1. Record Nr. UNINA9910629277003321

Titolo	Stabilization, safety, and security of distributed systems : 24th International Symposium, SSS 2022, Clermond Ferrand, France, November 15-17, 2022, proceedings / / edited by Stephane Devismes, [and four others]
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-21017-4
Descrizione fisica	1 online resource (378 pages)
Collana	Lecture Notes in Computer Science ; ; v.13751
Disciplina	929.605
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Invited Papers -- Invited Paper: Simple, Strict, Proper, Happy: A Study of Reachability in Temporal Graphs -- 1 Introduction -- 2 Temporal Graphs -- 2.1 Strictness/Properness/Simpleness -- 2.2 Does It Really Matter? (Example of Spanners) -- 2.3 Happy Temporal Graphs -- 3 Expressivity in Terms of Reachability -- 3.1 Separations -- 3.2 Transformations -- 3.3 Summary and Discussions -- 4 More Facts About Happy Temporal Graphs -- 5 Concluding Remarks and Open Questions -- References -- Invited Paper: One Bit Agent Memory is Enough for Snap-Stabilizing Perpetual Exploration of Cactus Graphs with Distinguishable Cycles -- 1 Introduction -- 2 Preliminaries -- 2.1 Cactus Graph -- 2.2 Mobile Agent and Graph Exploration -- 3 Snap-Stabilizing Perpetual Exploration -- 3.1 Port Traversal Graph -- 3.2 Algorithm for a Single Agent with One-Bit Agent Memory -- 4 Exploration by an Oblivious Agent -- References -- Invited Paper: Towards Practical Atomic Distributed Shared Memory: An Experimental Evaluation -- 1 Introduction -- 2 Algorithms Overview -- 2.1 ARES -- 2.2 Cassandra -- 2.3 Redis -- 3 Experimental Evaluation -- 3.1 Experimentation Setup -- 3.2 Scenarios -- 3.3 Experimental Results -- 4 Conclusions -- References -- Invited Paper: Cross-Chain State Machine Replication -- 1 Introduction -- 2 Model of Computation -- 3 State Machines -- 3.1

Example: Simple Swap -- 3.2 Example: Decentralized Autonomous Organization (DAO) -- 4 State Machine Replication Protocol -- 4.1 Path Signatures -- 4.2 Reliable Delivery -- 4.3 Initialization, Moves, and Settlement -- 4.4 Dynamic Funding -- 5 Remarks -- 6 Related Work -- References -- Regular Papers -- Plateau: A Secure and Scalable Overlay Network for Large Distributed Trust Applications -- 1 Introduction -- 1.1 Our Contribution -- 1.2 Related Works.
2 Model and Preliminaries -- 3 The Plateau Network Design and Statement of Results -- 4 Concluding Remarks and Future Work -- References -- The Limits of Helping in Non-volatile Memory Data Structures -- 1 Introduction -- 1.1 Contributions -- 1.2 Related Work -- 2 Characterization of the Crash-Recovery Model -- 3 Process Helping -- 4 Strict-Linearizability vs. Linearization-Helping -- 4.1 Sticky-Bit Object -- 4.2 An Equivalence Between Linearizability and Strict-Linearizability -- 5 Strict-Linearizability vs. Universal-Helping -- 5.1 Equivalence Between Strict-Linearizability and Universal-Help Freedom -- References -- Treasure Hunt in Graph Using Pebbles -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Model and Problem Definition -- 1.3 Contribution -- 1.4 Related Work -- 2 Treasure Hunt Algorithm When k&lt -- D -- 2.1 D2k &lt -- D -- 2.2 k&lt -- D2 -- 3 Treasure Hunt Algorithm When kD -- 3.1 Idea of Treasure Hunt in Tree for k=cD Pebbles -- 3.2 Extending the Idea for General Graphs -- 4 Lower Bound -- 5 Conclusion -- References -- Blockchain in Dynamic Networks -- 1 Introduction -- 2 Notation, Definitions and Problem Statement -- 3 Decisive Computations -- 4 Impossibility -- 5 Solutions -- 6 Extensions and Optimizations -- 7 Performance Evaluation -- 8 Conclusion -- References -- Improving the Efficiency of Report and Trace Ring Signatures -- 1 Introduction -- 2 Preliminaries -- 3 Syntax and Security Model -- 3.1 Security Model -- 4 An Efficient Instantiation of Fraser and Quaglia's Protocol -- 4.1 A Pairing-Based ElGamal Variant -- 4.2 Discussion -- 5 A New RTR Signature Construction -- 5.1 Description of Our Protocol -- 5.2 Security Analysis -- 6 Concluding Remarks -- References -- Flexible Scheduling of Transactional Memory on Trees -- 1 Introduction -- 2 Technical Preliminaries -- 3 A Single Object -- 4 Multiple Objects -- References.
Perpetual Torus Exploration by Myopic Luminous Robots -- 1 Introduction -- 2 Related Work -- 3 Model -- 4 Impossibility Results -- 5 Visibility Range One: A32 -- 6 Visibility Range Two: A41 -- 7 Conclusion -- References -- Optimal Algorithms for Synchronous Byzantine k-Set Agreement -- 1 Introduction -- 2 k-Set Agreement for n=3t, k=2 and t&gt -- 1 -- 2.1 Algorithm: Local Data Structures -- 2.2 Algorithm: Code of pi -- 2.3 Properties of a Matrix Mi -- 2.4 Basic Patterns: Squares and Regions -- 2.5 Proof of Correctness of Algorithm 1 -- 2.6 Finding Regions { R: =1,...,k} -- 2.7 Proof of Correctness of the Algorithm -- 3 Optimality -- 4 Conclusion -- References -- Reaching Consensus in the Presence of Contention-Related Crash Failures -- 1 Introduction -- 2 Computing Model -- 3 Base Algorithm (k=1): Consensus from Read/Write Registers -- 3.1 Presentation of the Algorithm -- 3.2 Proof of Algorithm 1 -- 4 General Algorithms (k1): Consensus from Objects whose Consensus Number is k -- 4.1 Presentation of Algorithm 2 -- 4.2 Further Explanations -- 4.3 Proof of Algorithm 2 -- 4.4 When k Divides n: Tolerating k-1 Classical Any-Time Failures -- 4.5 When k Divides n: Tolerating 2k-1 Contention-Related Crash Failures -- 5 Impossibility Results -- 6 Conclusion -- References -- Self-stabilizing Byzantine Fault-Tolerant Repeated Reliable Broadcast -- 1 Introduction -- 2 System Settings for BAMPn,t [FC,t &lt -- n/3] -- 3 The Non-Self-Stabilizing BT Algorithm -- 4 Self-

stabilizing Byzantine-Tolerant Single-Instance BRB -- 5 Self-stabilizing Recycling in Node-Failure-Free Systems -- 6 SSBFT BRB Recycling via Muteness Detection -- 7 Discussion -- References -- Capacity Planning for Dependable Services -- 1 Introduction -- 2 System Design -- 3 Implementation -- 4 Evaluation -- 4.1 Experimental Measurements -- 4.2 Dependability Evaluation -- 5 Conclusion -- References.
Lower Bound for Constant-Size Local Certification -- 1 Introduction -- 1.1 Three Typical Regimes for the Certificate Sizes -- 1.2 Motivation for Studying the Constant-Size Regime -- 1.3 Our Results and Techniques -- 2 Models and Definitions -- 3 k-colorability Does Not Have a Binary Certification -- 3.1 Indistinguishability Setting -- 3.2 Notion of Score -- 3.3 Our Graph Construction and Its Properties -- 3.4 Anonymous Case -- 3.5 Extension to Identifiers -- 4 Going Below "4264306 logk "5265307 -- 5 Challenges and Open Questions -- References -- Collaborative Dispersion by Silent Robots -- 1 Introduction -- 1.1 Background -- 1.2 Motivation and Problem Definition -- 1.3 The Model -- 1.4 Our Contribution -- 1.5 Related Works -- 2 Dispersion on Graphs -- 2.1 The Algorithm -- 2.2 Correctness and Analysis -- 3 Conclusion -- References -- Time Optimal Gathering of Myopic Robots on an Infinite Triangular Grid -- 1 Introduction -- 1.1 Background and Motivation -- 1.2 Earlier Works -- 1.3 Our Contribution -- 2 Models and Definitions -- 2.1 Model -- 2.2 Notations and Definitions -- 2.3 Problem Definition -- 3 Impossibility Result -- 4 Gathering Algorithm -- 4.1 Correctness Results: -- 4.2 Complexity Analysis -- 5 Conclusion -- References -- Card-Based ZKP Protocol for Nurimisaki -- 1 Introduction -- 2 Preliminaries -- 2.1 Pile-Shifting Shuffle ch19ShinagawaIEICE2017,ch19NishimuraIEICE18 -- 2.2 Input-Preserving Five-Card Trick ch19MiyaharaFUN2020 -- 2.3 Mizuki-Sone Copy Protocol ch19MizukiFAW09 -- 2.4 How to Form a White Polyomino ch19RobertNGCO2022 -- 2.5 Sum in Z ch19RuangwisesTCS2021 -- 3 ZKP Protocol for Nurimisaki -- 3.1 Setup Phase -- 3.2 Connectivity Phase -- 3.3 Verification Phase -- 4 Security Proofs -- 5 Conclusion -- References -- Consensus on Demand -- 1 Introduction -- 2 Model -- 3 Problem Statement -- 4 Related Work -- 5 A Simple Payment System.
6 Consensus on Demand -- 7 Discussion -- 8 Implementation -- References -- Better Incentives for Proof-of-Work -- 1 Introduction -- 1.1 Blockchain Game -- 1.2 Our Contribution -- 1.3 Intuitive Overview -- 2 Model and Preliminaries -- 2.1 Rounds -- 2.2 Players -- 2.3 Blocks -- 2.4 DAG -- 2.5 Mining -- 2.6 Action Space -- 3 The Block DAG -- 3.1 Block Order -- 4 Reward Schemes -- 4.1 Stale Blocks -- 4.2 Discussion of Flat Rewards -- 4.3 Penalizing Deviations -- 4.4 Nash Equilibria -- 4.5 Hurting Other Players -- 5 Related Work -- 5.1 Selfish Mining -- 5.2 DAG -- 5.3 Fruitchains -- 5.4 Bribery -- 6 Conclusions -- References -- Brief Announcements -- Brief Announcement: Self Masking for Hardening Inversions -- 1 Introduction -- 1.1 Preliminaries -- 1.2 Previous Work -- 1.3 Contribution -- References -- Brief Announcement: Dynamic Graph Models for the Bitcoin P2P Network: Simulation Analysis for Expansion and Flooding Time -- 1 Introduction -- 2 Edge-Dynamic RAES (E-RAES) -- 3 Vertex-Dynamic RAES (V-RAES) -- References -- Brief Announcement: Fully Lattice Linear Algorithms -- 1 Introduction -- 2 Preliminaries and Background -- 3 Lattice Linear Algorithms: Minimal Dominating Set -- 4 Convergence Time in Traversing a Lattice of States -- 5 Related Work -- 6 Conclusion -- References -- Brief Announcement: Distributed Reconfiguration of Spanning Trees -- 1 Introduction -- 1.1 Related Work -- 2 Distributed Spanning Tree

Reconfiguration -- 2.1 1-Simultaneous Add and Delete Requires (n) Rounds -- 2.2 2-Simultaneous Add and Delete in O(logN) Rounds -- References -- Brief Announcement: Mutually-Visible Uniform Circle Formation by Asynchronous Mobile Robots on Grid Plane -- 1 Introduction -- 2 Model and Problem Definition -- 3 Uniform Circle Formation -- 4 Uniform Circle Formation with Complete Visibility -- References.
Brief Announcement: Self-stabilizing Total-Order Broadcast.