Nikolaev, M. V.

On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with efficient automorphism. (English) [Zbl 1476.11143]


Summary: The two-dimensional discrete logarithm problem in a finite additive group $G$ consists in solving the equation $Q = n_1 P_1 + n_2 P_2$ with respect to $n_1, n_2$ for specified $P_1, P_2, Q \in G, 0 < N_1, N_2 < \sqrt{|G|}$ such that there exists solution with $|n_1| \leq N_1, |n_2| \leq N_2$.

In 2004, P. Gaudry and É. Schost [ANTS-VI, Lect. Notes Comput. Sci. 3076, 208–222 (2004; Zbl 1125.11360)] proposed an algorithm to solve this problem with average complexity $(c + o(1))\sqrt{N}$ of group operations in $G$ where $c \approx 2.43, N = 4N_1N_2, N \to \infty$. In 2009, S. Galbraith and R. S. Ruprai [Cryptography and Coding, 12th IMA International Conference, Lect. Notes Comput. Sci. 5921, 368–382 (2009; Zbl 1233.11128)] improved this algorithm to obtain $c \approx 2.36$.

We show that the constant $c$ may be reduced if the group $G$ has an automorphism computable faster than the group operation.

MSC:

11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
11Y16 Number-theoretic algorithms; complexity
94A60 Cryptography

Keywords:
two-dimensional discrete logarithm problem; Gaudry-Schost algorithm; elliptic curve; efficient automorphism

Full Text: DOI MNR

References:


This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.