Nikolaev, M. V.

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

Mat. Vopr. Kriptografii 6, No. 2, 45-57 (2015).

Summary: The two-dimensional discrete logarithm problem in a finite additive group G consists in solving the equation $Q = n_1P_1 + n_2P_2$ 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

Cited in **2** Documents

Keywords:

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

Full Text: DOI MNR

References:

[1] Galbraith S. D., Holmes M., "A non-uniform birthday problem with applications to discrete logarithms", Discrete Applied Mathematics, 160:10-11 (2012), 1547-1560 · Zbl 1246.60015 · doi:10.1016/j.dam.2012.02.019

[2] Galbraith S. D., Ruprai R. S., "An improvement to the Gaudry-Schost algorithm for multidimensional discrete logarithm problems", Cryptography and Coding, 12th IMA International Conference, Lect. Notes Comput. Sci., 5921, ed. Parker M. G., Springer, 2009, 368-382 · Zbl 1233.11128

[3] Galbraith S. D., Ruprai R. S., "Using equivalence classes to accelerate solving the discrete logarithm problem in a short interval", Public Key Cryptography - PKC 2010, Lect. Notes Comput. Sci., 6056, Springer, 2010, 368-383 · Zbl 1270.11124

[4] Gaudry P., Schost E., "A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm", Proceedings of Algorithm Number Theory Symposium - ANTS VI, Lect. Notes Comput. Sci., 3076, Springer-Verlag, 2004, 208-222 · Zbl 1125.11360

[5] Liu W., Improved algorithms for the 2-dimensional discrete logarithm problem with equivalence classes, MSc Thesis, University of Auckland, 2010

[6] Wiener M. J., Zuccherato R. J., "Faster attacks on elliptic curve cryptosystems", Lect. Notes Comput. Sci., 1556, 1999, 190-200 · Zbl 1025.94511

[7] Nikolaev M. V., Matyukhin D. V., "On the complexity of the two-dimensional problem of computing a discrete logarithm in a finite cyclic group with effective automorphism of order 6", Discrete Math. Appl., 23:3-4 (2013), 313-325 · Zbl 1353.11114 · doi:10.1515/dma-2013-022

[8] Gallant R., Lambert R., Vanstone S., "Faster point multiplication on elliptic curves with efficient endomorphisms", CRYPTO'01, Proc. 21st Ann. Int. Crypt. Conf. Advances in Cryptology, Lect. Notes Comput. Sci., 2139, ed. Kilian J., 2001, 190-200 · Zbl 1002.94022

[9] Duursma I. M., Gaudry P., Morain F., "Speeding up the discrete log computation on curves with automorphisms", ASIACRYPT'99, Lect. Notes Comput. Sci., 1716, eds. K.-Y. Lam, E. Okamoto, C. Xing, Springer, Heidelberg, 1999, 103-121 · Zbl 0968.14034