Criptosistemas basados en curvas hiperelípticas

Luis Hernández Encinas

Dpto. Tratamiento de la Información y Codificación
Instituto de Física Aplicada, C.S.I.C.
C/ Serrano 144, 28006-Madrid
luis@iec.csic.es

La seguridad de la mayoría de los criptosistemas de clave pública se basa en la supuesta intratabilidad computacional de un problema matemático, considerado difícil, como el de la factorización, el de la suma de un subconjunto o el del logaritmo discreto. En este último problema, utilizando el grupo multiplicativo $\mathbb{Z}_p^*$, se fundamentan criptosistemas como el de ElGamal y esquemas de autenticación y de firma digital.

Sin embargo, la longitud de las claves a emplear en estos protocolos (más de 1024 bits) los hacen poco recomendables cuando han de ser implementados en dispositivos con poca capacidad física, como es el caso de los localizadores, teléfonos móviles o tarjetas inteligentes. Por esta razón, desde hace algunos años se han propuesto grupos alternativos al grupo $\mathbb{Z}_p^*$, de modo que tengan propiedades tan deseables como las siguientes:

- Los elementos del grupo deben tener una representación compacta de modo que cada elemento se pueda representar como una única cadena de, aproximadamente, el número de bits del orden del grupo.
- Dada una representación de los elementos, se debería conocer un algoritmo eficiente para llevar a cabo la operación del grupo.
- Con el fin de preservar la seguridad y confidencialidad de los protocolos, debería ser computacionalmente difícil para cualquier atacante determinar la clave privada empleada, es decir, resolver el problema del logaritmo discreto sobre dicho grupo.

Entre estos grupos cabe destacar las variedades jacobianas de curvas hiperelípticas definidas sobre cuerpos finitos. Se presentarán en este trabajo las características básicas de los criptosistemas basados en estas curvas, su seguridad y las líneas de investigación presentes y futuras.