ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: LHOUSSAIN EL FADIL
Visited Location : NTNU, Norway
Duration of Visit: 12 months

I - Scientific activity

During this period, I worked in two areas:
1. General cryptology: Encryption and decryption based on linear sequences.
2. Computation in number theory: Computation of p-integral bases and Factorization of prime integers in quartic number fields.

In cryptology, the goal is to develop some encryption and decryption algorithms (Improving security and reducing the complexity). Based on linear sequences, many of works are done in this area. But the existing schemes are deterministic and are unsuitable for being directly used in special environments where semantic security is needed, such as the encryption of 0, 1.

II- Publication(s) during your fellowship

- A public-key cryptosystem based on third linear sequences (To appear in digital library of IEEE).
- Notes on the article "two methods for direct construction of probabilistic LFSR sequences of third order" (under reviewing).
- A Note on the article "A new public key encryption scheme based on Lucas sequences" (under reviewing).
- Explicite factorization of prime integer in quartic number fields defined by an irreducible trinomial X3+aX+b (under reviewing).
- Explicite factorization of prime integer in any quartic number fields (in preparation).

III -Attended Seminars, Workshops, and Conferences

- Catalan days of number theory, 26.01.2009-31.01.2009, "ub", Barcelona-Spain.
- ICMCS09, 02.04.2009-05.04.2009, Polydsciplinary faculty of Ouarzazate-Morocco.
- NIK 09, 23.11.2009-25.11.2009, "NTNU", Trondheim-Norway.
- Wotic09, 24.12.2009-25.12.2009, Faculty of scienc, Agadir-Morocco.

IV – Research Exchange Programme (12 month scheme)

- FNRS, 17.05.2009-02.06.2009 at Louvain-Belgium.
  During this period, I prepared the following “Separability of CP-graded ring”.

- Sparcim, 10.12.2009-16.12.2009 at Barcelone- Spain.
  During this period, I discussed with Professor Enric Nartat “UAB”, Montes algorithm which will help me to achieve the paper “Explicite factorization of prime integer in quartic number feilds”. I revised with Professor, Jorge Villar at “upc” the submited “A probabilitic crypto-system based on Lucas sequences”.