DOI 10.1007/s10559-015-9709-x
Cybernetics and Systems Analysis, Vol. 51, No. 2, March, 2015

CYBERNETICS

EXACT NUMBER OF ELLIPTIC CURVES IN THE CANONICAL FORM, WHICH ARE ISOMORPHIC TO EDWARDS CURVES OVER PRIME FIELD

A. V. Bessalov[a] **and L. V. Kovalchuk**[b]

UDC 681.3.06

Abstract. *The necessary and sufficient conditions for the parameters of the curve in the canonical form with two points of order 4 are found. Two lemmas about the properties of quadratic residues are proved, using the Gauss scheme for quadratic residues and non-residues. Based on this lemmas, the exact formulas are derived for the number of elliptic curves with non-zero parameters a and b and two points of order 4 that are isomorphic to Edwards curves over the prime field. It is proved that for large fields the share of such curves is close to 1/4.*

Keywords: *canonical elliptic curve, Edwards curve, twist curve, curve parameters, isomorphism, quadratic residue, quadratic non-residue.*

Among the forms of representation of elliptic curves in cryptographic problems, Edwards curves [1–5], which have the highest speed performance and are convenient for programming, are most promising. They possess double symmetry in field coordinates of performance $p > 2$, whereupon the number of points N_E of such curve is multiple of 4: $N_E \equiv 0 (\bmod 4)$. Therefore, cyclic Edwards curves always contain one point of order 2 and two points of order 4. There are relatively few curves in the canonical form $y^2 = x^3 + ax + b$ with such property (by estimate, about a quarter of various curves [3]); in this connection, constructing Edwards curves isomorphic to them involves the problem of finding curves in the Weierstrass form with two points of order 4. However, the well-known studies did not consider the problem of finding the exact number of such curves with nonzero parameters *a* and *b*.

We are the first to derive formulas for the number of curves with specified properties (and, respectively, Edwards curves isomorphic to them). We introduced a parameter *c* dependent on traditional parameters (a, b) of a curve in canonical form as a unique, in the field F_p, root of the cubic equation. We obtained the necessary and sufficient conditions for the existence of two points of order 4, as well as a system of linear equations to find the unknown parameters *a* and c^2, whose equations contain quadratic residues and non-residues. To find the exact number of canonical curves isomorphic to Edwards curves, it was required to formulate and prove two lemmas about the number of solutions of the equations that relate the sums of quadratic residues and non-residues. The proofs are based on the Gauss scheme of the distribution of quadratic residues [6]. As a result, we obtained formulas to calculate the exact number of curves with the specified properties over any prime finite field F_p of performance $p > 3$. Moreover, we proposed an algorithm to find curves with good cryptographic properties, isomorphic to Edwards curves.

[a]Institute of Physics and Technology, National Technical University of Ukraine “Kyiv Polytechnic Institute,” *bessalov@ukr.net*. [b]Institute of Special Communication and Information Security, National Technical University of Ukraine “Kyiv Polytechnic Institute,” *lv_kov_crypto@mail.ru*. Translated from Kibernetika i Sistemnyi Analiz, No. 2, March–April, 2015, pp. 3–12. Original article submitted December 30, 2013.

NECESSARY AND SUFFICIENT CONDITIONS FOR THE EXISTENCE OF EXACTLY TWO POINTS OF ORDER 4 FOR AN ELLIPTIC CURVE IN THE CANONICAL FORM

The canonical form of a curve over the field of performance $p > 3$ is described by the well-known equation [7]

$$E_p\colon\ y^2 = x^3 + ax + b,\ \Delta = 4a^3 + 27b^2 \neq 0,\ a, b \in F_p. \tag{1}$$

According to the definition, the operation of doubling of point $P = (x_1, y_1)$, which yields coordinates of the point $2P = (x_3, y_3)$, is specified as follows:

$$\begin{cases} x_3 = \nu^2 - 2x_1, \\ y_3 = -y_1 - \nu(x_3 - x_1), \quad \nu = \dfrac{3x_1^2 + a}{2y_1}. \end{cases} \tag{2}$$

We will need the following standard notation. Denote by Q_p the set of reduced quadratic residues modulo prime number p:

$$Q_p = \left\{ x \in F_p \,\middle|\, \left(\frac{x}{p}\right) = 1 \right\},$$

$\left(\frac{x}{p}\right)$ is Legendre symbol, where

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } x \text{ is a quadratic non-residue modulo } p, \\ 0 & \text{if } x \text{ is divisible by } p. \end{cases}$$

In the paper, we will consider only curves (1) whose order is divisible by 2. It is easy to prove that in such case the curve necessarily has a point of order 2 (in particular, this follows from the Silov theorem). According to (2), $P = (x_1, y_1)$ is a point of order 2 if and only if $y_1 = 0$ (in this case, division by 0 occurs when calculating the point 2*P* in (2)), i.e., the point of order 2 will have coordinates $(c, 0)$ for some $c \in F_p$. Substituting the value $y = 0$ into the equation of curve (1), we obtain that c is the solution of equation $x^3 + ax + b = 0$ in the field F_p (which necessarily exists due to the existence of point of order 2). Then in the above notation Eq. (1) can be rewritten as

$$y^2 = (x - c)(x^2 + cx + a + c^2),\ b = -c^3 - ac,\ c \in F_p. \tag{3}$$

As we mentioned above, curve in the canonical form is isomorphic to the Edwards curve if and only if it contains exactly two points of order 4. The theorem below provides the necessary and sufficient conditions (in terms of the parameters of curve (1)) for the existence of exactly two such points on the curve E_p.

THEOREM 1. The necessary and sufficient condition for the existence of exactly two points of order 4 on the curve E_p is simultaneous performance of the following equalities:

$$\text{(a)} \left(\frac{-(3c^2 + 4a)}{p}\right) = -1;\ \text{(b)} \left(\frac{\delta}{p}\right) = 1,\ \delta = 3c^2 + a. \tag{4}$$

Proof. Let us prove the necessity of these conditions. Assume that the curve has two points of order 4 and let us show that conditions (4) are satisfied in this case. Let exactly two points of order 4 exist on curve (1). Then it cannot contain more than one point of order 2 (since according to the definition of the order of a point of a curve, the sum of points of orders 4 and 2 will be a point of order 4). Hence, the parabola in the right-hand side of (3) has no roots in the field F_p, i.e., the discriminant of the respective quadratic equation is a quadratic non-residue. This discriminant is equal to

$$c^2 - 4(a + c^2) = -(3c^2 + 4a)$$

and since it is a quadratic non-residue, we get

$$\left(\frac{-(3c^2 + 4a)}{p}\right) = -1.$$

The necessity of the first condition in (4) has been proved. Note that the condition $(3c^2 + 4a) \neq 0$, which follows from item (a) in formula (4), excludes multiple roots of quadratic equation and thus singular curves with the discriminant $\Delta = 0$ [7].