorithms with Applications to Universal zk-SNARKs,” in *USENIX Security Symposium 2020*, pp. 2129-2146, August 2020
22. Javad Ghareh Chamani, **Dimitrios Papadopoulos**, “Mitigating Leakage in Federated Learning with Trusted Hardware,” in *Privacy Preserving Machine Learning Workshop (PriML/PPML Joint Edition) at the 34th Conference on Neural Information Processing Systems (NeurIPS 2020)*, December 2020

23. Alin Tomescu, Vivek Bhupatiraju, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Nikos Triandopoulos†, Srinivas Devadas, "Transparency Logs via Append-Only Authenticated Dictionaries," in *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2019*, pp. 1299-1316,
24. Javad Ghareh Chamani, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Rasool Jalili, "New Constructions for Forward and Backward Private Symmetric Searchable Encryption," in *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2018*, pp. 1038-1055, October 2018
25. Ioannis Demertzis, **Dimitrios Papadopoulos**, Charalampos Papamanthou. "Searchable Encryption with Optimal Locality: Achieving Sublogarithmic Read Efficiency," in *Annual International Cryptology Conference CRYPTO 2018*, Part I, pp. 371-406, August 2018
26. Yupeng Zhang, Daniel Genkin, Jonathan Katz, **Dimitrios Papadopoulos**, Charalampos Papamanthou, "vRAM: Faster Verifiable RAM with Program-Independent Preprocessing," in *IEEE Symposium on Security and Privacy (Oakland) 2018*, pp. 908-925, May 2018
27. *Christian Cachin, Esha Ghosh, **Dimitrios Papadopoulos**, Bjorn Tackmann, "Stateful Multi-client Verifiable Computation," in *Applied Cryptography and Network Security (ACNS) 2018*, pp. 637-656, 2018
28. Yupeng Zhang, Daniel Genkin, Jonathan Katz, **Dimitrios Papadopoulos**, Charalampos Papamanthou, "vSQL: Verifying arbitrary SQL queries over dynamic outsourced databases," in *IEEE Symposium on Security and Privacy (Oakland) 2017*, pp. 863–880, May 2017
29. *Foteini Baldimtsi, **Dimitrios Papadopoulos**, Stavros Papadopoulos, Alessandra Scafuro, Nikos Triandopoulos†, "Server-aided secure computation with off-line parties," in *European Symposium on Research in Computer Security (ESORICS) 2017*, Part I, pp. 103–123, September 2017
30. *Esha Ghosh, Olga Ohrimenko, **Dimitrios Papadopoulos**, Roberto Tamassia, Nikos Triandopoulos†, "Zero-knowledge accumulators and set algebra," in *International Conference on the Theory and Application of Cryptology and Information Security ASIACRYPT 2016*, Part II, pp. 67–100, December 2016
31. **Dimitrios Papadopoulos**, Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos†, "Practical authenticated pattern matching with optimal proof size," in *International Conference on Very Large Databases (VLDB) 2015*, pp. 750–761, September 2015
32. *Sharon Goldberg, Moni Naor, **Dimitrios Papadopoulos**, Leonid Reyzin, Sachin Vasant, Asaf Ziv, "NSEC5: Provably preventing DNSSEC zone enumeration," in *Network and Distributed System Security Symposium (NDSS) 2015*, February 2015
33. *Ahmed Kosba, **Dimitrios Papadopoulos**, Charalampos Papamanthou, Mahmoud Sayed, Elaine Shi, Nikos Triandopoulos†, "TRUESET: Faster verifiable set computations," in *USENIX Security Symposium 2014*, pp. 765–780, August 2014
34. **Dimitrios Papadopoulos**, S. Papadopoulos, N. Triandopoulos†, "Taking authenticated range queries to arbitrary dimensions," in *ACM SIGSAC Conference on Computer and Communications Security (CCS) 2014,* pp. 819–830, October 2014
35. *Ran Canetti, Omer Paneth, **Dimitrios Papadopoulos**, Nikos Triandopoulos†, "Verifiable set operations over outsourced databases," in *International Conference on Practice and Theory in Public-Key Cryptography (PKC) 2014*, March 2014
36. Michael A. Bekos, Michael Kaufmann, **Dimitrios Papadopoulos**, Antonios Symvonis, "Combining Traditional Map Labeling with Boundary Labeling," in *Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM) 2011*, January 2011

Refereed Journal Articles

1. Vlasis Koutsos, *Sankarshan Damle*, **Dimitrios Papadopoulos**, Sujit Gujar, Dimitris Chatzopoulos: AVeCQ: Anonymous Verifiable Crowdsourcing With Worker Qualities. *IEEE Transactions on Dependable and Secure Computing,* 22(1): 406-423 (2025)
2. Yun Wang, **Dimitrios Papadopoulos**, "Multi-User Collusion-Resistant Searchable Encryption for Cloud Storage," in *IEEE Transactions of Cloud Computing*, 11(3): 2993-3008 (2023)
3. Javad Ghareh Chamani, Yun Wang, **Dimitrios Papadopoulos**, Mingyang Zhang, Rasool Jalili, "Multi-User Dynamic Searchable Symmetric Encryption with Corrupted Participants," in *IEEE Transactions on Dependable and Secure Computing,* 20(1): 114-130 (2023)
4. Vlasis Koutsos, **Dimitrios Papadopoulos**, Dimitris Chatzopoulos, Sasu Tarkoma, Pan Hui, "Agora: a privacy-aware data marketplace," in *IEEE Transactions on Dependable and Secure Computing,* 19(6): 3728-3740 (2022).
5. Carlos Bermejo Fernandez, Dimitris Chatzopoulos, **Dimitrios Papadopoulos**, Pan Hui, "This Website Uses Nudging: MTurk Workers' Behaviour on Cookie Consent Notices," in *Proceedings of the ACM on Human-Computer Interaction (PACM-HCI),* Vol. 5, Issue CSCW2, Article 346 (2021)
6. Kewei Cheng, Tao Fan, Yilun Jin, Yang Liu, Tianjian Chen, **Dimitrios Papadopoulos**, Qiang Yang, "Secureboost: A lossless federated learning framework," in *IEEE Intelligent Systems*, Vol. 36, no. 6, (2021). (***Best Paper Award***)

7. Xuanwu Yue, Xinhuan Shu, Xinyu Zhu, Xinnan Du, Zheqing Yu, **Dimitrios Papadopoulos**, Siyuan Liu, "BitExTract: Interactive Visualization for Extracting Bitcoin Exchange Intelligence," in *IEEE Transactions on Visualization and Computer Graphics,* Vol. 25, no. 1, (2019)
8. Javad Ghareh Chamani, Mohammad Sadeq Dousti, Rasool Jalili, **Dimitrios Papadopoulos**, "SESOS: A Verifiable Searchable Outsourcing Scheme for Ordered Structured Data in Cloud Computing," in *ISC International Journal of Information Security*, Vol. 11, no. 1, (2019)
9. *Daniel Genkin, **Dimitrios Papadopoulos**, Charalampos Papamanthou. "Privacy in decentralized cryptocurrencies." *Communications of the ACM (CACM)*, Vol. 61, no. 6, (2018)

Standards Publications

1. Sharon Goldberg, Leonid Reyzin, **Dimitrios Papadopoulos,** Jan Včelák, "Verifiable Random Functions (VRFs) RFC 9381," *Internet Research Task Force (IRTF)*, *Internet Standards*, Active Internet Standard (https://datatracker.ietf.org/doc/rfc9381/)

Patents

1. Charalampos Papamanthou, Roberto Tamassia, Nikos Triandopoulos†, **Dimitrios Papadopoulos**, Edward Joseph Tremel, "Authenticated pattern matching and exact path queries," US Patent 10409845, 2019
2. **Dimitrios Papadopoulos**, Nikos Triandopoulos†, Ran Canetti, "Authenticated hierarchical set operations and applications," US Patent 9049185, 2015

E. Advising

Graduated RPg Students

1. **Jiajun XIN**, Degree: PhD (August 2025).
Thesis: Scaling Verifiable Computations with Hidden-order RSA groups
Placement: University of Sydney, Post-doctoral Research (under supervision by Prof. Qiang Tang)
2. **Javad GHAREH CHAMANI**, Degree: PhD (August 2022).
Thesis: Secure and Practical Search over Dynamic Encrypted Datasets.
Placement: Huawei Hong Kong Research Center (HKRC), Researcher
3. **Xiangan TIAN**, Degree: MPhil (January 2025).
Thesis: VEX: A zkRollup Architecture for Verifiable Exchange System
Placement: Software Engineer, BlockUp Solutions
4. **Christodoulos PAPPAS**, Degree: MPhil (August 2024).
Thesis: Pigeon: A Space-Efficient zkSNARK with Optimal Proving Time
Placement: PhD under my supervision
5. **Tai Tak Martin YIP,** Degree: MPhil (January 2023).
Thesis: An Integrated System for Privacy-Preserving, and Auditable Transactions on Hyperledger Fabric
Placement: Deloitte, Senior Cybersecurity Consultant
6. **Arman HAGHIGHI**. Degree: MPhil (August 2021).
Thesis: A Lattice-based Vector Commitment and Key-value Commitment with Homomorphic Properties
Placement: PhD under my supervision
7. **Vlasios KOUTSOS**. Degree: MPhil (August 2020).
Thesis: Design and Development of a Privacy-Aware Data Marketplace
Placement: PhD under my supervision
8. **Yun WANG** Degree MPhil: (July 2020).
Thesis: New Constructions for Multi-User Symmetric Searchable Encryption with Corrupted Parties

Current RPg Advisees

1. **Vlasios KOUTSOS**. PhD student since 2020
2. **Jiajun XIN**. PhD student since 2020
3. **Arman HAGHIGHI**. PhD student since 2021
4. **Xian WANG,** MPhil student since 2023
5. **Christodoulos PAPPAS**. PhD student since 2024
6. **Kianush ARSHI.** PhD Student since 2025
7. **Jonas BALLWEG**. PhD student since 2024 (co-supervised with Amir Goharshady)
8. **Togzhan BARAKBAYEVA**. PhD student since 2021 (co-supervised with Amir Goharshady)
9. **Zhuo CAI**. PhD student since 2022 (co-supervised with Amir Goharshady)
10. **Sergei NOVOZHILOV**. PhD student since 2022 (co-supervised with Amir Goharshady)