1. *Interested institution:*

Universitat Politècnica de Catalunya
http://www.upc.edu/
Departament of Applied Mathematics IV
http://www.ma4.upc.edu/
Escola Tècnica Superior d'Enginyeria de Telecomunicació de Barcelona
http://www.etsetb.upc.edu/
Research Group on Mathematics Applied to Cryptography (MAK)
http://www-ma4.upc.edu/mak/

2. *Brief Description of the Institution*

The Universitat Politècnica de Catalunya (UPC) is a public university that specializes in the fields of architecture, engineering, merchant seamanship, economics, health sciences and applied mathematics. The UPC is very active in post-graduate education, with an offer of 65 Masters Adapted to the European Higher Education System (including 13 Erasmus Mundus master's programs funded by the European Commission), and 51 doctoral programs with "Mention of Quality" (25 of which with a distinction of excellence awarded by the Spanish Ministry of Education and Science and 7 Erasmus Mundus Joint Doctorates). These educational programs have traditionally attracted Spanish and Latin American students, although more recently, the increased visibility of Erasmus Mundus programs and an active policy of the University have secured a steady flow of excellent students from Europe and Asia.

In order to develop its international policy, UPC has joined a number of networks of universities of excellence, each of which has different objectives and dedicates its efforts in the joint work of prestige institutions to obtaining results that position us, provide visibility and lead the interests and strategies of the institution at the highest level.
http://www.upc.edu/sri/alliances/international-networks-to-which-upc-belongs/international-networks-to-which-upc-belongs?set_language=en

UPC continues its commitment to economic development and strengthening its continuing education programs through the UPC Foundation. UPC's Technology Transfer Center (TTC) is a substantial R&D contributor to Catalonia's industrial sector. UPC is currently working in over 250 research areas, and we have a growing number of specific research centers and regional technology centers focusing on current research needs. Regarding the transfer of knowledge domain, it is to highlight that the main goals of the Technology Transfer Center:
- Fostering innovation and technological progress in industry by transferring results and technology.
- Enhancing the participation and performance of UPC researchers in technological research and development projects

The center is responsible for the management and the administration of the research projects participated or lead by UPC researchers, along with those projects in which the UPC is acting as host institution, such as Marie Curie Actions. TTC works closely with Innova Program the unit in charge of the promotion of innovation and entrepreneurship throughout the university community researchers, allowing the creation of new businesses and result evaluation instruments knowledge. Innova together with UPC Legal Services plays an important role in the management of IPR and the design of exploitation plans for the research results. A wide portfolio of services is offered to the researchers in disseminating, protecting or commercializing these results, as for example Specific training courses, Advice on the patentability of the technology or Assessment and commercialization of research results closer to the needs of the business research groups, and vice versa.

The Research Group on Mathematics Applied to Cryptography (MAK) was created in 1992. The research activity is focused on the mathematical problems appearing in Cryptography, mainly in Public key Cryptography, Distributed Cryptography and Unconditionally Secure Cryptographic Protocols. It is actually one of the main research Spanish groups in mathematical cryptology, with presence in the main international conferences in the area (like Crypto, Eurocrypt, Asiacrypt, TCC and PKC) and with active collaborations with other research groups in Europe. More than 7 PhD theses were elaborated in the group during the last 10 years, and more than 35 international publications (in specialized journals and conference proceedings) in the last 5 years.

The MAK Research Group is located in the Campus Nord of Barcelona, which is very well connected to the city center and is assisted by the general services of the university such as the Campus Library, computer rooms and laboratories among other facilities.

3. *Please tick the areas of research (as established in Marie Sklodowska Curie Actions)*

☐ Chemistry (CHE)	☐ Environmental Sciences and Geology (ENV)
☐ Social Sciences and Humanities (SOC)	☐ Life Sciences (LIF)
☐ Economic Sciences (ECO)	☒ Mathematics (MAT)
☒ Information Science and Engineering (ENG)	☐ Physics (PHY)

4. *Research / Project Description*

In the last decade both the number of scientific publications and the new and different applications of cryptology beyond encryption and digital signatures grew exponentially fast, in parallel to the development of the Information Society. The new applications typically involve scenarios in which the potential number of users range from dozens to thousands, and the actions users can perform are far richer than just encrypting or signing messages. As a consequence, new theoretical and practical problems continuously challenged cryptographers in the last years. The research on most of these problems involved the use of new mathematical techniques like bilinear maps on elliptic curves, or ideal lattices, and some algebraic frameworks were developed, like the concepts of Hash Proof Systems or Lossy Trapdoor.

On the practical side, cryptography can be applied to a wide class of scenarios in which privacy, authenticity and/or confidentiality are necessary. Applications include for instance e-auctions, e-voting, pay TV, secure e-mail, e-commerce, e-contract signing or secure social networking. Dealing with a large number of potential users makes the design of such protocols a challenging task as there is a natural tradeoff between efficiency and security. This tradeoff often results in protocols which security can only be heuristically proved (i.e., by means of idealized computational models) and further research is needed to improve the known constructions to achieve provable security in the real world.

Our research focus on some of the most active topics in cryptologic research, ranging from the theoretical to the practical problems. The specific problem choice is based on the current state-of-the art and the research topics on which some researchers from reference international research centers are working.

Some of the current main topics are:

- Enhanced-Security for Public-Key Encryption, and Foundations of Security in Cryptographic Protocols
- Attribute-Based Cryptography and Applications to Access Control Systems
- Distributed Cryptosystems and Applications
- Security in Electronic Voting Protocols
- Security and Verifiability in Computation and Storage Outsourcing
- Secret Sharing and Multiparty Computation

5. *Who can apply?*

At the deadline for the submission of proposals (10/09/2015), researchers (*):

- shall be in possession of a doctoral degree or have at least four years of full-time equivalent research experience.
- must not have resided or carried out their main activities in the country of Spain for more than 12 months in the 3 years immediately prior to the abovementioned deadline.

6. *Contact person*

Associate Prof. Paz Morillo
e-mail: paz@ma4.upc.edu

Associate Prof. Jorge Luis Villar:
e-mail: jvillar@ma4.upc.edu

web: http://www-ma4.upc.edu/~jvillar/

7. *Applications: documents to be submitted and deadlines*

-Curriculum Vitae
-Motivation letter
-One or Two Recommendation letters

Please note that:

- Deadline of the next call for proposals for Marie Sklodowska – Curie Individual Fellowships is **September, 10th 2015.**
- Oficina Europea is only responsible for the display of the expressions of interests received by the institutions; further contact and information requests will take place directly between the host institutions and the interested researchers.

(*) Further details on the Call and additional eligibility criteria can be found at the Participants´Portal