Prime points on elliptic curves and it possible impact on ECDLP

Grzegorz Wojtenko
Wincor Nixdorf EFT Laboratory, Poland
Grzegorz.Wojtenko@wincor-nixdorf.com

Abstract

In this paper we present that some statistical properties of points on elliptic curve can be used to form new equivalence classes. This can have an impact on solving discrete logarithm (*ECDLP*) owing to the reduction of the number of points among which a logarithm is searched to points of particular features. It should lead to an improvement of the Pollard-rho algorithm.

Introduction

Many papers were published about elliptic curve (*EC*) and the discrete logarithm problem (*ECDLP)* related to them. For good survey one can turn to [1]. There was also presented over there an idea of using equivalence classes to solve *ECDLP*. Final conclusion that the equivalence class method in general is a slower one than the standard Pollard method was not optimistic.
Nevertheless, one can find some interesting statistical properties of points on elliptic curve (*EC*-points) and thanks to it propose some new equivalence class-like method.

Let *E* be an elliptic curve defined over a prime field *F*:

$$E:\ y^2 = x^3 + ax + b$$

where $a, b \in F$, whose characteristic is *p*.

Let a *base point* be the generator of the group of points on an elliptic curve.

Let any point on a curve whose *x*-coordinate is a prime number be called as *prime point*.

Let a term *localization of prime point* means finding a number of base points that must be added to a particular prime point to get some next prime point.

In the article, the distribution of prime points in the group of *EC*-points is discussed. Probability of random finding a prime point, relation between that probability and the order of the elliptic curve and some other useful statistics were checked too.
There are also given examples of application of the Pollard-rho algorithm to groups of prime points which could reduce number of steps required to solve *ECDLP*.

Equivalence classes

There is a number of attacks on *ECLDP*, some of them apply only to certain special classes of elliptic curves. The most popular general purpose attack is the Pollard-rho algorithm whose complexity is:

$\sqrt{\frac{\pi n}{2}}$ where *n* is a size of a set.

To speed up the Pollard-rho algorithm one should reduce the size of the set over which the logarithm is searched or act on the set of equivalence classes rather then on the whole set. The idea of equivalence classes is related to endomorphism of the elliptic curve. If there is an easily computed endomorphism for a given elliptic curve then one can accelerate Pollard's method. Some useful endomorphisms have been presented e.g. in [17]. Nevertheless, approaches based on equivalence classes seem in general to be less effective than the standard Pollard-rho method due to complexity of calculation of an endomorphism.

New equivalence class

As the order of a group of *EC*-points should be a prime number, there is no formal subgroup of points in the group. One can however consider a group of points having some special characteristics, e.g. aforementioned prime points. Knowing their distribution among all points in the group one can treat those special points as a kind of equivalence class. One can also contrive other characteristics and form next equivalence classes.
In consequences, instead of the Pollard-rho search over the whole group one can restrict its search to that specific group.

Let's consider some exemplary small curves among which localization of prime points is known and see how effectively the Pollard-rho algorithm will act on these points.

Let these curves be:

E1:
$E(F_{1021}): y^2 = x^3 + 5x + 2$

E2:
$E(F_{4093}): y^2 = x^3 + 9x + 7$

E3:
$E(F_{8191}): y^2 = x^3 + 10x + 17$

E4:
$E(F_{16381}): y^2 = x^3 + 1x + 17$

E5:
$E(F_{65521}): y^2 = x^3 + 7x + 29$

For the curves the standard Pollard-rho algorithm was used twice. In first scenario the whole group of point was searched through and in the second one only the group of prime points. Results of the search are given in Table 1.

Curve	Case I: Pollard-rho over the whole group of points		Case II: Pollard-rho over the group of prime points			Ratio of the Case II results to Case I results
	Rank of the group	Theoretical number of iterations	Rank of the group	Theoretical number of iterations	Practical number of iterations	
E1	1063	40	170	16	19	0.4
E2	4093	80	575	30	27	0.38
E3	8231	114	961	39	40	0.35
E4	16381	160	1850	54	54	0.34
E5	65437	321	6561	101	110	0.31

Table 1

As seen in Table 1, usage of the group of prime points reduces number of Pollard-rho steps for examined curves by about 60% to 70%. A ratio between numbers of steps in those two scenarios varies between about 0.4 to 0.3. For all curves the ratio is:

(*) $\sqrt{\frac{1}{\ln n}}$ where *n* is the order of the group of all *EC*-points.

As seen on Figure 1 the ratio for small curves is about 0.4 and 0.09 for cryptographically strong ones.

The bigger order of a curve the smaller percentage of prime points among all points. In other words, the smaller value of the ratio (*) the better speed-up of the Pollard-rho algorithm.

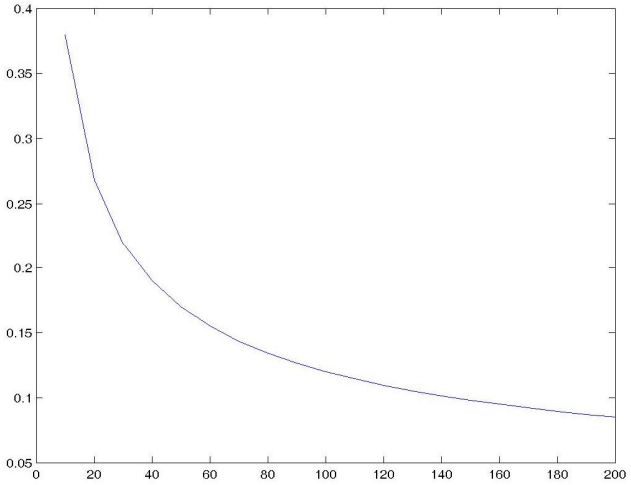

Figure 1: Dependence of the ration (*) (the axis of ordinates) on the order of a curve (on the axis of abscissae are exponents of the power of 2)

Comparison of complexities of the Pollard-rho algorithm applied the whole group of *EC*-points and to the group of prime points for curves with orders between 2^{10} and 2^{25} is presented on Figure 2. The growing difference between the complexities depends directly on the ratio (*)

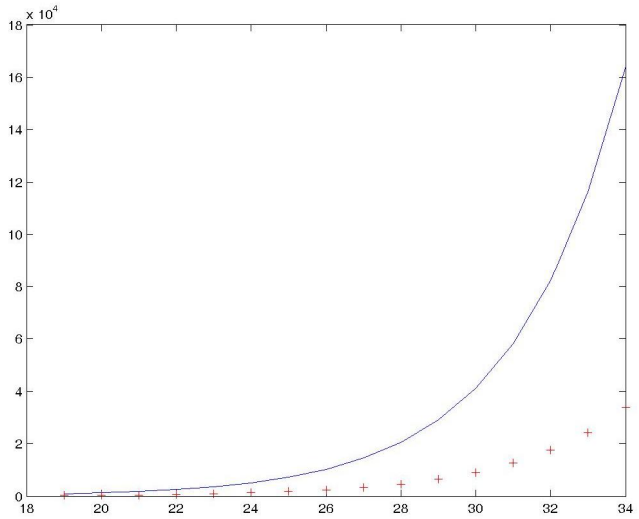

Figure 2: Complexity of Pollard-rho over the whole group (solid line) and over the prime group (crosses)

Those optimistic results must however be confronted with a case when localization of prime points among all points in the group is not given. Instead, one must use only some probabilistic measure to estimate that localization. To solve the problem of the localization of prime points we need some statistical information about distribution of prime points among the whole group of points.

Statistical survey of points on EC

The most desired transformation used in a Pollard-rho-like algorithm would be that one, which would generate only prime points. Then, in Pollard-rho iterations would appear only prime points and the *ECDLP* would be reduced in a straightforward way by the ratio(*). This transformation does not exist however.

Instead, to find localization of prime points one needs to know their distribution. Having known the distribution one should try to come across prime points during Pollard-rho walking and restrict the random search to that particular group. Exemplary results, as presented above, were possible as the distribution of prime points was known in advance thanks to an exhaustive search which is obviously impractical. As any statistical distribution gives only some hints about localization of prime points so finding them must bring an overhead to the method.

Let *d* be a random variable describing a number of base points that must be added to a prime point to reach next, closest prime point.

Probability *P** of random finding a prime point (i.e. numbers which are both prime and an *x*-coordinate of a point):

$P^* = 2 \cdot P(A) \cdot P(B)$ where 2 is due to existing of two points in one group (inverse ones) with the same *x*-coordinate

$$P(A) = \frac{\pi(p)}{p} = \frac{\frac{p}{\ln p}}{p} = \frac{1}{\ln p} \quad \text{where } \pi(p) \text{ is the Euler function}$$

$P(B) = \frac{\frac{p-1}{2}}{p} \cong \frac{1}{2}$ is probability that a given number is a square residue mod p

$$P^* = \frac{1}{\ln p}$$

For the curve $E(F_{16381}) : y^2 = x^3 + 1x + 17$ have been examined properties of d.

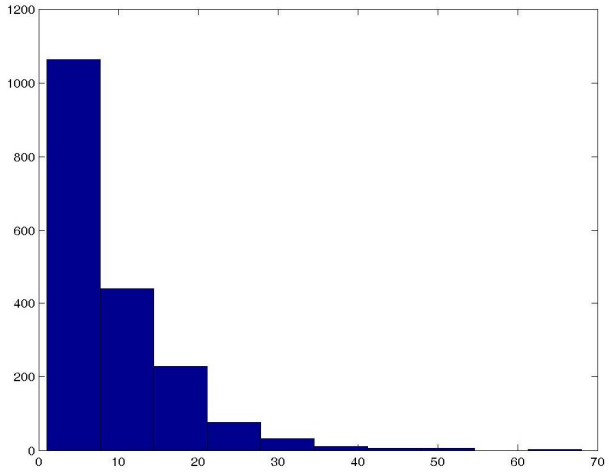

Figure 3: Exemplary histogram of the variable *d*

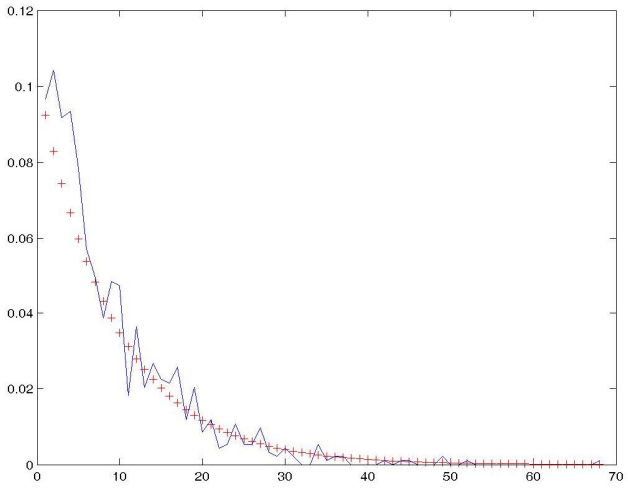

Figure 4: Distribution of the variable *d* (solid line) and geometric distribution (crosses)

As seen on Figure 4, a distribution of the variable *d* may be approximated by geometric distribution.

Idea of the improved Pollard-rho algorithm

As shown above, random walk through specific points can reduce workload for solving *ECDLP*. The idea behind improvement of the Pollard-rho algorithm is to jump randomly over the specific points. It is clear that no simple formula for generating prime points can be presented which would also solve many problems related to prime numbers. Nevertheless, it seems that statistical methods maybe used to solve *ECDLP*.

Some more advanced hints for the proposed modification of the Pollard-rho algorithm should be announced in next paper.

Summary and future works

Due to lack of formal subgroup of *EC*-points one may try to reduce complexity of the Pollard-rho algorithm by usage of equivalence classes. Most of them however suffer from some computational overhead. In the article has been presented a new approach based on some statistical features of *EC*-points. This can be used to locate particular points on a curve and restrict Pollard-like steps to the group of characteristic points. Apart from prime points one should consider also points with other arithmetic features. That extra features combined together should allow further decrease in the number of points in that "artificial" subgroup to which Pollard-rho algorithm will be applied.

References

[1] Galbraith S.D., Smart N.P. "Evaluation report for Cryptrec: security level of cryptography – ECDLP mathematical problem", http://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1029_report.pdf

[2] Semaev I. "A reduction of the space for the parallelized Pollard lambda search on elliptic curves over prime finite fields and on anomalous binary elliptic curves", http://eprint.iacr.org/2003/166

[3] Guajard J., Paar Ch. „Efficient Algorithms for Elliptic Curve Cryptosystems" http://citeseer.ist.psu.edu/guajardo97efficient.html

[4] Solinas J. „An Improved Algorithm for Arithmetic on a Family of Elliptic Curves" http:// cat.inist.fr/?aModele=afficheN&cpsidt=2734203

[5] Agnew G.B., Mellin R.C., Vanstone S. „A Fast Elliptic Curve Cryptosystems"

[6] Escott Adrian „Implementing a Parallel Pollard Rho Attack on ECC" http:// www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/escott.ps

[7] Gallant R., Lambert R., Vanstone S. „Accelerating Pollard's Log Methods for ABC's" http:// www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/lambert.ps

[8] Smart N.P. "Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic", Journal of Cryptology, Vol.12, No.2

[9] Műller V. "Fast Multiplications on Elliptic Curves over Small Fields of Characteristic Two", Journal of Cryptology, Vol.11, No.4

[10] Bailey D.V., Paar C. "Efficient Arithmetic in Finite Field Extension with Application in Elliptic Curve Cryptography", Journal of Cryptology, Vol.14, No.3,

[11] Blake, I.F., Seroussi G., Smart N.P. "Elliptic Curves in Cryptography", Cambridge University Press, 1999

[12] van Oorschot, Wiener M.J. “Parallel Collision Search with Cryptanalytic Applications”, Journal of Cryptology, Vol.12, No.1,

[13] Pollard J.M. “Kangaroos, Monopoly and Discrete Logarithms”, Journal of Cryptology, Vol.13, No.4,

[14] Stinson D.R. “Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem”, 1999
http:// www.cacr.math.uwaterloo.ca/~dstinson/papers/DL.ps

[15] Gallant R., Lambert R., Vanstone S. ”Faster point multiplication on elliptic curves with efficient endomorphism”
http:// citeseer.ist.psu.edu/gallant01faster.html

[16] Teske E. „Better random walks for pollard’s rho method”
Research Report CORR 98-52, Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada. November, 1998.

[17] Ciet M., Lange T., Sica F., Quisquater J. “Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms”, Advances in Cryptology – Eurocrypt 2003,