Finite Fields and Their Applications 51 (2018) 168–182

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the discrete logarithm problem for prime-field elliptic curves

Alessandro Amadori [a], Federico Pintore [b,*,1], Massimiliano Sala [b,2]

[a] *Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, P.O. Box 513, 5600 MB Eindhoven, The Netherlands*
[b] *Department of Mathematics, University of Trento, 38123 Trento, Italy*

ARTICLE INFO

Article history:
Received 11 July 2017
Received in revised form 16 January 2018
Accepted 18 January 2018
Available online xxxx
Communicated by Neal Koblitz

MSC:
11T71
11Y16
11G20
13P10
14G15
14H52

Keywords:
Elliptic curve
Discrete logarithm problem (DLP)
Prime field
Summation polynomials
Groebner basis

ABSTRACT

In recent years several papers have appeared that investigate the classical discrete logarithm problem for elliptic curves by means of the multivariate polynomial approach based on the celebrated summation polynomials, introduced by Semaev in 2004. With a notable exception by Petit et al. in 2016, all numerous papers on the subject have investigated only the composite-field case, leaving apart the laborious prime-field case. In this paper we propose a variation of Semaev's original approach that reduces to only one the relations to be found among points of the factor base, thus decreasing drastically the necessary Groebner basis computations. Our proposal holds for any finite field but it is particularly suitable for the prime-field case, where it outperforms both the original Semaev's method and the specialised algorithm by Petit et al..

* Corresponding author.
E-mail addresses: a.amadori@tue.nl (A. Amadori), federico.pintore@unitn.it, federico.pintore@gmail.com (F. Pintore), maxsalacodes@gmail.com (M. Sala).

[1] This work was supported by CARITRO Foundation [grant number: 2014.0500].

[2] This research was partially funded by the Italian Ministry of Education, Universities and Research, with the project PRIN 2015TW9LSR "Group theory and applications".

https://doi.org/10.1016/j.ffa.2018.01.009
1071-5797/© 2018 Elsevier Inc. All rights reserved.

1. Introduction

Several cryptographic schemes base their security upon the hardness of the discrete logarithm problem for elliptic curves (ECDLP) [13,15]. For an elliptic curve E defined over a finite field $\mathbb{K}$, an instance of the ECDLP is the following:

given $P, Q \in E(\mathbb{K})$, compute an integer w, if it exists, s.t. $Q = wP$.

The best known algorithms for the ECDLP are algorithms that work on arbitrary cyclic groups – like Pollard's Rho algorithm [19], which runs in time $\mathcal{O}(\sqrt{|E(\mathbb{K})|})$ if $|E(\mathbb{K})|$ is prime – exception made for algorithms that are specific for some families of weak curves (see, for example, [14]).

In 2004 Semaev introduced [20] a family of polynomials, named *summation polynomials*, proposing their exploitation for an index calculus algorithm for elliptic curves. The Index Calculus is originally a subexponential algorithm to compute discrete logarithms in the multiplicative groups of finite fields. However, it is customary to use the name *index calculus algorithm* to refer to any algorithm that computes discrete logarithms in a cyclic group G by first collecting linear relations and, afterwards, using linear algebra. Following [6] and restricting to the case $G = E(\mathbb{K})$, with $r = |E(\mathbb{K})|$ a prime integer, the simplest version of index calculus algorithm consists of the following *relation collection* step and *linear algebra* step. In the *relation collection* step:

1. a factor base $\mathcal{F} \subset E(\mathbb{K})$ is defined;
2. for random integers u, v, the point $R = uP + vQ$ is computed;
3. if possible, R is written as a sum of multiples of points of $\mathcal{F}$:

$$R = uP + vQ = \sum_{F \in \mathcal{F}} \ell_F F, \tag{1}$$

   with the integers ℓ_F's ranging in a small coefficient set;
4. u, v and the vector (ℓ_F) are stored as a row of a matrix M;
5. the procedure from item 2 to item 4 is repeated until at least $|\mathcal{F}|$ points R as in (1) are found.

After the collection of a large enough number of relations, the *linear algebra* step solves the discrete logarithm problem, as follows:

1. by using linear algebra on M, a linear dependency of points R is computed, obtaining the relation $\lambda P + \mu Q = \infty$ with $\lambda, \mu \in \mathbb{Z}$;
2. w is recovered from the linear congruence $\lambda + \mu w = 0 \pmod{r}$, which is solvable except in the extremely unlikely case when $\mu = 0$.