UDC 512.54

Criterion of supersingularity of Montgomery and Edwards curves over finite field

Ruslan Skuratovskii, Aled Williams

Igor Sikorsky Kiev Polytechnic Institute, ruslcomp@gmail.com, r.skuratovskii@kpi.ua

Cardiff University, williamsae13@cardiff.uk

As well known supersingular curves due to pairing of Weil and pairing of Tate [4] are implemented in identity-based cryptosystems so we propose new criterion of supersingularity of Montgomery and Edwards curves. We denote by E_d the Edwards curve with coefficient $d \in {F_p}^*$, $ad(a-d) \neq 0$, $d \neq 1$, $p \neq 2$ defined as

$$x^2 + y^2 = 1 + dx^2y^2,$$

over $\mathbb{F}_p$. We recall the basic Montgomery form for an elliptic curve:

$$By^2 = x^3 + Ax^2 + x. \tag{1}$$

The use of isogeny of supersingular elliptic curves as well as Edwards curves which we have studied in [3] with as many subgroups of their points as possible.

Since supersingular elliptic curves are vulnerable to pairing-based attacks then we find a criterion for Edwards curve supersingularity [3].

The method proposed has complexity $\mathcal{O}\left(p \log_2^2 p\right)$. This is an improvement over both Schoof's basic algorithm and the variant which makes use of fast arithmetic (suitable for only the Elkis or Atkin primes numbers) with complexities $\mathcal{O}(\log_2^8 p^n)$ and $\mathcal{O}(\log_2^4 p^n)$ respectively.

Theorem 1. *The Montgomery curve (1) is supersingular over F_p if and only if*

$$\sum_{j=0}^{\frac{p-1}{2}} (C^j_{\frac{p-1}{2}})^2 r^{-2j} \equiv 0 (mod p),$$

where r is one of the roots of the equation $x^2 + Ax + 1 = 0$.

Based on the Weil formulas [1, 4] which were also mentioned in [1], using the laws of the addition of the points of the curve in the general Weierstrass form, for the curve ([3]) one can obtain the 2-isogeny ([1]. the example 12.4)

$$\psi(u, v) = (\tfrac{u^2+cu+b}{u}, \tfrac{u^2-b}{u^2}v) = (X, Y) \tag{2}$$

as a result the equation of the isogenous curve is the following:

$$Y^2 = X^3 - 2cX^2 + (c^2 - 4b)X. \tag{3}$$

$$\begin{aligned}
v^2 &= \left(x - \tfrac{c}{3}\right)^3 + c\left(x - \tfrac{c}{3}\right)^2 + e\left(x - \tfrac{c}{3}\right) = \\
&= x^3 - x^2C + x\tfrac{C^2}{3} - \tfrac{C^3}{27} + x^2C - 2x\tfrac{C^2}{3} + \tfrac{C^3}{9} + ex - \tfrac{eC}{3} = \\
&= x^3 + x\tfrac{C^2}{3} - 2x\tfrac{C^2}{3} + x - \tfrac{C}{3} + \tfrac{C^3}{9} - \tfrac{C^3}{27} = \\
&= x^3 + (\tfrac{C^2}{3} - 2\tfrac{C^2}{3} + e)x + (\tfrac{2C^3}{27} - \tfrac{eC}{3}) = \\
&= x^3 + (e - \tfrac{C^2}{3})x + (\tfrac{2C^3}{27} - \tfrac{eC}{3}) = x^3 + ax + b.
\end{aligned}$$

Theorem 2. *If* $p \equiv 3 (\mathrm{mod}\ 4)$, *where* $p \in \mathbb{P}$ *and*

$$\sum_{j=0}^{\frac{p-1}{2}} \left(C^j_{\frac{p-1}{2}}\right)^2 d^j \equiv 0 (\mathrm{mod}\ p), \tag{4}$$

is true, then the orders of the Edwards curves $x^2 + y^2 = 1 + dx^2y^2$ *and* $x^2 + y^2 = 1 + d^{-1}x^2y^2$ *over* F_p *are equal to*

$$N_{d[p]} = \begin{cases} p+1 & \textit{if } \left(\frac{d}{p}\right) = -1 \\ p-3 & \textit{if } \left(\frac{d}{p}\right) = 1 \end{cases}$$

1. A.J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

2. Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphism Fourteenth Algorithmic Number Theory Symposium. The open book series 4, (2020). https://doi.org/10.2140/obs.2020.4.7

3. Ruslan Skuratovskii, Volodymyr Osadchyy. The Order of Edwards and Montgomery Curves. *WSEAS TRANSACTIONS on MATHEMATICS*. Volume 19, 2020. pp. 1-12. DOI: 10.37394/23206.2020.19.25

4. D. Page, N.P. Smart and F. Vercauteren A comparison of MNT curves and supersingular curves, Applicable Algebra in Engineering, Communication and Computing, volume 17, 2006, pp. 379-392,

Критерій суперсингулярності над скінченним полем кривих Монгомері і Едвардса.

Ми наводимо необхідні і достатні умови суперсингулярності над скінченним полем кривих Монгомері і Едвардса. Будуємо деякі ізогенії між кривою Едвардса кривою Монгомері і еліптичною кривою у формі Веєрштрасса