Okamoto, Tatsuaki; **Sakurai, Kouichi**

Efficient algorithms for the construction of hyperelliptic cryptosystems. (English)

Zbl 0788.14024

Advances in cryptology, Proc. Conf., CRYPTO '91, Santa Barbara/CA (USA) 1991, Lect. Notes Comput. Sci. 576, 267-278 (1992).

Let $g > 0$ be a fixed integer. The authors prove that the problem of computing the structure of the group of rational points $J(\mathbb{F}_q)$ on the Jacobian J of a hyperelliptic curve X over a finite field $\mathbb{F}_q$ of cardinality q is in $NP \cap co - NP$. The certificate is a set of independent generators of the group of prime power order. The independence is checked by means of the Weil pairing. To prove that the points generate the entire group, the authors employ Pila's algorithm [*J. Pila*, Mth. Comput. 55, No. 192, 745-763 (1990; Zbl 0724.11070)] to compute the number of points in $J(\mathbb{F}_q)$. This last part is not really necessary; it suffices to use the fact that $(\sqrt{q}-1)^{2g} \leq \#J(\mathbb{F}_q) \leq (\sqrt{q}+1)^{2g}$.

For the entire collection see [Zbl 0753.00024].

Reviewer: R.Schoof (Povo)

MSC:

14H40 Jacobians, Prym varieties
14Q05 Computational aspects of algebraic curves
94A60 Cryptography
68Q25 Analysis of algorithms and problem complexity
14G15 Finite ground fields in algebraic geometry
14H52 Elliptic curves
68Q15 Complexity classes (hierarchies, relations among complexity classes, etc.)

Keywords:

Jacobian of a hyperelliptic curve; group of rational points; finite field; Weil pairing