ERCIM Alain Bensoussan Fellowship Programme

ABCDE Seminar II
24-25 October 2012
Sophia Antipolis, France

Dimitris E. Simos

INRIA Paris-Rocquencourt, France

SBA Research, Austria

ERCIM

MARIE CURIE ACTIONS

My Career

Positions

- 2012 – now: ERCIM Fellow, INRIA Rocquencourt, Project-Team SECRET, France

Education

- 2011: Ph.D. In Discrete Mathematics & Combinatorics, National Technical University of Athens, Greece
- 2007: M.Sc. In Applied Mathematical Sciences, National Technical University of Athens, Greece
- 2006: B.Sc. In Mathematics, University of Athens, Greece

Service in Academia

- 2012: Fellow of the Institute of Combinatorics & its Applications (FTICA)
- Editorial Board Member of AMIS, IJCM and ISL

Research Profile

- *Research Areas*: Combinatorial Designs, Coding Theory, Cryptography
- *Publication Record*: 1 Monograph (in progress) and 33 Papers in Discrete Mathematics

Code-based Cryptography

- Cryptosystems that resist attacks mounted by Quantum Computers
- Attacks include decoding (message security) and structural attacks (key security)

My Line of Research within INRIA

- Generalization of efficient algorithms for structural attacks on Code-based Cryptosystems

Current Status

- Development of a polynomial-time algorithm in some cases for the first time

What is Next ?

- Devise new zero-knowledge protocols that require little computing power for usage in telecommunications and industry (like mobile phones, PDA's and smart cards)

Collaboration between Hosts (INRIA – SBA Research)

SBA Research organized this year one of the leading conferences in Security (*International Conference on Availability, Reliability and Security* - ARES)

- Chaired the *1st International Workshop on Modern Cryptography and Security Engineering (MoCrySEn 2012)*, August 20-24, 2012, IEEE-CPS, Prague, Czech Republic (held in conjuction with ARES)

- Invited speaker from INRIA, Team SECRET

- *Aim* : Bridging the gap between academic cryptographers and security experts

My Dream

Contribution of ERCIM Fellowship so far

- Opportunity to collaborate with internationally recognized experts
- Benefit from high level working environments
- Broaden my research perspectives with new themes

Future Career Plans

- Lead a Scientific Team focused on R&D and promote the disciplines of Academic Cryptography and Industrial Security in a top-level EU Institute
- Obtain an EU Career Grant (like ERC or MC)
- Become an ERCIM representative for Greece