Ερευνητικές Προκλήσεις στην Επιστήμη Υπολογιστών
Δευτέρα 9 Ιανουαρίου 2023, 16:00 – 20:00
Αίθουσα Εκδηλώσεων, Κτήριο Διοίκησης, ΕΜΠ

Ο *Τομέας Τεχνολογίας Πληροφορικής και Υπολογιστών* (https://www.cs.ntua.gr) της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου, και το Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών «*Επιστήμη Δεδομένων και Μηχανική Μάθηση*» (https://dsml.ece.ntua.gr) σας προσκαλούν σε επιστημονική ημερίδα με θέμα τις σύγχρονες ερευνητικές προκλήσεις στην Επιστήμη Υπολογιστών. Η ημερίδα θα γίνει την **Δευτέρα 9 Ιανουαρίου 2023**, στην **Αίθουσα Εκδηλώσεων**, στο ισόγειο του Κτηρίου Διοίκησης, στην Πολυτεχνειούπολη Ζωγράφου, σύμφωνα με το παρακάτω πρόγραμμα.

Πρόγραμμα Ομιλιών

16:00 – 16:10	Έναρξη - χαιρετισμοί
16:10 – 17:00	**Secure Decentralization for a Global-Scale Trustworthy Infrastructure** Vassilis Zikas, *Purdue University*
17:00 – 17:50	**SECRECY: Secure collaborative analytics in untrusted clouds** Vasiliki (Vasia) Kalavri, *Boston University*
17:50 – 18:10	Σύντομο διάλειμμα
18:10 – 19:00	**Multi-Arm Bandits: side information and non-stationarity** Constantine Caramanis, *Univ. Texas at Austin*
19:00 – 19:50	**Connections Between Continuous and Combinatorial Total Problems** Manolis Zampetakis, *UC Berkeley*
19:50 – 20:00	Κλείσιμο

Περιλήψεις και Σύντομα Βιογραφικά Ομιλητών

Τίτλος: Secure Decentralization for a Global-Scale Trustworthy Infrastructure

Περίληψη: The wide adoption of global computer networks, such as the Internet, creates immense opportunities, and challenges the traditional centralized trust model. The idea of giving control of a widely-used critical infrastructure, e.g., centralized banking or immutable record-keeping, to its users is becoming ever more popular. Modern cryptography, security, and distributed computing have taken on the challenge to bring this decentralization ideas to reality by leveraging – and transitioning to practice – decades-long research on secure (distributed) computation, and combining it with modern Blockchain and Distributed Ledger Technologies (DLT). This has the potential to disrupt traditional strongholds of trust in the financial, digital, biomedical, and manufacturing sectors, as well as in governance. In this talk I will discuss secure decentralization with a focus on blockchain – from its current state to its vast potential for future applications. The talk will discuss novel design choices that go into deployed and widely adopted blockchain-based DLTs, and how these choices critically impact the security of the solutions and address implementation and deployment challenges.

Bio: Vassilis Zikas (https://www.cs.purdue.edu/homes/vzikas) is an Associate Professor of Computer Science and Director of the Purdue Blockchain Lab at Purdue University. Prior to his current appointment, he was an Associate Professor at the School of Informatics of the University of Edinburgh and Vice-Director of its Blockchain Technology Lab, and an Assistant Professor at RPI. He is one of the pioneers in the blockchain and decentralization research, and has been affiliated with (and supported by) leading blockchain and cryptocurrency companies. Indicatively, he was research fellow and area leader of IOG (formerly known as IOHK), where as a member of its core research team he co-developed the basis for the decentralization of its flagship Cardano blockchain – holding a top-ten cryptocurrency; he is currently the Chief Scientist of Sunday Group, and the lead architect of its flagship Mobby blockchain. In the past, he was a fellow of the Simons Institute, UC Berkeley, and a Swiss NSF fellow. His work is supported by government agencies both in the US (NSF, DoD) and in Switzerland (Swiss NSF), and by the blockchain industry including multi-million faculty gifts and grants by Sunday Group and the Algorand Foundation.

Τίτλος: SECRECY: Secure collaborative analytics in untrusted clouds

Περίληψη: Enabling secure outsourced analytics with practical performance has been a long-standing research challenge in the databases and systems communities. In this talk, I will present our work towards realizing this vision with SECRECY, a new framework for secure relational analytics in untrusted clouds. SECRECY targets offline collaborative analytics, where data owners (hospitals, companies, research institutions, or individuals) are willing to allow certain computations on their collective private data, provided that data remain siloed from untrusted entities. To ensure no information leakage and provable security guarantees, SECRECY relies on cryptographically secure Multi-Party Computation (MPC). Instead of treating MPC as a black box, like prior works, SECRECY exposes the costs of oblivious queries to the planner and employs novel logical, physical, and protocol-specific optimizations, all of which are applicable even when data owners do not participate in the computation. As a result, SECRECY outperforms state-of-the-art systems and can comfortably process much larger datasets with good performance and modest use of resources.

Bio: Vasiliki (Vasia) Kalavri (https://www.bu.edu/cs/profiles/vasiliki-kalavri) is an Assistant Professor of Computer Science at Boston University, where she leads the Complex Analytics and Scalable Processing Systems lab. Vasia and her team enjoy doing research on multiple aspects of data-centric systems: designing self-managed systems for data stream processing, scaling graph Machine Learning on modern storage, and developing practical solutions for private collaborative analytics with Multi-party Computation. Before joining BU, Vasia was a postdoctoral fellow at ETH Zurich and she received her PhD from KTH, Sweden, and UCLouvain, Belgium. Her PhD dissertation won the IBM Innovation Award in 2017. Vasia received an MSc in Distributed Computing from KTH and UPC BarcelonaTech and her undergraduate diploma from the School of Electrical and Computer Engineering at NTUA. Vasia's work is supported by several grants, including a NSF SaTC Medium award, a Hariri Institute Focused Research Program award, and industry awards from Google, Samsung, and RedHat.

Τίτλος: Multi-Arm Bandits: side information and non-stationarity

Περίληψη: Multi-armed bandits are a classical model to study dynamic decision-making in an uncertain environment. The central question they explore is the tradeoff between playing actions with well-understood rewards, versus taking the chance to explore unknown actions. In this talk, we consider two important extensions of the bandit model. In the first, we consider the setting where playing an action yields not only a reward, but also information about the quality of other actions. Therefore, one has to balance the value of information as well as the value of the reward. We next consider non-stationarity, where playing a certain action may change its reward in the future, as is often the case with recommendation systems. In this setting, one must consider how the present reward can impact the ability to collect good rewards in the future.

Joint work with Alexia Atsidakou, Orestis Papadigenopoulos and Sanjay Shakkottai.

Bio: ***Constantine Caramanis*** (http://users.ece.utexas.edu/~cmcaram) is a Professor in Electrical and Computer Engineering at UT Austin. He received the Ph.D. degree in EECS from MIT. He is a recipient of a NSF CAREER award, and is an IEEE Fellow. His research interests focus on optimization, machine learning and statistics.

Τίτλος: Connections Between Continuous and Combinatorial Total Problems

Περίληψη: In this talk, we will present a line of work that tries to identify non-trivial connections between combinatorial and continuous optimization problems from a computational and query complexity point of view. In particular, we will talk about the complexity of finding the following points in continuous spaces and their combinatorial analogs: (1) stationary points of constrained and unconstrained non-convex functions, and (2) points that satisfy the multi-dimensional analogs of the intermediate value theorem.

Bio: ***Manolis Zampetakis*** (https://mzampet.com) is a postdoc at the EECS Department of UC Berkeley, working with Michael Jordan, and will join the Computer Science Department of Yale University in July 2023 as an Assistant Professor. He received his PhD from the EECS Department at MIT advised by Constantinos Daskalakis. For his PhD thesis, he was awarded the ACM SIGEcom Doctoral Dissertation Award. In fall 2018, he received the Google PhD Fellowship. His research interests include Theoretical Machine Learning, Statistics, Optimization, Computational Complexity, Game Theory, Mechanism Design and Sublinear Algorithms.
