R. V. SKURATOVSKII[1], Aled WILLIAMS[2]

ROZWIĄZANIE ZAGADNIENIA ODWROTNEGO DO PODWAJANIA PUNKTU ZNAJDUJĄCEGO SIĘ NA SKRĘCONEJ KRZYWEJ EDWARDSA NAD CIAŁEM SKOŃCZONYM

Streszczenie: Rozwiązanie zagadnienia odwrotnego do podwajania punktu otrzymano dla skręconych krzywych Edwardsa. Jest ono istotne z punktu widzenia wyznaczania rzędu punktu w kryptosystemie.
Opisano także możliwość konstruowania skręconych krzywych Edwardsa rzędu $4p,\ p\in \mathbf{P}$.
Krzywe Edwardsa są wykorzystywane do generowania kodów w kryptografii, które cechują się dłuższym czasem użytkowania.

Słowa kluczowe: ciało skończone, krzywa eliptyczna, krzywa Edwardsa, rząd krzywej, rząd punktu, symbol Legendre'a, kwadratowe i niekwadratowe skręcone krzywe

A SOLUTION OF THE INVERSE PROBLEM TO DOUBLING OF TWISTED EDWARDS CURVE POINT OVER FINITE FIELD

Summary: A solution for the inverse doubling problem is obtained for elliptic curves represented in the twisted Edwards form. Estimates of the complexity of the division operation into two are obtained in comparison with the doubling of the point. One of the applications of the divisibility properties of a point into two is considered to determine the order of a point in a cryptosystem.
The possibility of constructing a twisted Edwards curve of order $4p,\ p\in \mathbf{P}$, i.e. having the cofactor four, has been found. The possibility of using these curves to generate a long-term crypto-resistant sequence is shown.
Pairing-friendly curves of prime or near-prime order are essential for certain pairing-based schemes such as for short signatures which feature a longer useful life.

Keywords: finite field, elliptic curve, Edwards curve, curve order, points order, Legendre symbol, square, non-square, twisted curves

[1] Lecturer of the Department of Computational Mathematics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kiev, email: ruslan@imath.kiev.ua
[2] School of Mathematics, Cardiff University

Introduction

We consider the algebraic curves which have form of Edwards and elliptic curves with curve with a little embedding degree coordinates in F_{p^n}. These curves are most effective support for a cyclic group of points which have many applications now. In particular for pairing of Tate it is very convinient to apply this curve also it can be used in asymmetric cryptographical algorithms. Some properties of this curve were investigated. Conditions of minimal cofactor of twisted Edwards curve were found.

Many modern cryptosystems can naturally be viewed as an elliptic curve. We consider algebraic curves in the Edwards form [1] over a finite field F_p, which are one of the most promising carriers for the groups used in asymmetric cryptosystems. The goal of the paper is to obtain new [2, 3] and to refine the old criteria for the divisibility of the curve's point not only by half but also by four over the field F_{p^n}. The importance of the operation of point divisibility by half in cryptanalysis has already been partially described by the authors [4, 6]. Our goal is to find these conditions and explore the possibilities for applying them to the twisted Edwards curve.

The main result

Twisted Edwards curve $E_{a,d}$

$$ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in F_p^*,\ ad(a-d) \neq 0,\ d \neq 1,\ p \neq 2,\ a \neq d. \qquad (1)$$

By the divisibility of the point (*X, Y*) by half we consider finding its prototype, i.e. the point (*x, y*) which is obtained by applying the point's doubling formula [1].

Theorem 1

Let *G = (X, Y) be the point of the twisted Edwards curve. Then the necessary condition for divisibility of the point G by 2 is the condition*

$$\left(\frac{1-aX^2}{p}\right) \neq -1.$$

Proof

For the twisted Edwards curve the doubling law [4,9] is of the form

$$2(x_1, y_1) = \left(\frac{2x_1y_1}{y_1^2 + ax_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2y_1^2}\right) = (X, Y). \qquad (2)$$

Now applying the curve equation, we can derive a modified formula for adding a point with itself, namely

$$2(x_1,y_1)=\left(\frac{2x_1y_1}{1+dx_1^2y_1^2},\frac{y_1^2-ax_1^2}{1-dx_1^2y_1^2}\right)=(X,Y)=G. \tag{3}$$

Let us now consider the equation $\frac{2x_1y_1}{1+dx_1^2y_1^2}=X$ which is equivalent to $dXx_1^2y_1^2-2x_1y_1+X=0$ and $1+dx_1^2y_1^2\neq 0$. Upon applying the substitution $t=x_1y_1$, we obtain the equation $dXt^2-2t+X=0$. The solution to which exists if and only if $\left(\frac{1-dX^2}{p}\right)=1$ (or equivalently if $1-dX^2\equiv 0(\mathrm{mod}\ p)$).

The solutions are in the form $t_{1,2}=\frac{1\pm\sqrt{1-dX^2}}{dX}$ and they exist if $\left(\frac{1-dx_1^2}{p}\right)=1$. We note that $(-x_1,-y_1)=(x_1,y_1)+D$.

Taking into consideration that $y_1^2-dx_1^2y_1^2=1-ax_1^2$ we obtain that $y_1^2(1-dx_1^2)=1-ax_1^2$. Last equation implies that

$$\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right).$$

From the equation (2) for the first coordinate we have the following equation

$$\frac{2x_1y_1}{y_1^2+ax_1^2}=X.$$

Upon substituting $u=\frac{y_1}{x_1}$, we note that the correctness follows from the indivisibility of the second-order points $D_{0,1}=(0,\pm 1)$ in (2) [3]. Since these are points for which the task of division by two is meaningless and the other points of the form $(0,y)$ do not exist, we obtain that $\frac{2u}{u^2+a}=X$ or $2u=X(u^2+a)$. Simply rewriting the latter equation as a quadratic equation with respect to u yields $Xu^2-2u+Xa=0$, where the determinant is precisely $D_2=4(1-aX^2)$. Therefore, it implies that we have the equations $dXt^2-2t+X=0$ and $Xu^2-2u+Xa=0$ whose solutions exist or do not exist simultaneously. This gives us expressions for the coordinates of the point $P_j=(x_j,y_j)$: $x_j=\sqrt{t_ju_j^{-1}},y_j=\sqrt{t_ju_j}$, $j\in\{0,1\}$.

By equating the left-hand sides of the equations $\frac{2x_1y_1}{1+dx_1^2y_1^2}=X$ and $\frac{2x_1y_1}{y_1^2+ax_1^2}=X$, we obtain $ax_1^2+y_1^2=1+dx_1^2y_1^2$, i.e. we have obtained pairs of coordinates (x_1,y_1)

which satisfy the equation of the curve. Note that, together with (x_1, y_1), the points $(-x_1,-y_1)$, $\left(-\frac{y_1}{\sqrt{a_1}},-x_1\right)$, $\left(\frac{y_1}{\sqrt{a_1}},x_1\right)$ satisfy the aforementioned equations.

Let us now analyze which of the obtained points satisfies the equation of doubling the point by the second coordinate

$$\frac{y_1^2 - ax_1{}^2}{1-dx_1{}^2y_1^2} = Y .$$

We transform the equation of curve (1) into $Y^2 = \frac{1-aX^2}{1-dX^2}$ and then substitute the obtained $X = \frac{2x_1y_1}{1+dx_1{}^2y_1{}^2}$, where we set $x = x_1,\ y = y_1$. Then expression for Y in the previous variables is the following:

$$Y^2 = \frac{1-aX^2}{1-dX^2} = \frac{1-a\frac{4t^2}{(y^2+ax^2)^2}}{1-d\frac{4t^2}{(y^2+ax^2)^2}} = \frac{(y^2+ax^2)^2-4at^2}{(y^2+ax^2)^2-4dt^2} = \frac{(y^2+ax^2)^2-4at^2}{(1+dt^2)^2-4dt^2} =$$

$= \frac{(y^2-ax^2)^2}{(1-dt^2)^2} = \frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}$. We have therefore obtained an equation that specifies the second coordinate obtained by doubling the point (x_1, y_1). We will now utilize this equation to choose the correct additional root from $(-x_1,-y_1)$, $\left(-\frac{y_1}{\sqrt{a_1}},-x_1\right)$, $\left(\frac{y_1}{\sqrt{a_1}},x_1\right)$ to be the true root (x_1, y_1). Thus, the second equation satisfies the points (x_1, y_1) and $(-x_1,-y_1)$. It should be noted that $(-x_1,-y_1) = (x_1, y_1) + D$ given that $y_1^2 - dx_1^2y_1^2 = 1-ax_1^2$ whence $y_1^2(1-dx_1^2) = 1-ax_1^2$ Therefore, we obtain

$$\left(\frac{1-ax_1^2}{p}\right) = \left(\frac{1-dx_1^2}{p}\right).$$

From the equality (2), we have the following expression for the second coordinate

$$\frac{y_1^2 - ax_1{}^2}{1-dx_1{}^2y_1^2} = Y .$$

We introduce the variable substitution $t = x_1y_1$. The latter equation now takes the form $y_1^2 - ax_1{}^2 = Y(1-dt^2)$ and we obtain that

$$\frac{t^2}{x_1^2} - ax_1{}^2 = Y(1-dt^2)$$

$$t^2 - ax_1^4 = Y(1-dt^2)x_1^2$$

$$ax_1^4 + Y(1-dt^2)x_1^2 - t^2 = 0 \ .$$

Consequently, we have

$$x_1^2 = \frac{Y(\mathrm{dt}^2-1) \pm \sqrt{Y^2(1-\mathrm{dt})^2 + 4dt^2}}{2a} . \tag{4}$$

After performing the substitution $t_{1,2} = \frac{1 \pm \sqrt{1-dX^2}}{dX}$ we have

$$x_{1,2}^2 = \frac{Y(dt_{1,2}^2 - 1) \pm \sqrt{Y^2(1-dt_{1,2}^2)^2 + 4dt_{1,2}^2}}{2a} . \tag{5}$$

It should be noted that the ± signs before the $\sqrt{1-dX^2}$ in fraction $t_{1,2} = \frac{1 \pm \sqrt{1-dX^2}}{dX}$ that are present in the expression (5) are precisely the same in all three occurrences in the expression (5). Because these roots are conjugate irrationalities then we know that the point $(\pm x, \pm y)$ simultaneously satisfy the curve equation which is sufficient for the execution of the theorem's conditions. In addition, since $y^2 = \frac{t^2}{x^2} = \frac{(1 \pm \sqrt{1-dx^2})^2}{dx^3}$ which is the element dx where x is determined by (4) then we must have a square in $\mathbb{F}_p$. Noting that both roots of equations (4) and (5) are conjugate irrationalities numbers and thus if one of them satisfies the equation over Z or $\mathbb{F}_p$, then the elements obtained by the operations of addition, multiplication and exponentiation to the natural order must also be satisfied. In consequence, all the coordinates found must satisfy both the equation of the curve (1) and the equation of the operation of doubling the point.

Let us denote $Y^2(1-\mathrm{d}\frac{1 \pm \sqrt{1-dX^2}}{dX})^2 + 4d(\frac{1 \pm \sqrt{1-dX^2}}{dX})^2$ by g . In this case, the signs "+" or "–" are substituted into both fractions in a similar way. We will denote the obtained expressions as g_1 and g_2 for the "+" and "-" signs respectively. We will denote by a neutral element in the group of points of the curve $E_{a,d}$ by E.

Theorem 2

For any point A satisfying the dividing by two, there are so many points with property $2B = A$, as exist points D at the curve $E_{a,d}$, for which $2D = E$.

Proof. Let D_i , $i \in \{2,4\}$ denote a family of points satisfying the condition $2D = E$. Then we know that each of them also satisfies the equation $2(B + D_i) = A$. It should be noted that this is precisely the equation (2) where the point $B + D_i = (x_1, y_1)$ additionally satisfies the condition

$2(x_1, y_1) = \left(\frac{2x_1 y_1}{y_1^2 + ax_1^2}, \frac{y_1^2 - ax_1^2}{1 - dx_1^2 y_1^2} \right) = (X, Y)$, or equivalently the equation $2(x_1, y_1) = 2(B + D_i) = 2B + 2D_i = A + E = A.$ Thus, general amount of solutions of equation (2) is equal to I, where I is precisely the number of preimages in the group of points $E_{a,d}$.

Remark

Necessary and sufficient conditions for dividing the point $G = (X, Y)$ *of the curve* $E_{a,d}$ *by two are the conditions*

$$\left(\frac{1 - aX^2}{p} \right) \neq -1 \text{ and } (x_1, y_1) \in E_{a,d}.$$

Proof

Because the resulting split by two point (x_1, y_1) does not necessarily lie on the original curve however it satisfies the equations of doubling the point (2) and (3), we can obtain such a pair (*X*; *Y*) which are not a point of the curve $E_{a,d}$ and we have not required the condition of belonging of the point (*X*; *Y*) to the curve $E_{a,d}$. Since this group of points of curve $E_{a,d}(\mathrm{F}_{p^n})$ is not limited divisible, i.e. not for every $n \in \mathbb{N}$, $n < m$ and $g \in G$, the equation $x^n = h$ has solution $h \in G$, then it is not executed automatically. This is why the condition formulated in the Theorem 3 is only necessary.

Upon adding it to the condition $(x_1, y_1) \in E_{a,d}$ we obtain the following criterion.

Corollary 1

The sufficient condition for the existence of exactly four distinct points which result from doubling is equal to *G*, namely: $(\frac{1 - dX^2}{p}) = 1$ and $(\frac{g}{p}) = 1$.

Corollary 2

If $(\frac{1 - dX^2}{p}) = 1$ but $(\frac{g_1}{p}) = 0$ and $(\frac{g_2}{p}) = 0$, then for a point $A = (X, Y)$, there are either two or four prototypes depending on the number of points D with the property $2D = E$. The latter is precisely determined by the condition $\left(\frac{ad}{p} \right) = 1$ [2,3,7].

Corollary 3

For the point $A = (X, Y)$, there are either two prototypes in the case of dividing it by two if $\left(\frac{ad}{p}\right) = -1$, or four if $\left(\frac{ad}{p}\right) = 1$.

The proof is based on Theorem 2 and the conditions for the existence of singular points of the second order which is written as $\left(\frac{ad}{p}\right) = 1$ [2, 3, 7]. The number of points by dividing a point A by two is therefore determined by the number of points D with the property $2D = E$.

Conclusion

This paper studies the inverse operation of doubling of the point for a twisted Edwards curve over simple and extended fields. The operation of doubling of the point can be applied to construction of generator of random numerical sequences analogously as in [10].

REFERENCES

1. BERNSTEIN D.J., BIRKNER P., JOYE M., LANGE T., PETERS Ch.: Twisted Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT,and in part by the National Science Foundation under grant ITR-0716498, 2008., pp. 1-17.
2. SKURATOVSKII R.V.: Construction of elliptic curves with zero trace of Frobenius endomorphism. Information Security, Volume 20, Issue 1, January-March, (2018), pp. 32-45.
3. SKURATOVSKII R.V.: Super-singularity of elliptic and Edwards curves over Fpn. Research in mathematics and mechanics. T 31, No.1, (2018), pp. 17-26.
4. BESSALOV A.V., TRETYAKOV D.B.: Double point doubling and inverse problem for the Edwards curve over a simple field. Modern protection of information. Number 3 (2013), pp. 16-27.
5. BERNSTEIN, D. J., LANGE T.: Faster addition and doubling on elliptic curves. IST Contract 2002-507932 ECRYPT, - 2007. - P. 1-20.
6. PAULO S. L. M. BARRETO M. N.: Pairing-Friendly Elliptic Curves of Prime Order. International Workshop in Cryptography SAC – 2005. – pp. 319-331.
7. BESSALOV A.V.: Elliptic curves in the shape of Edwards and cryptography: monograph. - Kiev. Polytechnika_2017, P. 272.
8. SKURATOVSKII R. V.: Ideals of one-branched singularities of curves of type *W,* Ukr. Mat. Zh. – 2009. –61, № 9. – P. 1257 – 1266.
9. DROZD Y.A., SKURATOVSKII R.V.: Cubic rings and their ideals (in Ukraniane), Ukr. Mat. Zh. – 2010.–V. 62, №11–P.464-470. (arXiv:1001.0230 [math.AG])

10. KALISKI B. S.: Elliptic Curves and Cryptography: A pseudorandom Bit Generator and Other Tools. PhD thesis, MIT, Cambridge, MA, USA, 1988.