Ioannis (Yannis) Demertzis

Assistant Professor
Computer Science & Engineering Dept.
University of California, Santa Cruz
http://www.idemertzis.com
✉ idemertz@ucsc.edu

"My research mission is to bridge the gap between cryptography/security and real-world systems/databases by working and publishing papers in both areas; aiming to build cryptographic solutions and real systems that are simultaneously practical, efficient and provably secure."

Research Interests

Applied cryptography, computer security, secure databases and systems, secure hardware enclaves/TEEs, mitigating side channel and leakage-abuse attacks, query processing over encrypted data, searchable encryption, oblivious computation.

Professional Appointments

July 2020 – present: **Assistant Professor**, *Computer Science & Engineering*, Baskin School of Engineering, University of California, Santa Cruz.

September 2020 – August 2021: **Postdoctoral Researcher**, *Electrical Engineering & Computer Science*, University of California, Berkeley, mentor: Prof. Raluca Ada Popa.

Education

September 2015 – August 2020: **Ph.D.**, *Electrical & Computer Engineering*, University of Maryland **(UMD)**.
Dissertation: Improving Efficiency, Expressiveness and Security of Searchable Encryption
Advisor: Prof. Charalampos (Babis) Papamanthou

October 2013 – July 2015: **Master of Science**, *Electronic & Computer Engineering*, Technical University of Crete **(TUC)**, Chania, Greece.
Thesis Topic: Privacy Preserving Range Queries in Cloud Computing Environments,
Advisor: Prof. Minos Garofalakis

October 2008 – September 2013: **Diploma (5-year program)**, *Electronic & Computer Engineering*, Technical University of Crete **(TUC)**, Chania, Greece.
Thesis Topic: Private Data Analytics in Cloud Computing Environments,
Advisor: Prof. Minos Garofalakis

Research & Work Experience

September 2015 – August 2020: **Research Assistant at UMD**, mentor: Prof. Charalampos (Babis) Papamanthou.

May 2019 – August 2019: **Research Intern at Microsoft Research Labs (MSR)**, Redmond, USA, mentors: Dr. Melissa Chase and Dr. Esha Ghosh.

Sept. 2018 – December 2018: **Visiting Research Assistant at Hong Kong University of Science and Technology (HKUST)**, mentor: Prof. Dimitrios Papadopoulos.

May 2018 – August 2018: **Research Intern at Symantec Research Labs (SRL)**, Mountain View, USA, mentor: Dr. Saurabh Shintre.

June 2017 – August 2017: **Research Intern at VISA Research**, Palo Alto, USA, mentors: Dr. Shashank Agrawal and Dr. Payman Mohassel.

June 2013 – August 2015: **Graduate/Undergraduate Research Assistant at TUC**, Chania, Greece, mentor: Prof. Minos Garofalakis.

Awards & Distinctions

November 2021 **ACM SIGSAC Doctoral Dissertation Award Runner-up**.

May 2020 **Distinguished Dissertation Award**, *from the Department of Electrical and Computer Engineering, University of Maryland (UMD)*, (Grant $3,000).

February 2018 **Symantec Research Labs Graduate Fellowship**, *fellowship to conduct research on Searchable Encryption*, (Grant $20,000).

June 2016 **Outstanding Academic Performance Scholarship**, *from the Gerondelis Foundation*, (Grant $5,000).

September 2015 – August 2016 **Clark School of Engineering Distinguished Graduate Fellowship**, *from the Department of Electrical and Computer Engineering, University of Maryland (UMD)*, (Grant $15,000).

November 2013 **Award of Academic Excellence:**, *for graduating in 2013 with the **2nd** highest GPA from the School of Electronic & Computer Engineering of the Technical University of Crete*, Award by the LIMMAT STIFTUNG organization, (Grant 8,000 Euro).

Publications

[14] A. Mavrogiannakis, X. Wang, **I. Demertzis**, D. Papadopoulos, M. Garofalakis. OBLIVIATOR: OBLIVIous Parallel Joins and other OperATORs in Shared Memory Environments. **USENIX'25**

[13] K.Fredrickson, **I. Demertzis**, J Hughes, D. Long. Sparta: Practical Anonymity with Long-Term Resistance to Traffic Analysis. **IEEE SP'25**

[12] P. Mondal, J. G. Chamani, **I. Demertzis**, D. Papadopoulos. I/O-Efficient Dynamic Searchable Encryption meets Forward & Backward Privacy. **USENIX'24**

[11] N. Ngai, **I. Demertzis**, J. G. Chamani, D. Papadopoulos. Distrtibuted & Scalable Oblivious Sorting and Shuffling. **IEEE S&P'24**

[10] J. G. Chamani, **I. Demertzis**, D. Papadopoulos, C. Papamanthou, R. Jalili. GraphOS: Towards Oblivious Graph Processing. **PVLDB'23**

[9] J. G. Chamani, D. Papadopoulos, M. Karbasforushan, **I. Demertzis**. Dynamic Searchable Encryption with Optimal Search in the Presence of Deletions. **USENIX'22**

[8] E. Dauterman, V. Fang, **I. Demertzis**, N. Crooks, R. Popa . Snoopy: Surpassing the Scalability Bottleneck of Oblivious Storage. **SOSP'21**

[7] **I. Demertzis**, D. Papadopoulos, C. Papamanthou, S. Shintre. SEAL: Attack Mitigation for Encrypted Databases via Adjustable Leakage. **USENIX'20**

[6] **I. Demertzis**, J. G. Chamani, D. Papadopoulos, C. Papamanthou. Dynamic Searchable Encryption With Small Client Storage. **NDSS'20**

[5] **I. Demertzis**, D. Papadopoulos , C. Papamanthou. Searchable Encryption with Optimal Locality: Achieving Sublogarithmic Read Efficiency. **CRYPTO'18**

[4] **I. Demertzis**, R. Talapatra, C. Papamanthou. Efficient Searchable Encryption Through Compression. **PVLDB'18**

[3] **I. Demertzis**, S. Papadopoulos, O.Papapetrou, A. Deligiannakis, M. Garofalakis, C. Papamanthou. Practical Private Range Search In Depth. **TODS'18** (SIGMOD/PODS'16 Special Issue)

[2] **I. Demertzis**, C.Papamanthou. Fast Searchable Encryption with Tunable Locality. **SIGMOD'17**

[1] **I. Demertzis**, S. Papadopoulos, O.Papapetrou, A. Deligiannakis, M. Garofalakis. Practical Private Range Search Revisited. **SIGMOD'16** (Selected as one of the **best papers** submitted to the conference and invited to ACM Transactions on Database Systems TODS)

Current Students

Apostolos Mavrogiannakis, since September 2022 (PhD).
Kyle Fredrickson, (co-advised with Prof. Long), since January 2023 (PhD).
Nihal Talur, since September 2023 (PhD).

Alumni

Priyanka Mondal (PhD) (co-adv. w/ Arden), 2022-2024—next: Privacy Engineer at Snap Inc.
Muhammad Hamza Shahzad (MSc), since Sept. 2022 - December 2024 .
Amin Karbas (MSc), Sept. 2021 - June 2025—next: Software Engineer at ResolveAI
Surya Keswani (MSc), January 2022 - May 2022 —next: Software Engineer at Amazon.

Teaching

Winter 2025: CSE239A Private Computation on Encrypted Data
Winter 2025: CSE108C Computing on Encrypted Data
Fall 2024: CSE108 Algorithmic Foundations of Cryptography
Fall 2024: CSE206C The Foundations of Modern Cryptography
Fall 2024: CSE101 Introduction to Data Structures and Algorithm
Spring 2023: CSE108 Algorithmic Foundations of Cryptography
Spring 2023: CSE206C The Foundations of Modern Cryptography
Winter 2023: CSE290X Cryptography and Computer Security
Fall 2022: CSE101 Introduction to Data Structures and Algorithms
Winter 2022: CSE 108 Algorithmic Foundations of Cryptography
Fall 2021: CSE290X Cryptography and Computer Security

Patents

I. Demertzis, S. Shintre, Adjustable Oblivious Random Access Memory for Data Protection.

Professional Service

External/Sub-Reviewer: CCS 2016, SIGMOD 2016, NDSS 2018, CRYPTO 2018, FC 2018, ICDE 2018, S&P 2018, SIGMOD 2019, CCS 2019, NDSS 2019, NDSS 2020, S&P 2020, EURO S&P 2020, PKC 2020, VLDB J. 2020, TOPS 2020, TSC 2020, EuroS&P 2021, TKDE 2021, PVLDB 2021, ACISP 2021, USENIX 2021, USENIX 2022, CCS 2024, TOPS 2024.

Program Committee: CCSW 2019 and 2020, FCS 2021 and 2022, SIGMOD 2023, 2024, 2025 and 2026, EDBT 2024 Demo Track, ICDE 2024 and 2025, ASIACCS 2024, CCS 2025.