Efficient Algorithms to Solve the Elliptic Curve Discrete Logarithm Problem over Finite Fields of Characteristic Two

黄, 筠茹

https://doi.org/10.15017/1500510

出版情報：九州大学, 2014, 博士（機能数理学）, 課程博士
バージョン：

（様式３）

氏　　名　：　**黄　筠茹**

論 文 名　：　Efficient Algorithms to Solve the Elliptic Curve Discrete Logarithm Problem over Finite Fields of Characteristic Two
(標数２の有限体上の楕円曲線離散対数問題の効率的な解法アルゴリズム)

区　　分　：　**甲**

論　文　内　容　の　要　旨

In the last two decades, elliptic curves have become increasingly important. In 2009, the American National Security Agency (NSA) to advocate the use of elliptic curves for public key cryptography, which are based on the hardness of elliptic curve discrete logarithm problem (ECDLP) or other hardness problem on elliptic curves. Elliptic curves used in practice are defined either over a prime field F_p or over a binary field F_{2^n}. Like any other discrete logarithm problem, ECDLP can be solved with generic algorithms such as Baby-step Giant-step algorithm, Pollard's ρ method and their variants. These algorithms can be parallelized very efficiently, but the parallel versions still have an exponential complexity in the size of the parameters. Better algorithms based on the index calculus framework have long been known for discrete logarithm problems over multiplicative groups of finite fields or hyperelliptic curves, but generic algorithms have remained the best algorithms for solving ECDLP until recently.

A key step of an index calculus algorithm for solving ECDLP is to solve the point decomposition problem. In 2004, Semaev introduced the summation polynomials (also known as Semaev's polynomials) to solve this problem. Solving Semaev's polynomials is not a trivial task in general, in particular if K is a prime field. At Eurocrypt 2012, Faugère, Perret, Petit and Renault re-analized Diem's attack in the case F_{2^n} (denoted as FPPR in this work), and showed that the systems arising from the Weil descent on Semaev's polynomials are much easier to solve than generic systems. Later at Asiacrypt 2012, Petit and Quisquater provided heuristic evidence that ECDLP is subexponential for that very important family of curves, and would beat generic algorithms when *n* is larger than about 2000. In 2013, Shantz and Teske provided further experimental results using the so-called ``delta method'' with smaller factor basis to solve the FPPR system.

Even though these recent results suggest that ECDLP is weaker than previously expected for binary curves, the attacks are still far from being practical. This is mainly due to the large memory and time required to solve the polynomial systems arising from the Weil descent in practice. In particular, the experimental results presented in Asiacrypt by Petit and Quisquater for primes *n* were limited to *n* = 17. In order to validate the heuristic assumptions taken in Petit and Quisquater's analysis and to estimate the exact security level of binary elliptic curves in practice, experiments on larger parameters

are definitely required.

In this paper, we introduced several variants to solve ECDLP. In our first approach, we focus on Diem's version of index calculus for ECDLP over a binary field of prime extension degree *n*. In that case, the Weil descent is performed on a vector space that is not a subfield of F_{2^n}, and the resulting polynomial system cannot be re-written in terms of symmetric variables only. We introduce a different method to take advantage of symmetries even in the prime degree extension case. While Shantz and Teske use the same multivariate system as FPPR, in this work we re-write the system with both symmetric and non-symmetric variables. The total number of variables is increased compared to the FPPR system, but we limit this increase as much as possible thanks to an appropriate choice of the vector space V. On the other hand, the use of symmetric variables in our system allows reducing the degrees of the equations significantly. Our experimental results show that our systems can be solved faster than the original systems of FPPR method as long as *n* is large enough.

In our second approach, we focus on the new method to calculate the Semaev's summation polynomial by breaking it down into several pieces of smaller Semaev's summation polynomial. In this case, we limited the degree of Semaev's summation polynomial as well as the degree of regularity of the new system by introducing more intermediate variables. By this new method, we can solve larger Semaev's summation polynomial to at least seven variables, while the first approach can only solved the Semaev's summation polynomial with at most four variables. Our experimental results show that our systems can be solved faster than the first approach. We also introduced more variants to solve ECDLP based on the idea to break the Semaev's summation polynomial down into several smaller pieces.

Keywords: elliptic curve cryptography, discrete logarithm problem, index calculus method, multivariate polynomial system, Gröbner basis