Universidad Complutense de Madrid
Facultad de Ciencias Matemáticas
Departamento de Algebra, Geometría y Topología
Teléfono: 91 394 45 70, Fax: 91 394 46 62
Correo electrónico: Algebra@mat.ucm.es

SEMINARIO DE GEOMETRÍA ALGEBRAICA

Martes, 27 de febrero de 2018, **15:30**, Seminario Alberto Dou (209)

Miguel Ambrona

IMDEA Software/UPM

Impartirá la conferencia

El modelo del Grupo Genérico en Criptografía: demostraciones automáticas

Resumen.

La criptografía es un elemento esencial en el mundo en el que vivimos. Muchas de las tareas que hoy desempeñamos con normalidad serían imposibles sin ella: hacer operaciones bancarias por internet, comunicarnos de forma confidencial, identificarse en servicios web... Es crucial tener garantías de que las primitivas criptográficas que utilizamos son seguras, pero... ¿qué significa que sean seguras? ¿cómo podemos saber si se puede confiar en dichos algoritmos?

El método estándar y más aceptado para analizar constructiones criptográficas consiste en demostrar que si se pudiera atacar la primitiva, existiría un algoritmo que podría resolver un problema considerado "difícil": factorización, logaritmo discreto... Sin embargo, no siempre es posible encontrar una reducción de este tipo a uno de estos problemas. En estos casos, todavía se puede obtener cierta confianza sobre la primitiva, analizándola en modelos más débiles que el Modelo Estándar, e.g., el Modelo del Grupo Genérico o el Modelo del Oráculo Aleatorio.

En esta presentación, describiré en qué consisten estos modelos alternativos y qué garantías de seguridad proporcionan, con especial énfasis en el Modelo del Grupo Genérico. Éste permite analizar primitivas criptográficas y ganar confianza sobre su seguridad, aunque no se conozca una prueba estándar para ellas.

Adicionalmente, mostraré cómo se puede automatizar el análisis de construciones criptográficas en este modelo, ya que es especialmente adecuado para este fin.

Referencias: - U. Maurer. Abstract models of computation in cryptography. In N. Smart, editor, Cryptography and Coding, volume 3796 of Lecture Notes in Computer Science, pages 112. Springer Berlin Heidelberg, 2005

- M. Ambrona, G. Barthe, and B. Schmidt. Automated unbounded analysis of cryptographic constructions in the generic group model. In M. Fischlin and J.-S. Coron, editors, EUROCRYPT 2016, Part II, volume 9666 of LNCS, pages 822851. Springer, Heidelberg, May 2016