Facultad de Informática
Universidad Complutense de Madrid

ANUNCIO DE CONFERENCIA

Funciones hash criptográficas y la competición SHA-3

Profª. María Naya Plasencia.
FHNW Hochschule Für Technik

Sala de Grados • 9 de junio de 2011 • 16:00
entrada libre hasta completar el aforo

resumen:

Las funciones hash criptográficas son una de las tres grandes ramas de la criptografía simétrica. Son funciones que reciben un mensaje cualquiera de una longitud arbitraria y devuelven un valor de longitud fija. Las funciones hash son ampliamente utilizadas en diversas aplicaciones de seguridad informática, como los códigos de autentificación de mensajes (MAC), garantizar la integridad de ejecutables, firmas digitales y otras formas de autentificación. Tienen que ser fáciles de calcular y verificar ciertas propiedades. Las funciones hash actualmente estandarizadas han sufrido diversos análisis y ataques a lo largo de los últimos años, teniendo especial interés los ataques sobre la familia MD4. SHA-1, que pertenece a ésta familia, sufre de ataques teóricos, y SHA-2, debido a su parecido con SHA-1, ha perdido la confianza de la comunidad criptóloga. Debido a esto el NIST, Instituto Nacional de Estándares y Tecnología americano, decidió lanzar una competición pública e internacional en 2008 y encontrar un nuevo estándar de función hash: SHA-3. Actualmente, dos años y dos rondas más tarde, 5 algoritmos (Blake, Gröstl, JH, Keccak, Skein) han sido seleccionados como finalistas de esta competición entre los 64 que fueron presentados en un primer momento. La función ganadora será elegida en 2012 ... y aún queda mucho trabajo por hacer antes de que esta decisión sea tomada.

sobre *María Naya*:

María Naya se graduó en 2005 en Ingeniería de Telecomunicaciones conjuntamente por las Universidades Politécnica de Madrid (España) y por el INT Télécom - Evry (Francia), en 2006 en Máster en Álgebra Aplicada a la Criptografía por la University of Versailles (Francia) y en 2009 obtuvo su Doctorado (Stream Ciphers and Hash Functions: Design and Cryptanalysis) en el INRIA-Rocquencourt bajo la dirección de Anne Canteaut. Desde 2009 es Postdoc en el FHNW (Suiza) financiado por Swiss National Science Foundation. Su área de investigación es la criptografía simétrica, especialmente el Cifrado en Flujo y las Funciones Hash. Cuenta en su haber con un gran número de publicaciones en las mejores revistas y congresos del área.