

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Mitsu Okada Ichiro Satoh (Eds.)

Advances in Computer Science - ASIAN 2006

Secure Software and Related Issues

11th Asian Computing Science Conference
Tokyo, Japan, December 6-8, 2006
Revised Selected Papers

Volume Editors

Mitsu Okada
Keio University
Japan
E-mail: mitsu@abelard.flet.keio.ac.jp

Ichiro Satoh
National Institute of Informatics
Japan
E-mail: ichiro@nii.ac.jp

Library of Congress Control Number: 2007943082

CR Subject Classification (1998): F.3, E.3, D.2.4, D.4.6-7, K.6.5, C.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

ISSN	0302-9743
ISBN-10	3-540-77504-8 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-77504-1 Springer Berlin Heidelberg New York

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12210770 06/3180 5 4 3 2 1 0

Gilles Kahn: A Humble Tribute

Gilles Kahn was one of the visionary leaders whose accomplishments will be remembered for generations. In fact, the ASIAN series of conferences owes a great deal to him. He saw long ago the need to harness Southeast Asia for the next generation. He kindly accepted to be on our Steering Committee and indeed took personal interest and physically participated in the 1995 and 2002 conferences. His sharp criticisms, suggestions and support helped nurture the ASIAN conference from its birth.

Two of his distinct fundamental contributions in computer science that have had a big impact are: natural semantics and a framework for distributed asynchronous computation (often referred to as Kahn's networks of processes). The first one provides a theory that allows computation of properties of programs. This has had a big impact on the development of programming environments from specifications. The latter has had tremendous impact on the specification of asynchronous computation and contributed in many ways to early UNIX development and to formal theories of concurrent processes including communicating sequential processes. Not only did he pioneer the foundational area of computer science or formal methods through his personal contributions, but he also enriched his involvement in the measures of commissioning reliable software for space rocket missions.

He was one of the early members of IRIA (INRIA's name then) and the architect of the INRIA Sophia Antipolis Center. His leadership vision can be seen in the way INRIA has grown in the areas of science and technology, industry cooperations and international relations.

Above all he was always a simple, accessible, charismatic person who was easy to talk to. The ASIAN series owes its growth to his support. It was a great privilege for us to have an opportunity to learn from his visionary leadership through this series of conferences.

Asian Computing Science Conference
Steering Committee

Preface

The series of annual Asian Computing Science Conferences (ASIAN) was initiated in 1995 by AIT, INRIA and UNU/IIST to provide a forum for researchers in computer science from the Asian region and to promote interaction with researchers from other regions. The first ten conferences were held, respectively, in Bangkok, Singapore, Katmandu, Manila, Phuket, Penang, Hanoi, Mumbai, Chiang Mai, and Kunming. The 11th ASIAN conference was held in Tokyo, Japan, December 6-8, 2006. Each year, the conference focuses on a different theme at the cutting edge of computer science research. The theme of ASIAN 2006 was secure software. Three distinguished speakers were invited to the conference:

- Li Gong (Windows Live China, Microsoft Corporation, China)
- John Mitchell (Stanford University, USA)
- Patrick Cousot (Ecole Normale Supérieure-Paris, France)

We had 115 submission papers. The Program Committee reviewed all the papers carefully and then selected 17 regular papers and 10 short papers. After the conference, 1 invited paper, 17 regular papers and 8 short papers were selected for this post-conference formal proceedings volume. We wish to thank the Program Committee members and the external referees for their work in selecting the contributed papers. The conference was sponsored by the National Institute of Informatics, the Embassy of France in Japan, INRIA, and Keio University. We thank the Steering Committee for inviting us to organize the 11th ASIAN conference in Japan. Finally, many thanks to S. Nakajima and his Local Organizing Committee, for their sustained efforts in the organization of the conference.

March 2007

Mitsuhiro Okada
Ichiro Satoh

Organization

ASIAN 2006 was sponsored by the National Institute of Informatics, the Embassy of France in Japan, INRIA, and Keio University.

Executive Committee

General Chairs	Aki Yonezawa (University of Tokyo, Japan) Philippe Codognet (Embassy of France in Japan)
Program Chairs	Mitsuhiro Okada (Keio University, Japan) Ichiro Satoh (National Institute of Informatics, Japan)
Organization Chair	Shin Nakajima (National Institute of Informatics, Japan)
Organization	Kensuke Fukuda (National Institute of Informatics, Japan) Soichiro Hidaka (National Institute of Informatics, Japan) Hiroschi Hosobe (National Institute of Informatics, Japan) Hiroyuki Kato (National Institute of Informatics, Japan) Michihiro Koibuchi (National Institute of Informatics, Japan)
Steering Committee	Stephane Grumbach (INRIA, France) Joxan Jaffar (NUS, Singapore) Gilles Kahn (INRIA, France) Kanchana Kanchanasut (AIT, Thailand) R.K. Shyamasundar (TIFR, India) Kazunori Ueda (Waseda University, Japan)

Program Committee

Iliano Cervesato (Carnegie Mellon University, Qatar)
Shigeru Chiba (Tokyo Institute of Technology, Japan)
Patrick Cousot (Ecole Normale Supérieure-Paris, France)
Anupam Datta (Stanford University, USA)
Yuxi Fu (Shanghai Jiaotong University, China)
Sumanta Guha (AIT, Thailand)
Masami Hagiya (University of Tokyo)
Joxan Jaffar (National University of Singapore, Singapore)

Kanchana Kanchanasut (AIT, Thailand)
Kenji Kono (Keio University, Japan)
Ching-Laung Lei (Taiwan National University, Taiwan)
Xavier Leroy (INRIA, France)
Ninghui Li (Purdue University, USA)
John Mitchell (Stanford University, USA)
Atsushi Ohori (Tohoku University, Japan)
Mitsuhiro Okada (Keio University, Japan)
Andreas Podelski (Freiburg University, Germany)
Michael Rusinowitch (INRIA-Lorraine/University of Nancy/CNRS, France)
Ichiro Satoh (National Institute of Informatics, Japan)
Etsuya Shibayama (Tokyo Institute of Technology, Japan)
L. Yohanes Stefanus (University of Indonesia, Indonesia)
Kazushige Terui (National Institute of Informatics, Japan)
Kazunori Ueda (Waseda University, Japan)

Sponsoring Institutions

National Institute of Informatics, Japan
The Embassy of France in Japan
INRIA, France
Keio University, Japan

The program committee thanks the following people for their assistance on the refereeing process.

Siva Anantharaman	Mastroeni Isabella	Isao Sasano
Stephan Arlt	Florent Jacquemard	Ichiro Satoh
Anindya Banerjee	Joxan Jaffar	Etsuya Shibayama
Adam Barth	Bertrand Jeannet	Rie Shigetomi
Julien Bertrane	Wen-Shenq Juang	Junji Shikata
Frédéric Besson	Shin-ya Katsumata	SeongHan Shin
Bruno Blanchet	Nguyen Tan Khoa	Yutaro Sugimoto
Mun Choon Chan	Kazukuni Kobara	Martin Sulzmann
Wei Ngan Chin	Kenji Kono	Yunfeng Tao
Samarjit Chakraborty	Kenichi Kourai	Yasuyuki Tsukada
Hong Chen	Steve Kremer	Mathieu Turuani
Kuan-Ta Chen	Ralf Kuesters	Kazunori Ueda
Yu-Shian Chen	Donggang Liu	Masashi Une
Shigeru Chiba	Francesco Logozzo	Daniele Varacca
Chansophea Chuon	Ken Mano	Laurent Vigneron
Veronique Cortier	Ziqing Mao	Razvan Voicu
Véronique Cortier	Yutaka Matsuno	Tep Vuthy
Jin Song Dong	Antoine Miné	Qihua Wang
Yuxin Deng	Mitchell	Bogdan Warinschi
Ling Dong	Ian Molloy	Martijn Warnier
Chun-I Fan	David Monniaux	Takuo Watanabe
Jérôme Feret	Francesco Zappa Nardelli	Hajime Watanabe
Benjamin Gregoire	Huu-Duc Nguyen	Xian Xu
Yonggen Gu	Qun Ni	Mitsuharu Yamamoto
Sumanta Guha	Shin-ya Nishizaki	Yoshisato Yanagisawa
Masami Hagiya	Yutaka Oiwa	Roland Yap
Goichiro Hanaoka	Mitsuhiro Okada	Eugene Zalinescu
Koji Hasebe	Olivier Perrin	Steve Zdancewic
Chaodong He	Tamara Rezk	Han Zhu
Chun-Ying Huang	Xavier Rival	Hengming Zou
Run-Junn Hwang	Arnab Roy	
Samuel Hym	Abhik Roychoudhury	
Katsuyoshi Iida	Takamichi Saito	

Table of Contents

ASIAN'2006

Security Evaluation of a Type of Table-Network Implementation of Block Ciphers	1
<i>Akira Matsunaga and Tsutomu Matsumoto</i>	
A Symbolic Intruder Model for Hash-Collision Attacks	13
<i>Yannick Chevalier and Mounira Kourjeh</i>	
A Denotational Approach to Scope-Based Compensable Flow Language for Web Service	28
<i>Huibiao Zhu, Geguang Pu, and Jifeng He</i>	
Certificateless Authenticated Two-Party Key Agreement Protocols	37
<i>Tarjei K. Mandt and Chik How Tan</i>	
FORM: A Federated Rights Expression Model for Open DRM Frameworks	45
<i>Thierry Sans, Frédéric Cuppens, and Nora Cuppens-Boulahia</i>	
A Method of Safety Analysis for Runtime Code Update	60
<i>Masatomo Hashimoto</i>	
Automata-Based Confidentiality Monitoring	75
<i>Gurvan Le Guernic, Anindya Banerjee, Thomas Jensen, and David A. Schmidt</i>	
Efficient and Practical Control Flow Monitoring for Program Security	90
<i>Nai Xia, Bing Mao, Qingkai Zeng, and Li Xie</i>	
Modular Formalization of Reactive Modules in COQ	105
<i>Ming-Hsien Tsai and Bow-Yaw Wang</i>	
Closing Internal Timing Channels by Transformation	120
<i>Alejandro Russo, John Hughes, David Naumann, and Andrei Sabelfeld</i>	
Responsiveness in Process Calculi	136
<i>Lucia Acciai and Michele Boreale</i>	
Normal Proofs in Intruder Theories	151
<i>Vincent Bernat and Hubert Comon-Lundh</i>	

Breaking and Fixing Public-Key Kerberos	167
<i>Iliano Cervesato, Aaron D. Jaggar, Andre Scedrov, Joe-Kai Tsay, and Christopher Walstad</i>	
Computational Soundness of Formal Indistinguishability and Static Equivalence	182
<i>Gergei Bana, Payman Mohassel, and Till Stegers</i>	
Secrecy Analysis in Protocol Composition Logic	197
<i>Arnab Roy, Anupam Datta, Ante Derek, John C. Mitchell, and Jean-Pierre Seifert</i>	
A Type-Theoretic Framework for Formal Reasoning with Different Logical Foundations	214
<i>Zhaohui Luo</i>	
On Completeness of Logical Relations for Monadic Types	223
<i>Śławomir Lasota, David Nowak, and Yu Zhang</i>	
A Spatial Logical Characterisation of Context Bisimulation	231
<i>Zining Cao</i>	
Information Hiding in the Join Calculus	240
<i>Qin Ma and Luc Maranget</i>	
Modeling Urgency in Component-Based Real-Time Systems	248
<i>Nguyen Van Tang, Dang Van Hung, and Mizuhito Ogawa</i>	
Maintaining Data Consistency of XML Databases Using Verification Techniques	256
<i>Khandoker Asadul Islam and Yoshimichi Watanabe</i>	
An Operational Semantics of Program Dependence Graphs for Unstructured Programs	264
<i>Souhei Ito, Shigeki Hagihara, and Naoki Yonezaki</i>	
Combination of Abstractions in the ASTRÉE Static Analyzer	272
<i>Patrick Cousot, Radhia Cousot, Jérôme Feret, Laurent Mauborgne, Antoine Miné, David Monniaux, and Xavier Rival</i>	
Proving Noninterference by a Fully Complete Translation to the Simply Typed λ -Calculus	301
<i>Naokata Shikuma and Atsushi Igarashi</i>	
Formalization of CTL* in Calculus of Inductive Constructions	316
<i>Ming-Hsien Tsai and Bow-Yaw Wang</i>	
Inferring Disjunctive Postconditions	331
<i>Corneliu Popeea and Wei-Ngan Chin</i>	

An Approach to Formal Verification of Arithmetic Functions in
Assembly 346
 Reynald Affeldt and Nicolas Marti

Author Index 361