ERCIM “Alain Bensoussan”
Fellowship Scientific Report

Fellow: Javier Herranz Sotoca (contract number **2005-18**).
Visited Location: Centrum voor Wiskunde en Informatica (CWI, The Netherlands)
Duration of Visit: 9 months (01/02/2006 – 31/10/2006).

I - Scientific activity

During my stay in the ‘Cryptology and Information Security’ research group, headed by Ronald Cramer, in the Centrum voor Wiskunde en Informatica (CWI), I have worked mostly with Eike Kiltz and Dennis Hofheinz. In this case, since the research subjects of the members of this group are quite theoretical (relations between mathematics, theoretical computer science and cryptology), my research has focused on more theoretical topics than the ones I worked on during my previous stay at École Polytechnique (LIX). This research work has lead to two main results, described in two papers.

The first one has already been accepted for publication (see [P1] below) and deals with identity-based signature schemes with some special properties. Basically, we show that many of such schemes can be constructed in a generic way, starting from a standard signature scheme and from a PKI-based signature scheme with the desired properties. As an example of our construction, we detail the case of blind signatures, and show that the generic construction is even better than the specific identity-based blind signature schemes that had been proposed until now.

The second work deals with the KEM/DEM paradigm, which is well-known in the cryptographic community: to encrypt large messages in a public key setting, one first employs a KEM to encrypt a symmetric key K for the receiver, using his public key, and then one encrypts the message with a symmetric mechanism DEM, using the key K. The receiver can use his secret key to recover K and then decrypt the ciphertext to obtain the plaintext. In our work, we completely characterize which security notions of the KEM and the DEM are necessary, and which ones are sufficient, to ensure that the resulting hybrid encryption mechanism satisfies some of the existing levels of security for public key encryption. The manuscript containing this work can be found in: http://eprint.iacr.org/2006/265. An extended abstract will be submitted soon to an international conference.

During these 9 months, I have maintained the professional relation with some of the researchers with whom I worked during my stay (1st period or this ERCIM Fellowship) of 9 months in France. Specifically, we extended and generalized a previous work with Drs. Raghav Bhaskar and Fabien Laguillaumie; this paper has been accepted to be published in a journal (see [P2] below). Furthermore, Dr. Fabien Laguillaumie and I have written a paper (see [P3] below) about blind ring signature schemes, a kind of signature schemes which is very useful for real applications such as electronic cash or electronic voting systems.

Visit to Université Catholique de Louvaine (UCL)

I have spent two days of March 2006 in the Université Catholique de Louvaine-la-Neuve (Belgium), invited by the Crypto group of that university. There I gave a talk entitled ‘An

overview on aggregate signature schemes', and I worked with some members of the group about the application of distributed proxy signatures (a topic that I studied some years ago) to some of the practical problems they deal with.

Visit to Universitat Politècnica de Catalunya (UPC)

I have spent one week of September 2006 in the Universitat Politècnica de Catalunya (Spain), invited by the Mathematics Applied to Cryptography group of that university (where I obtained my PhD). There I worked on the one hand with Dr. Germán Sáez, and on the other hand I started a new collaboration with other members of that group: Dr. Paz Morillo, Dr. Vanesa Daza and Carla Ràfols. The collaboration with Dr. Sáez already comes from my PhD thesis, since he was my supervisor; Dr. Sáez and I have written a paper about secret sharing and multipartite access structures, which has been accepted to be published (see [P4] below).

Other work

- I have reviewed papers for international journals and conferences such as ICALP'06, Crypto'06, Asiacrypt'06, ICISC'06, Designs, Codes and Cryptography.
- I was a member of the Program Committee of the conference IS'06 (1st International Workshop on Information Security), to be held in Montpellier (France): October 30-November 1, 2006.

II- Publication(s) during your fellowship

[P1] David Galindo, Javier Herranz and Eike Kiltz. 'On the generic construction of identity-based signatures with additional properties'. Proceedings of Asiacrypt'06, Lecture Notes in Computer Science, 4284, pp. 178-193 (2006, to appear).

Abstract: It has been demonstrated by Bellare, Neven, and Namprempre (Eurocrypt 2004) that identity-based signature schemes can be constructed from any PKI-based signature scheme. In this paper we consider the following natural extension: is there a generic construction of ``identity-based signature schemes with additional properties'' (such as identity-based blind signatures, verifiably encrypted signatures, ...) from PKI-based signature schemes with the same properties? Our results show that this is possible for great number of properties including proxy signatures; (partially) blind signatures; verifiably encrypted signatures; undeniable signatures; forward-secure signatures; (strongly) key insulated signatures; online/offline signatures; threshold signatures; and (with some limitations) aggregate signatures.
Using well-known results for PKI-based schemes, we conclude that such identity-based signature schemes with additional properties can be constructed, enjoying some better properties than specific schemes proposed until know. In particular, our work implies the existence of identity-based signatures with additional properties that are provably secure in the standard model, do not need bilinear pairings, or can be based on general assumptions.

[P2] Raghav Bhaskar, Javier Herranz and Fabien Laguillaumie. 'Aggregate designated verifier signatures and application to secure routing'. To appear in the International Journal of Security and Networks, special issue on Cryptography in Networks (to appear in 2007).

Abstract: A designated verifier signature convinces only the specific recipient of the message of its integrity and origin. Following the notion of aggregate signature introduced by Boneh *et al.*, we introduce in this work the notion of *aggregate designated verifier signature*. After defining the protocols and the security model for such schemes, we give a general construction which is based on message authentication codes, and that can be extended to an identity-based scenario. The resulting schemes are proved to be secure under the CDH assumption, in the random oracle model. They are much more efficient than standard aggregate signature schemes, at the price of loosing some properties of standard signatures, in particular non-repudiation.
Finally we explain the possible application of aggregate designated verifier signatures to the authentication of messages in routing protocols. We compare our new scheme with existing standard aggregate signature schemes and show why our solution with aggregate designated verifier signatures is more suitable for securing routing in mobile ad-hoc networks.

[P3] Javier Herranz and Fabien Laguillaumie. 'Blind ring signatures secure under the chosen target CDH Assumption'. Proceedings of ISC'06, Lecture Notes in Computer Science, 4176, pp. 117-130 (2006).

Abstract: Blind signatures are a useful ingredient to design secure sophisticated systems like electronic voting or sensitive applications like e-cash. Multi-users signature schemes, like ring or group signatures, are also a useful tool to provide to such systems some properties like scalability, anonymity, (dynamic) group structure, revocation facilities… We propose in this article a simple blind ring signature scheme based on pairings on algebraic curves. We formally prove the security (anonymity, blindness and unforgeability) of our scheme in the random oracle model, under quite standard assumptions.

[P4] Javier Herranz and Germán Sáez. 'New results on multipartite access structures'. To appear in the journal IEE Proceedings of Information Security.

Abstract: In a multipartite access structure, the set of players is divided into K different classes, in such a way that all players of the same class play the same role in the structure. Not many results are known about these structures, when $K \geq 3$.
Even if the total characterization of ideal multipartite access structures seems a very ambitious goal, we take a first step in this direction. On the one hand, we detect some conditions that directly imply that a multipartite structure cannot be ideal. On the other hand, we introduce a new strategy which helps proving that a multipartite access structure is ideal, and we apply this strategy to three wide families of multipartite access structures.

III -Attended Seminars, Workshops, and Conferences

- SNDS 2006: 2nd International Workshop on Security in Networks and Distributed Systems. Vienna, Austria, April 18-20, 2006. Reimbursed by ERCIM. I presented there the paper 'Efficient authentication for reactive routing protocols', by Raghav Bhaskar, Javier Herranz and Fabien Laguillaumie.
- RECSI 2006: 9th Spanish Meeting on Cryptology and Information Security. Barcelona, Spain, September 7-9, 2006. Reimbursed by ERCIM. I presented there two papers: 'Time-based delegation of decryption capabilities' and 'New relations between graphs and ideal access structures', both by Javier Herranz.