37th International Symposium on Distributed Computing

DISC 2023, October 10-12, 2023, L'Aquila, Italy

Edited by

Rotem Oshman

Editors

Rotem Oshman
Blavatnik School of Computer Science, Tel Aviv University, Israel
roshman@tau.ac.il

ACM Classification 2012
Software and its engineering → Distributed systems organizing principles; Computing methodologies → Distributed computing methodologies; Computing methodologies → Concurrent computing methodologies; Hardware → Fault tolerance; Information systems → Data structures; Networks; Theory of computation; Theory of computation → Models of computation; Theory of computation → Design and analysis of algorithms

ISBN 978-3-95977-301-0

Published online and open access by
Schloss Dagstuhl – Leibniz-Zentrum für Informatik GmbH, Dagstuhl Publishing, Saarbrücken/Wadern, Germany. Online available at https://www.dagstuhl.de/dagpub/978-3-95977-301-0.

Publication date
October, 2023

Bibliographic information published by the Deutsche Nationalbibliothek
The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available in the Internet at https://portal.dnb.de.

Digital Object Identifier: 10.4230/LIPIcs.DISC.2023.0

LIPIcs – Leibniz International Proceedings in Informatics

LIPIcs is a series of high-quality conference proceedings across all fields in informatics. LIPIcs volumes are published according to the principle of Open Access, i.e., they are available online and free of charge.

ISSN 1868-8969

https://www.dagstuhl.de/lipics

Contents

Preface
Rotem Oshman 0:ix

Organization
..... 0:xi–0:xiii

Awards
..... 0:xv

2023 Principles of Distributed Computing Doctoral Dissertation Awards
..... 0:xvii

2023 Edsger W. Dijkstra Prize in Distributed Computing
..... 0:xix

Regular Papers

Colordag: An Incentive-Compatible Blockchain
Ittai Abraham, Danny Dolev, Ittay Eyal, and Joseph Y. Halpern 1:1–1:22

Certified Round Complexity of Self-Stabilizing Algorithms
Karine Altisen, Pierre Corbineau, and Stéphane Devismes 2:1–2:22

Network Agnostic Perfectly Secure MPC Against General Adversaries
Ananya Appan, Anirudh Chandramouli, and Ashish Choudhury 3:1–3:19

One Step Forward, One Step Back: FLP-Style Proofs and the Round-Reduction Technique for Colorless Tasks
Hagit Attiya, Pierre Fraigniaud, Ami Paz, and Sergio Rajsbaum 4:1–4:23

Topological Characterization of Task Solvability in General Models of Computation
Hagit Attiya, Armando Castañeda, and Thomas Nowak 5:1–5:21

Base Fee Manipulation in Ethereum's EIP-1559 Transaction Fee Mechanism
Sarah Azouvi, Guy Goren, Lioba Heimbach, and Alexander Hicks 6:1–6:22

On the Node-Averaged Complexity of Locally Checkable Problems on Trees
Alkida Balliu, Sebastian Brandt, Fabian Kuhn, Dennis Olivetti, and Gustav Schmid 7:1–7:21

Treasure Hunt with Volatile Pheromones
Evangelos Bampas, Joffroy Beauquier, Janna Burman, and William Guy–Obé 8:1–8:21

The FIDS Theorems: Tensions Between Multinode and Multicore Performance in Transactional Systems
Naama Ben-David, Gal Sela, and Adriana Szekeres 9:1–9:24

Communication Lower Bounds for Cryptographic Broadcast Protocols
Erica Blum, Elette Boyle, Ran Cohen, and Chen-Da Liu-Zhang 10:1–10:19

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Time and Space Optimal Massively Parallel Algorithm for the 2-Ruling Set Problem
Mélanie Cambus, Fabian Kuhn, Shreyas Pai, and Jara Uitto 11:1–11:12

Self-Stabilizing Clock Synchronization in Probabilistic Networks
Bernadette Charron-Bost and Louis Penet de Monterno 12:1–12:18

Every Bit Counts in Consensus
Pierre Civit, Seth Gilbert, Rachid Guerraoui, Jovan Komatovic, Matteo Monti, and Manuel Vidigueira 13:1–13:26

Efficient Collaborative Tree Exploration with Breadth-First Depth-Next
Romain Cosson, Laurent Massoulié, and Laurent Viennot 14:1–14:21

A Topology by Geometrization for Sub-Iterated Immediate Snapshot Message Adversaries and Applications to Set-Agreement
Yannis Coutouly and Emmanuel Godard 15:1–15:20

Send/Receive Patterns Versus Read/Write Patterns in Crash-Prone Asynchronous Distributed Systems
Mathilde Déprés, Achour Mostéfaoui, Matthieu Perrin, and Michel Raynal 16:1–16:24

Modular Recoverable Mutual Exclusion Under System-Wide Failures
Sahil Dhoked, Wojciech Golab, and Neeraj Mittal 17:1–17:24

Optimal Computation in Leaderless and Multi-Leader Disconnected Anonymous Dynamic Networks
Giuseppe A. Di Luna and Giovanni Viglietta 18:1–18:20

Fast Coloring Despite Congested Relays
Maxime Flin, Magnús M. Halldórsson, and Alexandre Nolin 19:1–19:24

Distributed Certification for Classes of Dense Graphs
Pierre Fraigniaud, Frédéric Mazoit, Pedro Montealegre, Ivan Rapaport, and Ioan Todinca 20:1–20:17

The Synchronization Power (Consensus Number) of Access-Control Objects: the Case of AllowList and DenyList
Davide Frey, Mathieu Gestin, and Michel Raynal 21:1–21:23

List Defective Colorings: Distributed Algorithms and Applications
Marc Fuchs and Fabian Kuhn 22:1–22:23

Conditionally Optimal Parallel Coloring of Forests
Christoph Grunau, Rustam Latypov, Yannic Maus, Shreyas Pai, and Jara Uitto .. 23:1–23:20

On the Inherent Anonymity of Gossiping
Rachid Guerraoui, Anne-Marie Kermarrec, Anastasiia Kucherenko, Rafael Pinot, and Sasha Voitovych 24:1–24:19

Durable Algorithms for Writable LL/SC and CAS with Dynamic Joining
Prasad Jayanti, Siddhartha Jayanti, and Sucharita Jayanti 25:1–25:20

Cordial Miners: Fast and Efficient Consensus for Every Eventuality
Idit Keidar, Oded Naor, Ouri Poupko, and Ehud Shapiro 26:1–26:22

Fast Reconfiguration for Programmable Matter
Irina Kostitsyna, Tom Peters, and Bettina Speckmann 27:1–27:21

Quorum Subsumption for Heterogeneous Quorum Systems
Xiao Li, Eric Chan, and Mohsen Lesani 28:1–28:19

Fast Deterministic Rendezvous in Labeled Lines
Avery Miller and Andrzej Pelc 29:1–29:22

Null Messages, Information and Coordination
Raïssa Nataf, Guy Goren, and Yoram Moses 30:1–30:21

Gorilla: Safe Permissionless Byzantine Consensus
Youer Pu, Ali Farahbakhsh, Lorenzo Alvisi, and Ittay Eyal 31:1–31:16

Distributed Sketching Lower Bounds for k-Edge Connected Spanning Subgraphs, BFS Trees, and LCL Problems
Peter Robinson 32:1–32:21

Memory-Anonymous Starvation-Free Mutual Exclusion: Possibility and Impossibility Results
Gadi Taubenfeld 33:1–33:17

Improved and Partially-Tight Lower Bounds for Message-Passing Implementations of Multiplicity Queues
Anh Tran and Edward Talmage 34:1–34:20

Brief Announcements

Brief Announcement: BatchBoost: Universal Batching for Concurrent Data Structures
Vitaly Aksenov, Michael Anoprenko, Alexander Fedorov, and Michael Spear 35:1–35:7

Brief Announcement: Multi-Valued Connected Consensus: A New Perspective on Crusader Agreement and Adopt-Commit
Hagit Attiya and Jennifer L. Welch 36:1–36:7

Brief Announcement: Relations Between Space-Bounded and Adaptive Massively Parallel Computations
Michael Chen, A. Pavan, and N. V. Vinodchandran 37:1–37:7

Brief Announcement: On Implementing Wear Leveling in Persistent Synchronization Structures
Jakeb Chouinard, Kush Kansara, Xialin Liu, Nihal Potdar, and Wojciech Golab .. 38:1–38:7

Brief Announcement: Subquadratic Multivalued Asynchronous Byzantine Agreement WHP
Shir Cohen and Idit Keidar 39:1–39:6

Brief Announcement: Distributed Derandomization Revisited
Sameep Dahal, Francesco d'Amore, Henrik Lievonen, Timothé Picavet, and Jukka Suomela 40:1–40:5

Brief Announcement: Byzantine Consensus Under Dynamic Participation with a Well-Behaved Majority
Eli Gafni and Giuliano Losa 41:1–41:7

Brief Announcement: Scalable Agreement Protocols with Optimal Optimistic Efficiency
Yuval Gelles and Ilan Komargodski 42:1–42:6

Brief Announcement: Let It TEE: Asynchronous Byzantine Atomic Broadcast with $n \geq 2f + 1$
Marc Leinweber and Hannes Hartenstein 43:1–43:7

Brief Announcement: Recoverable and Detectable Self-Implementations of Swap
Tomer Lev Lehman, Hagit Attiya, and Danny Hendler 44:1–44:7

Brief Announcement: Line Formation in Silent Programmable Matter
Alfredo Navarra and Francesco Piselli 45:1–45:8

Brief Announcement: The Space Complexity of Set Agreement Using Swap
Sean Ovens 46:1–46:6

Brief Announcement: Grassroots Distributed Systems: Concept, Examples, Implementation and Applications
Ehud Shapiro 47:1–47:7

Preface

Welcome to DISC 2023, the 37th International Symposium on Distributed Computing, held on October 10–12, 2023, in L'Aquila, Italy. DISC is an international forum on the theory, design, analysis, and implementation of distributed systems and networks, focusing on distributed computing in all its forms. DISC is organized in cooperation with the European Association for Theoretical Computer Science (EATCS).

DISC 2023 received 125 submissions in the "regular paper" category, and 14 submissions in the "brief announcement" category. The program was selected by a program committee consisting of 24 full members and 4 half-load members. The program committee was assisted by 127 external reviewers. As in previous years, the committee used a relaxed form of double-blind reviewing, where the submissions themselves were anonymous, but authors were permitted to disseminate their work by uploading it to online repositories or by giving talks about it. Each submission was evaluated by at least three reviewers, and final decisions were made during a 2-day virtual PC meeting. 34 regular papers were accepted (an acceptance rate of 27%), and 13 brief announcements. The keynote talks at DISC 2023 were given by Tal Rabin on behalf of the winners of the 2023 Dijkstra Award, by Amos Korman, and by Lorenzo Alvisi.

The following two awards are jointly sponsored by DISC and the ACM Symposium on Principles of Distributed Computing (PODC):

- The 2023 Edsger W. Dijkstra Prize in Distributed Computing was presented at DISC 2023. The award was given to Michael Ben-Or, Shafi Goldwasser and Avi Wigderson for their paper "Completeness Theorem for Non-Cryptographic Fault-Tolerant Distributed Computation", to David Chaum, Claude Crépeau and Ivan Damgård for their paper "Multiparty Unconditionally Secure Protocols", and to Tal Rabin and Michael Ben-Or for their paper "Verifiable Secret Sharing and Multiparty Protocols with Honest Majority".
- The 2023 Principles of Distributed Computing Doctoral Dissertation Award was presented at PODC 2023. The award was given to Dr. Siddhartha Jayanti for his dissertation "Simple, Fast, Scalable, and Reliable Multiprocessor Algorithms", and to Dr. Dean Leitersdorf for his dissertation "Fast Distributed Algorithms via Sparsity Awareness.".

This volume includes the citations for the best paper and best student paper awards at DISC 2023, as well as the citations for the 2023 Edsger W. Dijkstra Prize in Distributed Computing, which was presented at DISC 2023, and for the Best Dissertation Award, which was presented at PODC 2023.

I would like to warmly thank everyone who contributed to DISC 2023: the authors who submitted their work to PODC, the PC members and external reviewers, the keynote speakers, the organizing committee, the workshop chairs, members of the award committees, and participants of the conference. I am also grateful to the members of the steering committee and to former chairs of DISC, who shared their invaluable experience and advice; to EATCS for their support; and to the staff of Schloss Dagstuhl – Leibniz-Zentrum für Informatik for their help in preparing these proceedings.

October 2023

Rotem Oshman
DISC 2023 Program Chair

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organization

DISC, the International Symposium on Distributed Computing, is an annual forum for presentation of research on all aspects of distributed computing. It is organized in cooperation with the European Association for Theoretical Computer Science (EATCS). The symposium was established in 1985 as a biannual International Workshop on Distributed Algorithms on Graphs (WDAG). The scope was soon extended to cover all aspects of distributed algorithms and WDAG came to stand for International Workshop on Distributed AlGorithms, becoming an annual symposium in 1989. To reflect the expansion of its area of interest, the name was changed to DISC (International Symposium on DIStributed Computing) in 1998, opening the symposium to all aspects of distributed computing. The aim of DISC is to reflect the exciting and rapid developments in this field.

Program Chair

Rotem Oshman	Tel Aviv University (Israel)

Program Committee

Carole Delporte-Gallet	IRIF, Université Paris Cité (France)
Corentin Travers	LIS/Université d'Aix-Marseille (France)
Fabian Kuhn	University of Freiburg (Germany)
Gillat Kol	Princeton University (USA)
Gregory Chockler	University of Surrey (UK)
Guy Goren	Protocol Labs (Israel)
Jara Uitto	Aalto University (Finland)
Jennifer Welch	Texas A&M University (USA)
Juho Hirvonen	Helsinki Institute for Information Technology and Aalto University (Finland)
Kunal Agrawal	Washington University in St. Louise (USA)
Laurent Feuilloley	CNRS / Université de Lyon (France)
Manuela Fischer	ETH Zurich (Switzerland)
Mark Moir	Oracle Labs (USA)
Maurice Herlihy	Brown University (USA)
Nicola Santoro	Carleton University (Canada)
Oded Naor	Technion and StarkWare (Israel)
Orr Fischer	Weizmann Institute (Israel)
Paul G. Spirakis	University of Liverpool (UK)
Pedro Montealegre	Adolfo Ibáñez University (Chile)
Petr Kuznetsov	INFRES, Telecom Paris (France)
Petra Berenbrink	University of Hamburg (Germany)
Rafael Pass	Tel Aviv University, Israel and Cornell University (USA)
Rati Gelashvili	Aptos (USA)
Rob Johnson	VMWare (USA)
Siddhartha Visveswara Jayanti	Google Research and MIT (USA)
Tania Lorido Botran	Roblox (USA)
Wojciech Golab	University of Waterloo (Canada)
Zarko Milosevic	Informal Systems (Canada)

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

Organizing Committee

Alkida Balliu (co-Chair)	Gran Sasso Science Institute (Italy)
Dennis Olivetti (co-Chair)	Gran Sasso Science Institute (Italy)
Yannic Maus (Workshops Chair)	TU Graz (Austria)
Tijn de Vosa (Environmental co-Chair)	University of Salzburg (Austria)
Laurent Feuilloley (Environmental co-Chair)	Université Lyon 1 and CNRS (France)
William K. Moses Jr. (Publicity Chair)	Durham University (UK)
Gianlorenzo D'Angelo	Gran Sasso Science Institute (Italy)

Steering Committee

Jukka Suomela (Chair)	Aalto University (Finland)
Hagit Attiya (Vice Chair)	Technion (Israel)
Seth Gilbert (2021 PC Chair)	NUS (Singapore)
Christian Scheideler (2022 PC Chair)	University of Paderborn (Germany)
Rotem Oshman (2023 PC Chair)	Tel Aviv University (Israel)
Calvin Newport (Member-at-large)	Georgetown University (USA)
Moti Medina (Treasurer)	Bar-Ilan University (Israel)

External Reviewers

Davide Frey	Shantanu Das	Luciano Freitas de Souza
James Aspnes	Peter Robinson	George Skretas
Faith Ellen	Théo Pierron	Leonid Barenboim
Hossein Vahidi	Christopher Hahn	Grzegorz Stachowiak
Chien-Chih Chen	Ami Paz	Adam Gańczorz
Subhash Bhagat	Martín Ríos-Wilson	Alexander Spiegelman
Ivan Rapaport	Michael Elkin	Hagit Attiya
Nirupam Gupta	Gal Sela	Matej Pavlovic
Anup Joshi	Balaji Arun	Yuanhao Wei
Michiko Inoue	Michal Dory	Hagit Attiya
Felix Biermeier	Thomas Nowak	Ahmed Fahmy
Adam Morrison	Mikaël Rabie	Matej Pavlovic
Lewis Tseng	Ivan Rapaport	Giuseppe Prencipe
Euripides Markou	Arnaud Labourel	Raïssa Nataf
Gal Assa	Mélanie Cambus	Yannic Maus
Hafiz Imtiaz	Sergio Rajsbaum	Giuliano Losa
Lukas Hintze	Uri Meir	Chien-Chih Chen
Andrei Tonkikh	Dennis Olivetti	Francesco d'Amore
Achour Mostéfaoui	Ran Gelles	Josu Doncel
Gupta Nirupam	Tomer Koren	Yi-Jun Chang
Yadu Vasudev	Talya Eden	Sebastian Siebertz
Matthias Függer	Diana Ghinea	Peter Robinson
Sucharita Jayanti	Gal Assa	Daniel Collins
Armando Castaneda	Leqi Zhu	Chen-Da Liu Zhang
Yann Disser	Clément Legrand-Duchesne	Yitong Yin
Tijn de Vos	Michal Dory	Achour Mostéfaoui

Hsin-Hao Su
Shang-En Huang
Chetan Gupta
Zhuolun Xiang
Sergio Rajsbaum
Marios Mavronicolas
Peter Davies
Lioba Heimbach
Themistoklis Melissourgos
Chryssis Georgiou
Anissa Lamani
Stéphane Devismes
Laurent Viennot
Hendrik Molter
Hamed Hosseinpour
Mina Dalirrooyfard
Jeff Giliberti
Tom Friedetzky
Peter Kling
Andrea Richa
Saku Peltonen
Christoph Lenzen
Gokarna Sharma
Armando Castaneda
Shreyas Pai
William K. Moses Jr.
Sara Tucci-Piergiovanni
Saeed Akhoondian Amiri
Ivan Rapaport
Alan Kuhnle
Michel Raynal
Maximilian Hahn-Klimroth
Yi-Jun Chang
Keren Censor-Hillel
Gregory Schwartzman
Rustam Latypov
Seri Khoury
Marten Maack
Gal Assa
Malin Rau
Benjamin Jauregui
Yukiko Yamauchi
Mĺanie Cambus
Giorgi Nadiradze
Ami Paz
Xiaorui Sun
Hagit Attiya
Darya Melnyk
Leonid Barenboim
Hao Tan
Christoph Grunau
Valerie King
Elad Michael Schiller
George Giakkoupis
Thomas Nowak
Xavier Defago
Gabriele Di Stefano
Aaron Schild
Nina Klobas
Eric Ruppert
Giuseppe Antonio Di Luna
Igor Zablotchi
Slobodan Mitrović
João Paulo Bezerra
Shantanu Das
Benjamin Jauregui
Tigran Tonoyan
Ioan Todinca
Quentin Bramas
Alexander Spiegelman

Acknowledgements

DISC 2023 acknowledges the use of Easychair for handling submissions and managing the review process and LIPIcs for producing and publishing the proceedings.

DISC is organized in cooperation with the European Association for Theoretical Computer Science (EATCS).

Awards

Best Papers

The DISC Program Committee has selected the following two papers to receive the DISC 2023 best paper award:

Every Bit Counts in Consensus
by Pierre Civit, Seth Gilbert, Rachid Guerraoui, Jovan Komatovic, Matteo Monti and Manuel Vidigueira.

This paper improves the space complexity of multi-valued consensus by presenting an algorithm that requires only $O(n^{1.5}L + n^{2.5}k)$ bits for consensus on L-bit values (with security parameter k), an improvement of $\sqrt{n}$ upon prior work. Moreover, the paper devises a version of the protocol that uses stronger cryptographic assumptions – namely, the existence of STARK proofs – and achieves near-optimal bit complexity, $O(nL + n^2\text{poly}(k))$. Multi-valued consensus is an important problem in practice, where the value being agreed upon is often very large, and the paper uses interesting and novel techniques to achieve its strong results.

On the Node-Averaged Complexity of Locally Checkable Problems on Trees
by Alkida Balliu, Sebastian Brandt, Fabian Kuhn, Dennis Olivetti and Gustav Schmid.

This paper studies the node-averaged round complexity locally-checkable labeling (LCL) problems. The usual complexity measure in the LOCAL model is the *worst-case* round complexity across all nodes. The paper establishes relationships between the worst-case and the node-averaged complexity of LCL problems in trees, showing that every LCL problem whose worst-case complexity is $O(\log n)$ admits an algorithm with node-averaged complexity $O(\log^* n)$, and that every LCL problem with worst-case complexity $\Theta(n^{1/k})$ requires node-averaged complexity $\tilde{\Omega}(n^{1/(2^k-1)})$, which is in some cases tight. Node-averaged complexity is a new and interesting complexity measure, and the results of the paper show that node-averaged complexity can be significantly better than the worst-case complexity, making it a worthwhile measure to study.

Best Student Paper

The DISC Program Committee has selected the following paper to receive the DISC 2023 best student paper award:

The FIDS Theorems: Tensions between Multinode and Multicore Performance in Transactional Systems
by Naama Ben-David, Gal Sela and Adriana Szekeres

This paper studies the performance of transactional systems that are both parallel and distributed, meaning that they both use multiple nodes and employ multiple cores per node. The paper shows that there is an inherent tradeoff between the scalability of the system, the speed with which the system commits transaction in good executions, and its fault tolerance. On the positive side, the paper shows that if any one of the three requirements is dropped, then it is possible to construct a system satisfying the other two.

The tradeoff established and formalized in this paper is timely and relevant to large-scale transactional systems, and serves as an analog for the famous CAP theorem for this setting.

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

2023 Principles of Distributed Computing Doctoral Dissertation Awards

Many exceptionally high-quality doctoral dissertations were submitted for the 2023 Principles of Distributed ComputingDoctoral Dissertation Award. After careful deliberation, the award committee decided to share the award between:

- Dr. Siddhartha Jayanti for his dissertation "Simple, Fast, Scalable, and Reliable Multiprocessor Algorithms."
- Dr. Dean Leitersdorf for his dissertation "Fast Distributed Algorithms via Sparsity Awareness."

Dr. Siddhartha Jayanti completed his PhD on November 27th 2022, under the supervision of Prof. Julian Shun, at MIT. In his thesis, Dr. Jayanti identifies simplicity, speed, scalability, and reliability as four core design goals for multiprocessor algorithms, and designs and analyzes algorithms that meet these goals. The thesis comprises a vast number of novel results in the scope of distributed and concurrent synchronization. His algorithmic contributions include a scalable algorithm for concurrent union-find, a wait-free linearizable, fast array data structure that supports standard array operations in constant time and optimal space, and mutual exclusion (lock) algorithms with optimal complexity for real-time and persistent memory systems. Dr. Jayanti also defines a generalization of the fundamental wake-up problem, permitting him to prove fundamental new hardness results for many standard data structures, including queues, stacks, priority queues, counters, and union-find data structures. Moreover, he devises a novel simple-to-use technique for producing machine-verified proofs of the correctness (linearizability and strong linearizability) of concurrent algorithms, and successfully applied this method to verify fundamental data multicore data structures, such as queues, union-find, and snapshot objects. Dr. Jayanti also analyzes a parallel and asynchronous Markov Chain Monte Carlo (MCMC) algorithm, showing that it can speed-up the collection of low-bias statistics from probability distributions of interest in Machine Learning and Statistical Physics. Finally, Dr. Jayanti's PhD dissertation introduces the Samskrtam Technical Lexicon Project, which incorporates ideas from Panini's generative grammar to facilitate the coining of new technical vocabulary and increase the availability of scientific education and literature in Indian and other world languages. As part of the project, he uses Sanskrit roots to coin words for several concepts in algorithms and multiprocessors in Telugu, and contributes the first modern computer science research paper in the Telugu language, which has about 100 million speakers around the world.

Dr. Dean Leiterdorf completed his thesis on May 14th, 2022, under the supervision of Prof. Keren Censor-Hillel, at the Technion. In his thesis, Dr. Leitersdorf designs fast distributed algorithms for sparse matrix multiplication and demonstates their usefulness by applying them to shortest path and subgraph existence problems. Applications of matrix multiplication are found in many fields, including scientific computing, statistics, machine learning, and quantum computing, and therefore fast algorithms for matrix multiplication are critical for these. Dr. Leitersdorf does not just come up with solutions that can exploit the sparsity of the input matrices but also the sparsity of the output matrix, which allows him to come up with a large number of results for different communication models that partially significantly improve the state of the art. Among these are constant-round algorithms for computing graph spanners and approximate all-pairs-shortest-paths as well as constant-round algorithms

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

for computing the girth of the input graph up to an additive 1 in the Congested Clique model. Through reductions between various models and a number of advanced techniques, Dr. Leitersdorf extends his results also to the CONGEST model, hybrid networks, and various other models. On top of this, he also designs a variety of algorithms that speed up clique detection in quantum computing settings and whose runtime breaks lower bounds known for classical distributed computing.

The award is sponsored jointly by the ACM Symposium on Principles of Distributed Computing (PODC) and the EATCS Symposium on Distributed Computing (DISC). It is presented annually, with the presentation taking place alternately at PODC and DISC. This year it was presented at PODC, to be held in Orlando, Florida USA, June 19-23, 2023.

The 2023 Principles of Distributed Computing Doctoral Dissertation Award Committee

Shlomi Dolev (Chair), BGU (Israel)
Rachid Guerraoui, EPFL (Switzerland)
Fabian Kuhn, University of Freiburg (Germany)
Woelfel Philipp, University of Calgary (Canada)
Christian Scheideler, Paderborn University (Germany)

2023 Edsger W. Dijkstra Prize in Distributed Computing

The 2023 Edsger W. Dijkstra Prize in Distributed Computing has been awarded to the papers

- Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, by Michael Ben-Or, Shafi Goldwasser and Avi Wigderson (STOC 1988, 1–10).
- Multiparty Unconditionally Secure Protocols, by David Chaum, Claude Crèpeau and Ivan Damgård (STOC 1988, 11–19).
- Verifiable Secret Sharing and Multiparty Protocols with Honest Majority, by Tal Rabin and Michael Ben-Or (STOC 1989, 73–85).

for introducing Information-Theoretic Secure Multiparty Computations and showing how to achieve maximal resilience to malicious adversaries while providing unconditional security.

The area of Secure Multiparty Computation (MPC) answers the following fundamental question about distributed computations. How does a group of parties compute a function of their inputs while preserving not only correctness of the output but also, the secrecy of each party's input? Furthermore, this goal should be achieved in the case where some of the parties are malicious and try to foil the computation.

The awarded papers opened the vibrant area of MPC in the information theoretic setting, in which thousands of works have been published, and that is still going strong. Protocols in the information- theoretic model often are more efficient than their computational counterparts, in some cases by orders of magnitude, and thus have led to the most efficient state-of-the-art designs of MPC implementations. These protocols are an indispensable tool in the increasing demands for security and privacy in our modern digital society.

MPC and the techniques from the nominated papers have had tremendous impact on the broader area of cryptography with such results relating to zero-knowledge proofs and coding theory. They also have had far reaching impact on the broader area of theoretical computer science by providing a technical basis and inspiration for such results as locally random reductions, private information retrieval, and locally decodable codes.

The 2023 Dijkstra Award Committee

Magnús Halldórsson, Reykjavik University (chair)
Yehuda Afek, Tel-Aviv University
Idit Keidar, Technion
Rotem Oshman, Tel-Aviv University
Ulrich Schmid, TU Wien
Gadi Taubenfield, Reichman University

37th International Symposium on Distributed Computing (DISC 2023).
Editor: Rotem Oshman
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany