Barbulescu, Razvan; **Bouvier, Cyril**; **Detrey, Jérémie**; **Gaudry, Pierrick**; **Jeljeli, Hamza**; **Thomé, Emmanuel**; **Videau, Marion**; **Zimmermann, Paul**

Discrete logarithm in $\mathrm{GF}(2^{809})$ **with FFS.** (English) Zbl 1335.94029

Krawczyk, Hugo (ed.), Public-key cryptography – PKC 2014. 17th international conference on practice and theory in public-key cryptography, Buenos Aires, Argentina, March 26–28, 2014. Proceedings. Berlin: Springer (ISBN 978-3-642-54630-3/pbk). Lecture Notes in Computer Science 8383, 221-238 (2014).

Summary: The year 2013 has seen several major complexity advances for the discrete logarithm problem in multiplicative groups of small-characteristic finite fields. These outmatch, asymptotically, the function field sieve (FFS) approach, which was so far the most efficient algorithm known for this task. Yet, on the practical side, it is not clear whether the new algorithms are uniformly better than FFS. This article presents the state of the art with regard to the FFS algorithm, and reports data from a record-sized discrete logarithm computation in a prime-degree extension field.

For the entire collection see [Zbl 1283.94002].

MSC:

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

Keywords:

discrete logarithm; function field sieve; state of the art; cryptanalysis

Full Text: DOI