ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow:	Sasa Radomirovic
Visited Location :	NTNU
Duration of Visit:	1. November 2005 - 31. July 2006

I - Scientific activity

page at maximum)

The main theme of my research at NTNU was the composability of security protocols. There are two paradigms to study the security of protocols: *Universal Composability*, a theoretical framework, introduced by Ran Canetti in 2000, and the usually more practical Formal Methods. I have worked with both of these paradigms.

More specifically, I began by studying Universally Composable Security and proceeded to work with the security group at NTNU to prove a signcryption scheme secure in the Universal Composability framework using Formal Methods. This work has resulted in a paper accepted for the *Workshop on Formal and Computational Cryptography, FCC 2006*.

I have then extensively studied a Formal Method for verification of security protocols developed by Sjouke Mauw. In a collaboration with Sjouke Mauw's and NTNU's security group we have researched the composability of security protocols using this Formal Method. We have achieved significant progress and are expecting to submit our work soon.

More recently, I have studied Identity Based Encryption and given a talk on the subject in a security group workshop at NTNU. My research in this area is still in its early stages.

Throughout the tenure of my fellowship I have done research on counting restricted paths in certain graphs in collaboration with a researcher at the University of Auckland in New Zealand. This work has resulted in a paper submitted to the Electronic Journal of Combinatorics and is currently under review.

II- Publication(s) during your fellowship

Please insert the title(s), author(s) and abstract(s) of the published paper(s). You may also mention the paper(s) which were prepared during your fellowship period and are under reviewing.

Title: *An example of proving UC-realization with formal methods.*
Authors: Suzana Andova, Kristian Gjøsteen, Lillian Kråkmo, Stig Frode Mjølsnes and Sasa Radomirovic.

Abstract: In the universal composability framework we consider ideal functionalities for secure messaging and signcryption. Using traditional formal methods techniques we show that the secure messaging functionality can be UC-realized by a hybrid protocol that uses the signcryption functionality and a public key infrastructure functionality. We also discuss that the signcryption functionality can be UC-realized by a secure signcryption scheme.

Accepted at: Workshop on Formal and Computational Cryptography (FCC'06)

Title: *Restricted Walks in Regular Trees*
Authors: Laura Ciobanu, Sasa Radomirovic

Abstract: Let T be the Cayley graph of a finitely generated free group F. Given two vertices in T consider all the walks of a given length between these vertices that at a certain time must follow
a number of predetermined steps. We give formulas for the number of such walks by expressing the problem in terms of equations in F and solving the corresponding equations.

Submitted to: Electronic Journal of Combinatorics

III -Attended Seminars, Workshops, and Conferences

Please identify the name(s), date(s) and place(s) of the events in which you participated during your fellowship period.

I have given an invited presentation on my previous work in the Number Theory seminar in Barcelona (at UPC) on 16. December 2005, and at Massey University in New Zealand on 28. February 2006.
I have participated in and given presentations on my research activity at local workshops in January 2006 on Canetti's Universal Composability and in May 2006 on Identity-based encryption schemes. A related talk on Identity-based encryption schemes was given by me at the NTNU Mathematics Department on 14. June 2004.

I have attended a seminar on Formal Methods and Cryptography at CWI in Amsterdam on 9. March 2006.