A hyperelliptic cryptosystem based on the P1363 IEEE standard

Ramiro Moreno, Josep M. Miret and Francesc Sebé.

Dept. Matemàtica. Escola Universitària Politècnica. Universitat de Lleida.
Avgda. Jaume II, 69. 25001 Lleida (Spain).
e-mail: {ramiro,miret}@eup.udl.es

Extended Abstract

Nowadays, the security of a public key cryptosystem is based on certain mathematical problems which are computationally intractable. The discrete logarithm problem is one of the most used in order to design such cryptosystems. It consists in, given two elements in a finite group, finding the suitable exponent to raise the first element to obtain the second one, provided that such an integer exists.

The first cryptosystems based on the discrete logarithm problem were constructed over the multiplicative group of a finite field. But in this case it was necessary to work with fields whose order was very high owing to the existence of a subexponential cost algorithm. The fact of dealing with great order fields involved a lack of efficiency in the corresponding algorithms. Recently, in order to avoid this inconvenience, other groups have started to be studied to construct cryptosystems, such as the group of points of an elliptic curve [6, 3] or the group of divisor classes of the jacobian of an hyperelliptic curve [4].

In this paper we study a public key cryptosystem with hyperelliptic curves following the standard P1363 IEEE established for cryptosystems with elliptic curves [2]. More precisely, the cryptosystem is constructed over the group of the jacobian of an hyperelliptic curve of genus 2 defined over a finite field of characteristic 2. According to Koblitz [5], we choose hyperelliptic curves whose jacobian has order divisible by a large prime number of at least 40 decimal digits, since in this case the discrete logarithm problem is presumably intractable. To compute the order of the jacobian, we consider our hyperelliptic curves over $\mathbb{Z}_2$, for which we can find their order over $\mathbb{Z}_2$ and over $\mathbb{F}_4$ in a straightforward way; from this and from Weil's theorem we get the order of the jacobian over $\mathbb{F}_{2^m}$, for each $m \in \mathbb{N}$.

We have implemented the cryptosystem by using the Number Theory library [7] and considering the standard basis representation for the elements of the field $\mathbb{F}_{2^m}$.

The elements of the jacobian can be represented by means of a pair of polynomials that satisfy certain properties. The addition of the elements of the jacobian has been performed using the algorithms described in [4], whose cost for hyperelliptic curves of genus 2 in characteristic 2 has been studied in [1]. Finally, we give timing results for fields $\mathbb{F}_{2^m}$, with m in the interval $[60, 120]$, and we make several comparisons with public key cryptosystems based on elliptic curves.

References

[1] L. Hernández, A. Menezes, and J. Muñoz. Algunas propiedades de las curvas hiperelípticas de género 2 sobre un cuerpo finito de característica 2 y su uso criptográfico. In *V Reunión Española de Criptología y Seguridad de la Información*, pages 155–166, 1998.

[2] IEEE Standards Departament. *IEEE P1363 / D9 (Draft version 9): Standard Specifications for Public Key Cryptography*, February 1999.

[3] N. Koblitz. Elliptic Curve Cryptosystems. *Math. Comp.*, 177:203–209, 1987.

[4] N. Koblitz. Hyperelliptic Cryptosystems. *Journal of Cryptology*, 1:139–150, 1989.

[5] N. Koblitz. *Algebraic Aspects of Cryptography.* Springer-Verlag, 1998. With an appendix on hyperelliptic curves by A. Menezes, Y. Wu and R. Zuccherato.

[6] V. Miller. Use of elliptic curves in cryptography. In *Advances in Cryptology–Crypto'85*, pages 417–426. Springer–Verlag, 1986.

[7] V. Shoup. *Number Theory Library (NTL) v3.0.* http://www.shoup.net.