The order of projective Edwards curve over $\mathbb{F}_{p^n}$ and embedding degree of this curve in finite field

Ruslan Skuratovskii

Institute of Mathematics of NAS of Ukraine, Kiev, Ukraine
e-mail: `ruslan@imath.kiev.ua`

Summary. We consider algebraic affine and projective curves of Edwards [9, 12] over a finite field F_{p^n}. Most cryptosystems of the modern cryptography [2] can be naturally transform into elliptic curves [11]. We research Edwards algebraic curves over a finite field, which at the present time is one of the most promising supports of sets of points that are used for fast group operations. We find not only a specific set of coefficients with corresponding field characteristics, for which these curves are supersingular but also a general formula by which one can determine whether a curve $E_d[\mathbb{F}_p]$ is supersingular over this field or not.
The embedding degree of the supersingular curve of Edwards over $\mathbb{F}_{p^n}$ in a finite field is investigated, the field characteristic, where this degree is minimal, was found.
The criterion of supersungularity of the Edwards curves is found over $\mathbb{F}_{p^n}$. Also the generator of crypto stable sequence on an elliptic curve with a deterministic lower estimate of its period is proposed.
Key words: finite field, elliptic curve, Edwards curve, group of points of an elliptic curve.
Results. We calculate the genus of curve according to Fulton citeF $\rho^*(C) = \rho_\alpha(C) - \sum\limits_{p\in E} \delta_p = \frac{(n-1)(n-2)}{2} - \sum\limits_{p\in E} \delta_p = 3 - 2 = 1$ because $n = 4$, where $\rho_\alpha(C)$ - the arithmetic type of the curve C, parameter $n = degC = 4$.
In order to detect supersingular curves, according to Koblitsa's study [10, 11], one can use the search for such parameters for which the curve and its corresponding twisded curve have the same number of solutions.

Theorem 1. *If* $p \equiv 3 \ (mod\ 4)$ *and* p *is a prime number and* $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod p)$ *then the order of the curve* $x^2+y^2 = 1+dx^2y^2$ *coincides with order of the curve* $x^2+y^2 = 1+d^{-1}x^2y^2$ *over* F_p *and equal to* $N_{E_d} = p+1$ *if* $p \equiv 3(\bmod 8)$*, and it equals to* $N_E = p-3$ *if* $p \equiv 7(\bmod 8)$*. Over the extended field* F_{p^n}*, where* $n \equiv 1(mod 2)$ *order of this curve is* $N_E = p^n + 1$*, if* $p \equiv 3(\bmod 8)$*, and it is* $N_E = p^n - 3$*, if* $p \equiv 7(\bmod 8)$*.*

Example 3. *A number of points for* $d = 2$ *and* $p = 31$ $N_{E_2} = N_{E_2^{-1}} = p - 3 = 28$.

Corollary 1. *If coefficient* d *of* E_d *is such that* $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod p)$*, then* E_d *has* $p-1-2(\frac{d}{p})$ *points over* F_p *and birational equivalent [1] curve* E_M *has* $p+1$ *points over* F_p*.*

Corollary 2. *If the coefficient of the curve satisfies the supersingularity equation* $\sum\limits_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j \equiv 0(\bmod p)$ *studied in Theorem 1, then* E_d *has* $p-1-2(\frac{d}{p})$ *points over* F_p *a boundary-equivalent [8] curve with* $p+1$ *points over* F_p*.*

Theorem 2. *The number of points of the affine Edwards curve is equal to*

$$N_{E_d} = (p + 1 + (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j) \equiv ((-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j + 1)(\mathrm{mod} p).$$

Theorem 3. *The number of points of the projective Edwards curve is equal to* $N_{E_d} = (p+1+2+ (-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j) \equiv ((-1)^{\frac{p+1}{2}} \sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 d^j + 3)(\mathrm{mod} p)$.

Let curve contains a subgroup C_r of order r.

Definition 1. *We call the embedding degree a minimal power k of finite field extention such that can embedded in multiplicative group of* $\mathbb{F}_{p^k}$.

Let us obtain conditions of embedding [7] the group of supersingular curve $E_d[\mathbb{F}_p]$ of order q in multiplicative group of field $\mathbb{F}_{p^k}$ with embedding degree $k = 12$ [5]. For this goal we use Zigmondy theorem. This theorem implies that suitable characteristic of field $\mathbb{F}_p$ is an arbitrary prime q, which do not divide 12 and satisfy the condition $q\,|_{12}(p)$, where $_{12}(x)$ is the cyclotomic polynom. This p will satisfy the necessary conditions namely $(x^n - 1) \not{\vdots}\, p$ for an arbitrary $n = 1, ..., 11$.

Corollary 3. *The embedding degree [7] of the supersingular curve $E_{1,d}$ is equal to 2.*

Theorem 4. *If Edwards curve over finite field F_p, where $p \equiv 7(mod 8)$ is supersingular and $p - 3 = 4q$, where $p,\ q \in P$, then it has minimal cofactor* 4.

Theorem 5. *An arbitrary point of a twisted Edwards curve (1), which is not a point of the 2nd or 4th order, admits divisibility [4] if and only if* $\left(\frac{1-aX^2}{p}\right) \neq -1$.

We propose the generator of pseudo random sequence [13].

Take the elliptic curve of a given large simple order q [3], where $p \neq q$. As a one-sided, take the function: $P_i = f(P_{i-1}) = \phi(P_{i-1})G$, where $\phi(P_{i-1}) = x$, if $P_{i-1} = (x,\ y)$
and p, if $P_{i-1} = O$.

Apply the generation formula $P_i = f(P_{i-1}) = \phi(P_{i-1})G$. Therefore, the complexity of the inverse of this function is equivalent to the problems of a discrete logarithm.

A possible modification is the choice of the coordinate of the point $_i$ which gcd with $|E_d|$ is lesser. Otherwords, let $t := \underset{z\in\{x,y\}}{Argmin}\ (\gcd(x, |E_d|), \gcd(y, |E_d|))$ and as a factor we take:

$$\phi(P_{i-1}) = \begin{cases} t, & P_{i-1} = (x,\ y) \\ p, & P_{i-1} = O. \end{cases}$$

Conclusions. Apply the generation formula $P_i = f(P_{i-1}) = \phi(P_{i-1})G$. Therefore, the complexity of the inverse of this function is equivalent to the problems of a discrete logarithm.

Bibliography

[1] Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. *Twisted Edwards Curves.* IST Programme ECRYPT, and in part by grant ITR-0716498, 2008. 1-17.

[2] Skuratovskii R. V., *Modernized Pohlig-Hellman and Shanks algorithm*, Vol. 1 Visnuk of KNU. Cybernetics. pp. 56., 2015.

[3] Skuratovskii R. V., Movchan P. V.,*Normalizatsiya skruchenoyi kryvoyi Edvardsa ta doslidzhennya yiyi vlastyvostey nad Fp T*, Zbirnyk prats 14 Vseukrayinskoyi. FTI NTUU "KPI" 2016, Tom 2, S. 102-104.

[4] Skuratovskii R. V., Kvashuk D. M., *Vlastyvosti skruchenoyi kryvoyi Edvardsa, mozhlyvist podilu yiyi tochky na dva i zastosuvannya*, Zbirnyk naukovyx prac, Problemy informatyzaciyi ta upravlinnya.. 2017.4(60).S. 61-72.

[5] R. V. Skuratovskii, *Structure and minimal generating sets of Sylow 2-subgroups of alternating groups*, Sao Paulo Journal of Mathematical Sciences. (2018), no. 1, pp. 1-19. Source: https://link.springer.com/article/10.1007/s40863-018-0085-0.

[6] R. V. Skuratovskii, U. V. Skruncovich, *Twisted Edwards curve and its group of points over finite field F_p*, Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries. http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf

[7] Paulo S. L. M. Barreto Michael Naehrig, *Pairing-Friendly Elliptic Curves of Prime Order*, International Workshop on Selected Areas in Cryptography SAC 2005: pp. 319-331.

[8] W. Fulton, *Algebraic curves. An Introduction to Algebraic Geometry*, 2008.

[9] H. Edwards, *A normal form for elliptic curves. American Mathematical Society.*, 2007, Volume 44, Number 3, July, pp. 393-422.

[10] Koblitz N., *Eliptic Curve Cryptosystems*, Mathematics of Computation, **48**(177), 1987, pp.203-209.

[11] A. A. Bolotov, S. B. Gashkov, A. B. Frolov, A. A. Chasovskikh, *Elementarnoye vvedeniye v ellipticheskuyu kriptografiyu*, KomKnika. Tom 2., 2006. p. 328.

[12] Deepthi P.P., Sathidevi P.S., *New stream ciphers based on elliptic curve point multiplication*, Computer Communications (2009). pp 25-33.

[13] Shafi Goldwasser, Mihir Bellare., *Lecture Notes on Cryptography*, Cambridge, Massachusetts, July 2008. p. 289.

Minimal generating set and properties of commutator of Sylow subgroups of alternating and symmetric groups

Ruslan Skuratovskii

Institute of Mathematics of NAS of Ukraine, Kiev, Ukraine
e-mail: ruslan@imath.kiev.ua

Summary. Given a permutational wreath product sequence of cyclic groups [12, 6] of order 2 we research a commutator width of such groups and some properties of its commutator subgroup. Commutator width of Sylow 2-subgroups of alternating group A_{2^k}, permutation group S_{2^k} and $C_p \wr B$ were founded. The result of research was extended on subgroups $(Syl_2 A_{2^k})'$, $p > 2$. The paper presents a construction of commutator subgroup of Sylow 2-subgroups of symmetric and alternating groups. Also minimal generic sets of Sylow 2-subgroups of A_{2^k} were founded. Elements presentation of $(Syl_2 A_{2^k})'$, $(Syl_2 S_{2^k})'$ was investigated. We prove that the commutator width [14] of an arbitrary element of a discrete wreath product of cyclic groups C_{p_i}, $p_i \in \mathbb{N}$ is 1.

Let G be a group. The commutator width of G, $cw(G)$ is defined to be the least integer n, such