Kim, Hae Young; **Park, Jung Youl**; **Cheon, Jung Hee**; **Park, Je Hong**; **Kim, Jae Heon**; **Hahn, Sang Geun**

Fast elliptic curve point counting using Gaussian normal basis. (English) Zbl 1058.11075

Fieker, Claus (ed.) et al., Algorithmic number theory. 5th international symposium, ANTS-V, Sydney, Australia, July 7–12, 2002. Proceedings. Berlin: Springer (ISBN 3-540-43863-7). Lect. Notes Comput. Sci. 2369, 292-307 (2002).

Summary: In this paper we present an improved algorithm for counting points on elliptic curves over finite fields. It is mainly based on Satoh-Skjernaa-Taguchi algorithm [*T. Satoh, B. Skjernaa* and *Y. Taguchi*, Finite Fields Appl. 9, No. 1, 89–101 (2003; Zbl 1106.14302)], and uses a Gaussian Normal Basis (GNB) of small type $t \leq 4$. In practice, about 42% (36% for prime N) of fields in cryptographic context (i.e., for $p = 2$ and $160 < N < 600$) have such bases. They can be lifted from $\mathbb{F}_{p^N}$ to $\mathbb{Z}_{p^N}$ in a natural way. From the specific properties of GNBs, efficient multiplication and the Frobenius substitution are available. Thus a fast norm computation algorithm is derived, which runs in $O(N^{2\mu} \log N)$ with $O(N^2)$ space, where the time complexity of multiplying two n-bit objects is $O(n^\mu)$. As a result, for all small characteristic p, we reduced the time complexity of the SST-algorithm from $O(N^{2\mu+0.5})$ to $O(N^{2\mu+\frac{1}{\mu+1}})$ and the space complexity still fits in $O(N^2)$. Our approach is expected to be applicable to the AGM since the exhibited improvement is not restricted to only Satoh-Skjernaa-Taguchi (loc. cit.).

For the entire collection see [Zbl 0992.00024].

MSC:

11Y16	Number-theoretic algorithms; complexity
11G20	Curves over finite and local fields
12Y05	Computational aspects of field theory and polynomials (MSC2010)

Keywords:

elliptic curve; Gaussian normal basis; order counting

Full Text: Link