Volume Editor

Shlomi Dolev
Ben-Gurion University of the Negev
Beer-Sheva, Israel
E-mail: dolev@cs.bgu.ac.il
Preface

DISC, the International Symposium on DiStributed Computing, is an annual forum for presentation of research on all facets of distributed computing, including the theory, design, analysis, implementation, and application of distributed systems and networks. The 20th anniversary edition of DISC was held on September 18-20, 2006, in Stockholm Sweden.

There were 145 extended abstracts submitted to DISC this year, and this volume contains the 35 contributions selected by the program committee and one invited paper among these 145 submissions. All submitted papers were read and evaluated by at least three program committee members, assisted by external reviewers. The final decision regarding every paper was taken during the program committee meeting, which took place in Beer-Sheva, June 30th and July 1st, 2006.

The Best Student Award was split and given to two papers: the paper “Exact Distance Labelings Yield Additive-Stretch Compact Routing Schemes”, by Arthur Bradley, and Lenore Cowen, and the paper “A Fast Distributed Approximation Algorithm for Minimum Spanning Trees” co-authored by Maleq Khan and Gopal Pandurangan.

The proceedings also include 13 three-page-long Brief Announcements (BA). These BAs are presentations of ongoing works for which full papers are not ready yet, or of recent results whose full description will be soon or has been recently presented in other conferences. Researchers use the brief announcement track to quickly draw the attention of the community to their experiences, insights and results from ongoing distributed computing research and projects. The BAs included in this proceedings were selected among 26 BA submissions.

DISC 2006 is organized in cooperation with the European Association for Theoretical Computer Science (EATCS) and the European Research Consortium for Informatics and Mathematics (ERCIM), Swedish Institute of Computer Science (SICS). The support of Ben-Gurion University, Microsoft Research, Intel, Sun Microsystems, Deutsche Telekom Laboratories is also gratefully acknowledged.

July 2006

Shlomi Dolev
DISC 2006 Program Chair
DISC at its 20th anniversary: Past, Present and Future

Michel Raynal¹, Sam Toueg² and Shmuel Zaks³

¹ IRISA, Campus de Beaulieu, 35042 Rennes, France.
² Department of Computer Science, University of Toronto, Toronto, Canada.
³ Department of Computer Science, Technion, Haifa, Israel

Prologue

DISC 2006 marks the 20th anniversary of the DISC conferences. We list below the special events that took place during DISC 2006, together with some information and perspectives on the past and future of DISC.

Present: Special 20th anniversary events

The celebration of the 20th anniversary of DISC consisted in four main events: invited talks by three of the brightest figures of the distributed computing community, and a panel involving all the people who were at the very beginning of DISC:

- An invited talk “Time, clocks and the ordering of my ideas about distributed systems” by Leslie Lamport.
- An invited talk “Provably unbreakable hyper-encryption using distributed systems” by Michael Rabin.
- A panel on “The contributions of the W DAG/DISC community to distributed computing: a historical perspective” by Eli Gafni, Jan van Leeuwen, Michel Raynal, Nicola Santoro and Shmuel Zaks (who were the PC members of the second W DAG, Amsterdam, 1987).

Past: a short history

The Workshop on Distributed Algorithms on Graphs (WDAG) was initiated by Eli Gafni, Nicola Santoro and Jan van Leeuwen in 1985. It was intended to provide a forum for researchers and other interested parties to present and discuss recent results and trends in the design and analysis of distributed algorithms on communication networks and graphs.
Then, more than 10 years later, the acronym WDAG was changed to DISC (the international symposium on DIStributed Computing). This change was made to reflect the expansion from a workshop to a symposium as well as the expansion of the research areas of interest. So, following 11 successful WDAGs, DISC’98 was the 12th in the series.

Since 1996 WDAG/DISC has been managed by a Steering Committee consisting of some of the most experienced members of the distributed computing community. The main role of this committee is to provide guidance and leadership to ensure the continuing success of this conference. To do so, the committee oversees the continuous evolution of the symposium’s research areas of interest, it forges ties with other related conferences and workshops, and it also maintains contact with Springer-Verlag and other professional or scientific sponsoring organizations (such as EATCS). The structure and rules of the DISC Steering Committee, which were composed by Sam Toueg and Shmuel Zaks, and approved by the participants at the the 1996 WDAG business meeting in Bologna, can be found at http://www.dsic-conference.org. This site also contain information about previous WDAG and DISC conferences.

The location, program chairs, and proceedings of the past 20 WDAG/DISC meetings are summarized in Table 1, and the Steering Committee Chairs are listed in Table 2.

<table>
<thead>
<tr>
<th>Year</th>
<th>Location</th>
<th>Program Chair(s)</th>
<th>Proceedings</th>
</tr>
</thead>
<tbody>
<tr>
<td>1985</td>
<td>Ottawa</td>
<td>N. Santoro and J. van Leeuwen</td>
<td>Carleton Scientific</td>
</tr>
<tr>
<td>1987</td>
<td>Amsterdam</td>
<td>J. van Leeuwen</td>
<td>LNCS 312</td>
</tr>
<tr>
<td>1989</td>
<td>Nice</td>
<td>J.-Cl. Bermond and M. Raynal</td>
<td>LNCS 392</td>
</tr>
<tr>
<td>1990</td>
<td>Bari</td>
<td>N. Santoro and J. van Leeuwen</td>
<td>LNCS 486</td>
</tr>
<tr>
<td>1991</td>
<td>Delphi</td>
<td>S. Toueg and P. Spirakis</td>
<td>LNCS 579</td>
</tr>
<tr>
<td>1992</td>
<td>Haifa</td>
<td>A. Segall and S. Zaks</td>
<td>LNCS 647</td>
</tr>
<tr>
<td>1993</td>
<td>Lausanne</td>
<td>A. Schiper</td>
<td>LNCS 725</td>
</tr>
<tr>
<td>1994</td>
<td>Terschelling</td>
<td>G. Tel and P. Vitányi</td>
<td>LNCS 857</td>
</tr>
<tr>
<td>1995</td>
<td>Le Mont-Saint-Michel</td>
<td>J.-M. Héray and M. Raynal</td>
<td>LNCS 972</td>
</tr>
<tr>
<td>1996</td>
<td>Bologna</td>
<td>O. Babaoglu and K. Marzullo</td>
<td>LNCS 1151</td>
</tr>
<tr>
<td>1997</td>
<td>Saarbrücken</td>
<td>M. Mavronicolas and Ph. Tsigas</td>
<td>LNCS 1320</td>
</tr>
<tr>
<td>1998</td>
<td>Andros</td>
<td>S. Kutten</td>
<td>LNCS 1499</td>
</tr>
<tr>
<td>1999</td>
<td>Bratislava</td>
<td>P. Jayanti</td>
<td>LNCS 1693</td>
</tr>
<tr>
<td>2000</td>
<td>Toledo</td>
<td>M. Herlihy</td>
<td>LNCS 1914</td>
</tr>
<tr>
<td>2001</td>
<td>Lisbon</td>
<td>J. Welch</td>
<td>LNCS 2180</td>
</tr>
<tr>
<td>2002</td>
<td>Toulouse</td>
<td>D. Malkhi</td>
<td>LNCS 2508</td>
</tr>
<tr>
<td>2003</td>
<td>Sorrento</td>
<td>F.E. Fich</td>
<td>LNCS 2848</td>
</tr>
<tr>
<td>2004</td>
<td>Amsterdam</td>
<td>R. Guerraoui</td>
<td>LNCS 3274</td>
</tr>
<tr>
<td>2005</td>
<td>Cracow</td>
<td>P. Fraignaud</td>
<td>LNCS 3724</td>
</tr>
<tr>
<td>2006</td>
<td>Stockholm</td>
<td>S. Dolev</td>
<td>LNCS 4167</td>
</tr>
</tbody>
</table>

Table 1. The past WDAG/DISC
Epilogue, and Future

Together with the whole DISC community, we congratulate DISC for its 20th anniversary. We feel proud to have taken part in this important and successful activity of our research community, and are confident that DISC will continue to play a central role in years to come.

We wish to thank all those who contributed over the years to the success of DISC. Each played an essential role, and each forms a vital link in the DISC chain:

- The local organizers, and their teams, who did everything to ensure a smooth and successful conference,
- The program committee chairs, program committee members, and external referees, who ensured the high academic level of the conference,
- The participants of the WDAG and DISC conferences,
- The steering committee members,
- The sponsor organizations, for their generous support over the years, and - last but not least -
- All the members of the distributed computing community who submitted papers to WDAG and DISC.

We are confident that the DISC community will continue to play a central role within the distributed computing and communication networks research communities for many years to come.

HAPPY ANNIVERSARY TO DISC!

This photo is from DISC 2005 in Cracow, Poland, and was taken during the banquet at Wierzynek 136 restaurant (one of the oldest restaurants in Europe). It shows the first five chairs of the DISC steering committee (from left to right: Shmuel Zaks, Alex Shivartsman, Michel Raynal, André Schiper and Sam Toueg).
INVITED TALK I

Provably Unbreakable Hyper-Encryption Using Distributed Systems

Michael O. Rabin
DEAS Harvard University
Cambridge, MA 02138
rabin@deas.harvard.edu

Encryption is a fundamental building block for computer and communications technologies. Existing encryption methods depend for their security on unproven assumptions. We propose a new model, the Limited Access model for enabling a simple and practical provably unbreakable encryption scheme. A voluntary distributed network of thousands of computers each maintain and update random pages, and act as Page Server Nodes. A Sender and Receiver share a random key K. They use K to randomly select the same PSNs and download the same random pages. These are employed in groups of say 30 pages to extract One Time Pads common to S and R. Under reasonable assumptions of an Adversary’s inability to monitor all PSNs, and easy ways for S and R to evade monitoring while downloading pages, Hyper Encryption is clearly unbreakable. The system has been completely implemented.

Modern encryption methods depend for their security on assumptions concerning the intractability of various computational problems such as the factorization of large integers into prime factors or the computation of the discrete log function in large finite groups. Even if true, there are currently no methods for proving such assumptions. At the same time, even if these problems will be shown to be of super-polynomial complexity, there is steady progress in the development of practical algorithms for the solution of progressively larger instances of the problems in question. Thus there is no firm reason to believe that any of the encryptions in actual use is now safe, or an indication as to how long it will remain so. Furthermore, if and when the current intensive work on Quantum Computing will produce actual quantum computers, then the above encryptions will succumb to these machines.

At present there are three major proposals for producing provably unbreakable encryption methods. Quantum Cryptography employs properties of quantum mechanics to enable a Sender and Receiver to create common One Time Pads (OTPs) which are secret against any Adversary. The considerable research and development work as well as the funding invested in this effort are testimony to the need felt for an absolutely safe encryption technology. At present Quantum Cryptography systems are limited in range to a few tens of miles, are sensitive to noise or disturbance of the transmission medium, and require rather expensive special equipment.

The Limited Storage Model was proposed by U. Maurer. It postulates a public intensive source of random bits. An example would be a satellite or a
system of satellites containing a Physical Random Number Generator (PRNG) beaming down a stream of random numbers, say at the rate of 100GB/sec. S and R use a small shared key, and use those bits and the key to form OTPs which are subsequently employed in the usual manner to encrypt messages. The Limited Storage Model further postulates that for any Adversary or group of Adversaries it is technically or financially infeasible to store more than a fraction, say half, as many bits as there are in a. It was proved by Aumann, Rabin, and Ding and later by Dziembowski-Maurer, that under the Limited Storage Model assumptions, one can construct schemes producing OTPs which are essentially random even for a computationally unbounded (but storage limited) Adversary. The critique of the Limited Storage Model is three-fold. It requires a system of satellites, or other distribution methods, which are very expensive. The above rate of transmission for satellites is right now outside the available capabilities. More fundamentally, with the rapid decline of cost of storage it is not clear that storage is a limiting factor. For example, at a cost of $1 per GB, storing the above mentioned stream of bytes will cost about $3 Billion per year. And the cost of storage seems to go down very rapidly.

The Limited Access Model postulates a system comprising a multitude of sources of random bytes available to the Sender and Receiver. Each of these sources serves as a Page Server Node (PSN) and has a supply of random pages. Sender and Receiver initially have a shared key K. Using K, Sender and Receiver asynchronously in time access the same PSNs and download the same random pages. The Limited Access assumption is that an Adversary cannot monitor or compromise more than a fraction of the PSNs while the Sender or Receiver download pages. After downloading sufficiently many pages, S and are make sure that they have the same pages by employing a Page Reconciliation Protocol. They now employ the common random pages according to a common scheme in groups of, say, 30 pages to extract an OTP from each group. Let us assume that the extraction method is simply taking the XOR of these pages. The common OTPs are used for encryption in the usual manner.

A crucially important point is that a Page Server Node sends out a requested random page at most twice, then destroys and replaces it by a new page. Opportunity knocks only twice!

Why is this scheme absolutely secure? Assume that we have 5,000 voluntary participants acting as PSNs. Assume that a, possibly distributed, Adversary can eavesdrop, monitor or corrupt (including by acting as imposter) no more than 1000 of these nodes. Thus the probability that in the random choice of the 30 PSNs from which a group of 30 pages are downloaded and XORed, all 30 pages will be known to the Adversary is smaller than \((1/5)^{30}\), i.e., totally negligible. But if an Adversary misses even one page out of the 30 random pages that are XORed into an OTP then the OTP is completely random for him.

The send at most twice, then destroy policy, prevents a powerful Adversary from asking for a large number of pages from each of the PSNs and thereby gain copies of pages common to S and R. The worst that can happen is that, say, S will down load a page \(P\) from PSN\(i\) and the Adversary (or another user of
Hyper-Encryption) has or will download the same page P from PSNi. When R
now requests according to the key K the same page from PSNi, he will not get
it. So R and S never have a page P in common if P was also downloaded by
a third party. The only consequence of an Adversary’s down-loading from too
many PSNs is denial of service to the legitimate users of the system. This is a
problem for any server system and there are ways of dealing with this type of
attack.

What if an Adversary eavesdrops onto the Sender and or Receiver while they
are downloading pages from PSNs. Well, S and R can go to an Internet café or
one of those establishments allowing a customer to obtain an Internet connection.
They can use a device that does not identify them and download thousands of
pages from PSNs within a short time. The salient point is that S and R need not
time-synchronize their access to the PSNs. Once S and R have common OTPs,
they can securely communicate from their fixed known locations with immunity
against eavesdropping or code breaking.

The initial key K is continually extended and updated by S and R using
common One Time Pads. Each pair of random words from K is used to select a
PSN and a page from that PSN only once and then discarded. This is essential
for the absolute security of Hyper Encryption.

With all these provisions Hyper Encryption in the Limited Access Model also
provides Ever Lasting Secrecy. Let us make a worst case assumption that the
initial common key K or its later extensions were lost or stolen after their use
to collect common random pages from PSNs. Those pages are not available any
more as a result of the send only twice and destroy policy. Thus the extracted
OTPs used to encrypt messages cannot be reconstructed and the encryption is
valid in perpetuity. By contrast, all the existing public or private key encryption
methods are vulnerable to the retroactive decryption attack if the key is lost or
algorithms come up that break the encryption algorithm.

We shall also describe an additional scheme based on the use of search engines
for the generation of OTPs and of unbreakable encryption.

Our systems were fully coded in Java for distribution as freeware amongst
interested users. All the protocols described below are running in the background
on the participating computers and impose negligible computational and storage
overheads on the host computer.
INVITED TALK II

Time, Clocks, and the Ordering of My Ideas
about Distributed Systems

Leslie Lamport

Microsoft Corporation
1065 La Avenida
Mountain View, CA 94043
U.S.A.
lamport@microsoft.com

A guided tour through the labyrinth of my thoughts, from the Bakery Algorithm to arbiter-free marked graphs. This exercise in egotism is by invitation of the DISC 20th Anniversary Committee. I take no responsibility for the choice of topic.
INVITED TALK III
My Early Days in Distributed Computing
Theory: 1979-1982

Nancy Lynch

CSAIL, MIT
Cambridge, MA 02139
U.S.A.
lynch@theory.cslai.mit.edu

I first became involved in Distributed Computing Theory around 1978 or 1979, as a new professor at Georgia Tech. Looking back at my first few years in the field, approximately 1979-1982, I see that they were tremendously exciting, productive, and fun. I collaborated with, and learned from, many leaders of the field, including Mike Fischer, Jim Burns, Michael Merritt, Gary Peterson, Danny Dolev, and Leslie Lamport.

Results that emerged during that time included space lower bounds for mutual exclusion; definition of the k-exclusion problem, with associated lower bounds and algorithms; the Burns-Lynch lower bound on the number of registers needed for mutual exclusion; fast network-wide resource allocation algorithms; the Lynch-Fischer semantic model for distributed systems (a precursor to I/O automata); early work on proof techniques for distributed algorithms; lower bounds on the number of rounds for Byzantine agreement; definition of the approximate agreement problem and associated algorithms; and finally, the Fischer-Lynch-Paterson impossibility result for consensus.

In this talk, I will review this early work, trying to explain how we were thinking at the time, and how the ideas in these projects influenced later work.
Panel on the Contributions of the DISC Community to Distributed Computing: a Historical Perspective

Eli Gafni\textsuperscript{a}, Jan van Leeuwen\textsuperscript{b}, Michel Raynal\textsuperscript{c}, Nicola Santoro\textsuperscript{d} and Shmuel Zaks\textsuperscript{e}

\textsuperscript{a}: UCLA, CA, USA \texttt{eli@cs.ucla.edu}
\textsuperscript{b}: Utrecht University, The Netherlands \texttt{jan@cs.uu.nl}
\textsuperscript{c}: IRISA, Université de Rennes, France \texttt{raynal@irisa.fr}
\textsuperscript{d}: Carleton University, Ottawa, Canada \texttt{santoro@scs.carleton.ca}
\textsuperscript{e}: The Technion, Haifa, Israel \texttt{zaks@cs.technion.ac.il}

This panel discussed the contributions of the DISC community to distributed computing. The panelists (Eli Gafni, Jan van Leeuwen, Nicola Santoro, Shmuel Zaks) and the moderator (Michel Raynal) were the members of the program committee of the second DISC (called WDAG at that time), held in Amsterdam.

At the very beginning, WDAG was centered mainly on distributed algorithms on graphs. Subsequently, while keeping its main focus on distributed algorithms, WDAG evolved and adopted a more general view of the research area, changed its name and became DISC. In a continuous manner, new topics have always appeared in the DISC call for papers (and also in accepted papers!). These include ubiquitous computing, cryptography, autonomic computing to name only a few. The scientific DISC contributions are numerous. They are on distributed computing models, algorithm design, complexity, possibility/impossibility results, distributed computability, lower bounds, etc. The panel reviewed the status of many contributions to network protocol design and to the understanding of distributed computing in general. It also discussed the possible ways in which DISC may evolve in the future.
Organization

DISC, the International Symposium on DIStributed Computing, is an annual forum for research presentations on all facets of distributed computing. The symposium was called the International Workshop on Distributed Algorithms (WDAG) from 1985 to 1997. DISC 2006 is organized in cooperation with the European Association for Theoretical Computer Science (EATCS).

Steering Committee

Hagit Attiya  
Technion
Shlomi Dolev  
BGU
Pierre Fraigniaud  
Université Paris Sus
Rachid Guerraoui  
EPFL
Alexander Shvartsman  
UCONN, Chair
Paul Vitanyi  
CWI, vise-Chair
Roger Wattenhofer  
ETH Zurich

Organization Committee

Conference Chairs  
Lenka Carr-Motyckova, LUT, Luleå Tekniska Universitet
Seif Haridi, SICS, Swedish Institute of Computer Science AB

Program Chair  
Shlomi Dolev, Ben-Gurion University of the Negev

20th Anniversary Celebration Chair  
Michel Raynal IRISA, Université de Rennes

Web Chair  
Hélène Martin, SICS, Swedish Institute of Computer Science AB

Finance Chair  
Charlotta Jörsäter, SICS, Swedish Institute of Computer Science AB
Program Committee

Lenka Čarr-Motyckova  LUT
Shlomi Dolev  BGU, Program Chair
Christof Fetzer  Technische Universität Dresden
Tim Harris  Microsoft Research Cambridge
Maurice Herlihy  Brown University
Jaap-Henk Hoepman  RU Nijmegen
Prasad Jayanti  Dartmouth College
Dariusz Kowalski  University of Liverpool
Danny Krizanc  Wesleyan University
Fabian Kuhn  Microsoft Research Silicon Valley
Nancy Lynch  MIT
Anna Lysyanskaya  Brown University
Petros Maniatis  Intel Research Berkeley
Mark Moir  SUN Microsystems Laboratories
Seffi Naor  Microsoft Research and Technion
Marina Papatriantafillou  Chalmers University
Andrzej Pelc  Université du Québec
Michel Raynal  IRISA, Université de Rennes
André Schiper  EPFL
Gadi Taubenfeld  Interdisciplinary Center
Sébastien Tixeuil  Université Paris Sud
Frits Vaandrager  RU Nijmegen

Sponsors
Referees

<table>
<thead>
<tr>
<th>Ittai Abraham</th>
<th>Jittat</th>
<th>Ronen Kat</th>
<th>Rami Puzis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yehuda Afek</td>
<td>Fakharoenphol</td>
<td>Idit Keidar</td>
<td>Tomasz Radzik</td>
</tr>
<tr>
<td>Marcos Aguilera</td>
<td>Rui Fan</td>
<td>Alex Kesselman</td>
<td>Sylvia Ratnasamy</td>
</tr>
<tr>
<td>James Aspnes</td>
<td>Hugues Fauconnier</td>
<td>Ralf Klasing</td>
<td>Rodrigo Rodrigues</td>
</tr>
<tr>
<td>Hagit Attiya</td>
<td>Sasha Fedorova</td>
<td>Geir Koen</td>
<td>Mariusz Rokicki</td>
</tr>
<tr>
<td>Giklas Avoine</td>
<td>Eyal Felstain</td>
<td>Boris Koldehofer</td>
<td>Christian Scheideler</td>
</tr>
<tr>
<td>Liskov Barbara</td>
<td>Tim Finin</td>
<td>Kishori Konwar</td>
<td>Elad Michael Schiller</td>
</tr>
<tr>
<td>Amotz Bar-Noy</td>
<td>Hen Fitoussi</td>
<td>Marina Kopeetsky</td>
<td>Roberto Segala</td>
</tr>
<tr>
<td>Rida A. Bazzi</td>
<td>Pierre Fraigniaud</td>
<td>Maciej Kurowski</td>
<td>Ori Shalev</td>
</tr>
<tr>
<td>Amos Beimel</td>
<td>Nissim France</td>
<td>Klaus Kursawe</td>
<td>Nir Shavit</td>
</tr>
<tr>
<td>Fredik Bengtsson</td>
<td>Matt Franklin</td>
<td>Shay Kutten</td>
<td>Abhi Shelat</td>
</tr>
<tr>
<td>Vartika Bhandari</td>
<td>Eli Gafi</td>
<td>Limor Lahiani</td>
<td>Alex Shvartsman</td>
</tr>
<tr>
<td>Andreas Blass</td>
<td>Juan Garay</td>
<td>Kevin Lai</td>
<td>Radu Simineceanu</td>
</tr>
<tr>
<td>Paolo Boldi</td>
<td>Flavio Garcia</td>
<td>Zvi Lotker</td>
<td>Thanh Son</td>
</tr>
<tr>
<td>Glencora Borradaile</td>
<td>Vijay K. Garg</td>
<td>Victor Luchangco</td>
<td>Thanh Son Nguyen</td>
</tr>
<tr>
<td>Anat Bremler-Barr</td>
<td>Cyril Gavoille</td>
<td>Ritesh Madan</td>
<td>Paul Spirakis</td>
</tr>
<tr>
<td>Olga Brukman</td>
<td>Lezek Gasieniec</td>
<td>Adam Malinowski</td>
<td>Scott Stoller</td>
</tr>
<tr>
<td>Harry Buhrman</td>
<td>Roland Gemesi</td>
<td>Stéphane Messika</td>
<td>Michal Strojnowski</td>
</tr>
<tr>
<td>Chi Cao Minh</td>
<td>Chryssis Georgiou</td>
<td>Yves Metivier</td>
<td>Ram Swaminathan</td>
</tr>
<tr>
<td>Bernadette Charron-Bost</td>
<td>Sukumar Ghosh</td>
<td>Maria Meyerovich</td>
<td>Boleslaw K. Szymanski</td>
</tr>
<tr>
<td>Jingsen Chen</td>
<td>Andres Gidenstam</td>
<td>Maged Michael</td>
<td>Nesime Tatbul</td>
</tr>
<tr>
<td>Wei Chen</td>
<td>Seth Gilbert</td>
<td>Saya Mitra</td>
<td>Philippas Tsigas</td>
</tr>
<tr>
<td>Yan Chenyu</td>
<td>Mayer Goldberg</td>
<td>Emilia Monakhova</td>
<td>Nir Tzachar</td>
</tr>
<tr>
<td>Bogdan Chlebus</td>
<td>Maria Gradinaru</td>
<td>Achiour Mostefaoui</td>
<td>Shinya Umeno</td>
</tr>
<tr>
<td>Lukasz Cmiediewski</td>
<td>Michael Greenwald</td>
<td>Mikhail Nesterenko</td>
<td>Eli Upfal</td>
</tr>
<tr>
<td>Rachid Guerraoui</td>
<td>Calvin Newport</td>
<td>Sebastiano Vigna</td>
<td></td>
</tr>
<tr>
<td>Gregory Chockler</td>
<td>Phuong Ha Hoai</td>
<td>Tina Nolte</td>
<td>Jennifer Walter</td>
</tr>
<tr>
<td>Byung-Gon Chun</td>
<td>Yinnon Haviv</td>
<td>Bosz Patt-Shamir</td>
<td>Michael Warres</td>
</tr>
<tr>
<td>Mike Dahlin</td>
<td>Danny Hendler</td>
<td>Fernando Pedone</td>
<td>Mike Warres</td>
</tr>
<tr>
<td>Xavier Défago</td>
<td>Thomas Herault</td>
<td>David Peleg</td>
<td>Jennifer Welch</td>
</tr>
<tr>
<td>Carole Delporte-Gallet</td>
<td>Ted Herman</td>
<td>Franck Petit</td>
<td>Yang Xiang</td>
</tr>
<tr>
<td>Feodor Dragan</td>
<td>Chien-Chung</td>
<td>Kaustubh Phanse</td>
<td>Reuven Yagel</td>
</tr>
<tr>
<td>Michael Elkin</td>
<td>Michel Hurfin</td>
<td>Laurence Pilard</td>
<td>Praveen Yalagandula</td>
</tr>
<tr>
<td>Robert Ennals</td>
<td>Adam Iwanicki</td>
<td>Benny Pinkas</td>
<td>Piotr Zielinski</td>
</tr>
<tr>
<td>Leah Epstein</td>
<td>Tomas Johansson</td>
<td>Sara Porat</td>
<td>Michele Zito</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Guiseppe Prencipe</td>
<td>Uri Zwick</td>
</tr>
</tbody>
</table>
**Table of Contents**

Exploring Gafni's reduction land: from $\Omega^k$ to wait-free adaptive $(2p - \lceil \frac{p}{k} \rceil)$-renaming via $k$-set agreement .................................................. 1  
   Achour Mostefaoui, Michel Raynal, Corentin Travers

Renaming in Message Passing Systems with Byzantine Failures .......... 16  
   Michael Okun, Amnon Barak

Built-in Coloring for Highly-Concurrent Doubly-Linked Lists ............ 31  
   Hagit Attiya, Edsher Hillel

Fault-tolerant and Self-stabilizing Mobile Robots Gathering ............. 46  
   Xavier Défago, Maria Gradinariu, Stéphane Messika, Philippe Raipin-Pavédy

Fast Computation by Population Protocols With a Leader ............... 61  
   Dana Angluin, James Aspnes, David Eisenstat

On Self-Stabilizing Search Trees ........................................... 76  
   Doina Bein, Ajay K. Datta, Lawrence L. Larmore

Efficient Dynamic Aggregation ............................................... 90  
   Yitzhak Birk, Idit Keidar, Liran Liss, Assaf Schuster

Groupings and Pairings in Anonymous Networks ................................ 105  
   Jérémie Chalopin, Shantanu Das, Nicola Santoro

A New Proof of the GHS Minimum-spanning Tree Algorithm ............... 120  
   Yoram Moses, Benny Shimony

A Knowledge-Based Analysis of Global Function Computation ............ 136  
   Joseph Y. Halpren, Sabina Petride

Checking a Multithreaded Algorithm with +CAL ........................... 151  
   Leslie Lamport

Capturing Register and Control Dependence in Memory Consistency Models with Applications to the Itanium Architecture ....................... 164  
   Lisa Higham, Liliane Jackson, Jalal Kawash

Conflict Detection and Validation Strategies for Software Transactional Memory ................................................................. 179  
   Michael F. Spear, Virendra J. Marathe, William N. Scherer III, Michael L. Scott

Transactional Locking II ....................................................... 194
Less is More: Consensus Gaps Between Restricted and Unrestricted Objects ........................................ 209
        Yehuda Afek, Eran Shalom

One-Step Consensus Solvability ........................................ 224
        Taisuke Izumi, Toshimitsu Masuzawa

        Ran Canetti, Ling Cheung, Dilsun Kaynar, Moses Liskov, Nancy Lynch, Olivier Pereira, and Roberto Segala

On Consistency of Encrypted Files ................................... 255
        Alina Oprea, Michael K. Reiter

Agreeing to Agree: Conflict Resolution for Optimistically Replicated Data 270
        Michael B. Greenwald, Sanjeev Khanna, Keshav Kunal, Benjamin C. Pierce, Alan Schmitt

A Lazy Snapshot Algorithm with Eager Validation ........................ 285
        Torvald Riegel, Pascal Felber, Christof Fetzer

Bounded Wait-Free f-resilient Atomic Byzantine Data Storage Systems for an Unbounded Number of Clients .......... 300
        Rida A. Bazzi, Yin Ding

Time and Communication Efficient Consensus for Crash Failures ....... 315
        Bogdan S. Chlebus, Dariusz R. Kowalski

Subconsensus Tasks: Renaming is Weaker than Set Agreement ........... 330
        Eli Gafni, Sergio Rajasbaum, Maurice Herlihy

Exact Distance Labelings Yield Additive-Stretch Compact Routing Schemes ........................................... 341
        Arthur Brady, Lenore Cowen

A Fast Distributed Approximation Algorithm for Minimum Spanning Trees 356
        Maleq Khan, Gopal Pandurangan

On Randomized Broadcasting in Power Law Networks .................... 371
        Robert Elsasser

Distributed Approximation Algorithms in Unit-disk Graphs .............. 386
        A. Czygrinow, M. Hańczowiak

The Weakest Failure Detectors to Boost Obstruction-Freedom .......... 400
Rachid Guerraoui, Michal Kapalka, Petr Kouznetsov

Fully Adaptive Algorithms for Long-Lived Renaming .................. 414
Alex Brodsky, Faith Ellen, Philipp Woelfel

Constructing Shared Objects that are Both Robust and High-Throughput 429
Danny Hendler, Shay Kutten

Byzantine and Multi-writer K-quorums .............................. 444
Amitanand S. Aiyer, Lorenzo Alvisi, Rida A. Bazzi

On Minimizing the Number of ADMs in a General Topology
Optical Network ...................................................... 459
Michele Flammini, Mordechai Shalom, Shmuel Zaks

Robust Network Supercomputing with Malicious Processes .......... 474
Kishori M. Konwar, Sanguthevar Rajasekaran, Alexander A.
Shvartsman

Distributed Resource Allocation in Stream Processing .......... 489
Cathy H. Xia, James A. Broberg, Zhen Liu, Li Zhang

Low-latency Atomic Broadcast in the Presence of Contention ......... 504
Piotr Zielinski

Oblivious Gradient Clock Synchronization ............................ 519
Thomas Locher, Roger Wattenhofer

Brief Announcement: Abortable and Query-abortable Objects ....... 533
Marcos K. Aguilera, Svend Frolund, Vassos Hadzilacos, Stephanie
Lorraine Horn, Sam Toueg

Brief Announcement: Fault-Tolerant SemiFast Implementations of Atomic
Read/Write Registers .................................................. 536
Chryssis Georgiou, Nicolas C. Nicolaou, Alexander A. Shvartsman

Brief Announcement: Convergence Analysis of Scalable Gossip Protocols . 539
Stacy Patterson, Bassam Bamieh, Amr El Abbadi

Brief Announcement: Computing Automatically the Stabilization Time
Against the Best and the Worst Schedules .......................... 542
Joffroy Beauquier, Colette Johnen, Stéphane Messika

Brief Announcement: Many Slices are Better than One ............... 545
Vinit A. Ogale, Vijay K. Garg

Brief Announcement: on Augmented Graph Navigability ............... 548
Pierre Fraigniaud, Emmanuelle Lebhar, Zvi Lotker
Brief Announcement: Decoupled Quorum-based Byzantine-Resilient Coordination in Open Distributed Systems .......................... 551

Alysson Newes Bessani, Miguel Correia, Joni da Silva Fraga, Lau Cheuk Lung

Brief Announcement: Optimistic Algorithms for Partial Database Replication ................................................................. 554

Nicolas Schiper, Rodrigo Schmidt, Fernando Pedone

Brief Announcement: Performance Analysis of Cyclon, an Inexpensive Membership Management for Unstructured P2P Overlays .............. 557

François Bonnet, Frédéric Tronel, Spyros Voulgaris

Brief Announcement: Decentralized, Connectivity-Preserving, and Cost-Effective Structured Overlay Maintenance .......................... 560

Yu Chen, Wei Chen

Brief Announcement: Monitoring of Distributed Linear Computations..... 563

Anton Esin, Rostislav Yavorskiy, Nikolay Zemtsov

Brief Announcement: Communication-optimal Implementation of Failure Detector Class $P$ .................................................. 566

Mikel Larrea, Alberto Lafuente, and Joachim Wieland

Brief Announcement: Synchronous Distributed Algorithms for Node Discovery and Configuration in Multi-channel Cognitive Radio Networks .......... 569

Srinivasan Krishnamurthy, R. Chandrasekaran, Neeraj Mittal and S. Venkatesan

Author Index .............................................................................. 572
Author Index

Yehuda Afek 209
Marcos K. Aguilera 533
Amitanand S. Aiyer 444
Lorenzo Alvisi 444
Dana Angluin 61
James Aspnes 61
Hagit Attiya 31
Bassam Bamieh 539
Amnon Barak 16
Rida A. Bazzi 300, 444
Joffroy Beauquier 542
Doina Bein 76
Yitzhak Birk 90
François Bonnet 557
Arthur Brady 341
James A. Broberg 489
Alex Brodsky 414
Ran Canetti 239
Jérémie Chalopin 105
R. Chandrasekaran 569
Wei Chen 560
Yu Chen 560
Lau Cheuk Lung 551
Ling Cheung 239
Bogdan S. Chlebus 315
Miguel Correia 551
Lenore Cowen 341
A. Czygrinow 386
Shantanu Das 105
Joni da Silva Fraga 551
Ajoy K. Datta 76
Xavier Défago 46
Dave Dice 194
Yin Ding 300

David Eisenstat 61
Amr El Abbadi 539
Faith Ellen 414
Robert Elsässer 371
Anton Esin 563
Pascal Felber 285
Christof Fetzer 285
Michele Flammini 459
Pierre Fraigniaud 548
Svend Frolund 533
Eli Gafni 330
Vijay K. Garg 545
Chryssis Georgiou 536
Maria Gradinariu 46
Michael B. Greenwald 270
Rachid Guerraoui 400
M. Hańczowiak 386
Vassos Hadžilacos 533
Joseph Y. Halpren 136
Danny Hendler 429
Maurice Herlihy 330
Lisa Higham 164
Eshcar Hillel 31
Taisuke Izumi 224
LillAnne Jackson 164
Colette Johnen 542
Michal Kapalka 400
Jalal Kawash 164
Dilsun Kaynar 239
Idit Keidar 90
Cathy H. Xia 489
Rostislav Yavorskiy 563

Shmuel Zaks 459
Nikolay Zemtsov 563
Li Zhang 489
Piotr Zieliński 504