11. Meeting of the

IFIP WG 1.6 on Term Rewriting

July 2, 2009, Brasilia, Brazil

9:00 – 9:30	Georg Moser: *Complexity Analysis of Term Rewrite Systems*
9:30 – 10:00	Chris Lynch: *Cap Unification: Application to Protocol Security modulo Homomorphic Encryption*
10:00 – 10:30	Coffee Break
10:30 – 11:00	Maribel Fernández: *A Rewriting Framework for the Composition of Access Control Policies*
11:00 – 12:00	Mauricio Ayala-Rincón: *Report on ISR 2009* followed by discussion on ISR
12:00 – 14:00	Lunch
14:00 – 14:30	Albert Rubio: *SMT in Termination*
14:30 – 15:00	Johannes Waldmann: *SMT Solvers for Termination Provers*
15:00 – 15:30	Business Meeting
15:30 – 16:00	Coffee Break

Georg Moser: *Complexity Analysis of Term Rewrite Systems*

In order to assess the complexity of a (terminating) TRS it is natural to look at the maximal length of derivations. Roughly such an analysis is conceivable as a worst-case complexity analysis of the functions computed by the given TRS. In the talk I will review well-established results in this area, but also present recent results on automatable techniques that verify that the given TRS admits at most polynomial (in the size of the start term) lengths of derivations.

Chris Lynch: *Cap Unification: Application to Protocol Security modulo Homomorphic Encryption*

We address the insecurity problem for cryptographic protocols, for an active intruder and a bounded number of sessions. The protocol steps are modeled as rigid Horn clauses, and the intruder abilities as an equational theory. The problem of active intrusion – i.e., whether a secret term can be derived, possibly via interaction with the honest participants of the protocol – is then formulated as a Cap Unification problem. Cap Unification is an extension of Equational Unification: look for a cap to be placed on a given set of terms, so as to unify it with a given term modulo the equational theory. We give a

decision procedure for Cap Unification, when the intruder capabilities are modeled as homomorphic encryption theory. Our procedure can be employed in a simple manner to detect attacks exploiting some properties of block ciphers.
This is joint work with Siva Anantharaman, Hai Lin, Paliath Narendran and Michael Rusinowitch.

Maribel Fernández: *A Rewriting Framework for the Composition of Access Control Policies*

In distributed environments where access control information may be shared across multiple sites, individual access control specifications need to be combined in order to define a coherent global policy. In order to ensure non-ambiguous behaviour, formal languages, often relying on first-order logic, have been developed for the description of access control policies. We propose a formalisation of policy composition by means of term rewriting. We will describe how, in this setting, we can express a wide range of policy combinations and reason about them. Modularity properties of rewrite systems will be used to derive the correctness of the global policy, i.e., that every access request has an answer and this answer is unique.

Albert Rubio: *SMT in Termination*

In this talk we show that the use of SAT Modulo Theories (SMT) techniques for developing polynomial constraint solvers outperforms the best existing solvers. Moreover, we will see that the SMT framework provides a new and powerful approach for implementing better and more general solvers for termination provers.

Johannes Waldmann: *SMT Solvers for Termination Provers*

To prove termination via interpretations, one needs coefficients of polynomials or matrices. The compatibility of the interpretation with the rewrite system is expressed as a constraint system.
We will review some constraint languages available in the SMT (Satisfiability Modulo Theory) framework, give typical encodings, and evaluate the performance of current SMT solvers on those problems.
We compare with “homegrown bitblasting”, that is, encoding integer numbers in binary and translating to a Boolean satisfiability problem. This seems to be the method of choice for current termination provers.
These experiments may lead to a more modular design of termination provers (by factoring out the constraint solvers), and help to connect the SMT and termination communities.