Vercauteren, Frederik

Computing zeta functions of hyperelliptic curves over finite fields of characteristic 2. (English)

Zbl 1023.14007

Yung, Moti (ed.), Advances in cryptology - CRYPTO 2002. 22nd annual international cryptology conference, Santa Barbara, CA, USA, August 18-22, 2002. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 2442, 369-384 (2002).

Summary: We present an algorithm for computing the zeta-function of an arbitrary hyperelliptic curve over a finite field $\mathbb{F}_q$ of characteristic 2, thereby extending Kedlaya's algorithm for small odd characteristic. For a genus g hyperelliptic curve over $\mathbb{F}_{2^n}$, the asymptotic running time of the algorithm is $O(g^{5+\varepsilon}n^{3+\varepsilon})$ and the space complexity is $O(g^3n^3)$.

For the entire collection see [Zbl 0997.00039].

MSC:

14G15	Finite ground fields in algebraic geometry
14Q05	Computational aspects of algebraic curves
94A60	Cryptography
11T71	Algebraic coding theory; cryptography (number-theoretic aspects)

Keywords:

hyperelliptic curve; Kedlaya's algorithm; Monsky-Washnitzer cohomology; algorithm for computing the zeta-function; complexity

Full Text: Link