EDITORIAL

This special issue comprises research papers which are extended versions of some among those presented at the International Workshop on Security Analysis of Systems: Formalisms and Tools (SASYFT 2004). SASYFT 2004 was held in Orléans (France) in June 2004 (`http://www.univ-orleans.fr/lifo/Events/SASYFT2004/`), with the aim of offering an occasion to those working in research areas such as

- modelling information flow analysis on (infinite-state) systems,
- modelling and analyzing cryptographic protocols,
- verification of security properties,
- case studies in security analysis,
- security in the context of real-time and mobility,
- formal models for electronic commerce protocols,
- software tools for security analysis,

to get together, and discuss some of the recent developments (formalisms or software), that are relevant to the analysis of systems from the viewpoint of security.

Besides papers based on a variety of formalisms: Process Algebras, Petri Nets, Automata and Grammars, Rewriting, Clausal Theorem Proving, Lambda Calculi and Extensions ..., the program of SASYFT 2004 also included four invited talks on the following specific aspects:

- *Towards a Hierarchy of Cryptographic Protocol Models*,
  by Catherine MEADOWS, Naval Research Lab, Washington DC (USA),
- *Verification of Cryptographic Protocols and Automated Deduction*
  by Jean GOUBAULT-LARRECQ, LSV, Ecole Normale Supérieure, Cachan (Fr.),
- *Priority Systems*,
  by Joseph SIFAKIS, VERIMAG, Grenoble (Fr.),
- *Towards Control of Resources for Synchronous Systems*,
  by Roberto AMADIO, LIF, Marseille (Fr.).

Four among the papers presented at SASYFT 2004 were pre-selected by the program committee in view of this JALC special issue; and the extended versions presented by the authors concerned then underwent the usual anonymous refereeing process meeting the journal's standards. Our warmest thanks to the referees for having accepted the work, and for their timely feedbacks which have greatly helped the authors in preparing their final versions.

A few words by way of presenting these papers. The work of Mathieu Baudet (*Random polynomial-time attacks and Dolev-Yao models*) extends the notion of Dolev-Yao models for security protocols with a notion of probabilistic computational time, rather than just with probabilities of success; the benefit of this extension is to account for non-standard operations – e. g., guessing a key or breaking a cryptographic primitive – that will be viewed as transitions labelled with non-polynomial times. The objective behind the work of Jing Chen (*Timed Extensions of π calculus*) is to incorporate a notion of time into π-calculus; two different views are presented: one where the actions are assumed to consume no time, and the other with the opposite assumption that every action (including the so-called internal action) consumes a fixed amount of time; the expressive power and the axiomatizabilty of both views are discussed and illustrated with examples. The work of Hervé Grall (*A Confinement Criterion for Securely Executing Mobile Code*) addresses the following question: Given that a mobile program is executed by a host system in a local environment, how to ensure that the local environment is secure?; the answer is a confinement criterion, based on a suitable type system; if the type of the local environment satisfies the criterion, then no mobile program can directly access a local resource. The work of Sébastien Limet and Gernot Salzer (*Basic Rewriting via Logic Programming, with an Application to the Reachability Problem*) presents a rewrite approach that can be useful for verifying certain infinite state systems; the technique consists in formulating a reachability problem as one on descendants with respect to a rewrite system, then viewing the rewrite program as a logic program.

Finally, we are greatly obliged to the editorial board of the Journal of Automata, Languages and Combinatorics, for having accepted to bring out this JALC special issue based on SASYFT 2004.

For the SASYFT 2004 Program Committee:

Siva Anantharaman (LIFO, Orléans, France)
Paul Gastin (LSV, ENS-Cachan, France)
Gaétan Hains (LIFO, Orléans, France)
John Mullins (CRAC, Ecole Polytechnique, Montréal, Canada)
Michael Rusinowitch (LORIA, Nancy, France)