14. Задірака В. К., Олексюк О. С. Комп'ютерна арифметика багаторозрядних чисел. Київ, 2003. 264 с.
15. Сергиенко И. В., Задирака В. К., Бабич М. Д., Березовский А. И., Бесараб П. Н., Людвиченко В. А. Компьютерные технологии решения задач прикладной и вычислительной математики с заданными значениями характеристик качества. *Кибернетика и системный анализ*. 2006. № 5. С. 33–41.

FROM ERROR THEORY TO MODERN COMPUTER TECHNOLOGIES

The article summarizes the development of computational mathematics during 50 years' period (1969–2019) in the field of accuracy and efficiency of computational algorithms.

In particular, it is emphasized on the global error of the computational algorithm (c. a.), estimates of its quality, the formulation of computations optimization problems, computational algorithms that are optimal in accuracy and processing speed, reserves of calculations optimization, testing the quality of applied software, computer technologies solving the problems of applied and computational mathematics with the given values of quality characteristics in accuracy and processing speed.

Key words: *theory of computing, error theory, apriori information, optimal algorithms, computer technologies.*

Одержано 31.01.2019

УДК 512.7+512.9,688.321
DOI: 10.32626/2308-5878.2019-19.148-155

Р. В. Скуратовский, преподаватель

Межрегиональная академия управления персоналом, г. Киев

РЕШЕНИЕ ОБРАТНОЙ ЗАДАЧИ К УДВОЕНИЮ ТОЧКИ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НАД КОНЕЧНЫМ ПОЛЕМ

Получено решение задачи обратной к удвоению точки для кривой представленной в скрученной форме Эдвардса. Получены оценки сложности операции деления на два в сравнении с удвоением точки. Найдено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме основаной на проблеме дискретного логарифма.

Найдены необходимые и достаточные условия делимости точки $G=(X,Y)$ кривой $E_{a,d}$ на 2. Исследовано возможность применения данных кривых для генерации криптостойкой последовательности большого периода. Важность операции делимости точки на 2 при криптоанализе уже частично замечена криптографами.

© Р. В. Скуратовський, 2019

Исследованы все возможные количества результатов от деления точки на два и зависимости этих количеств от делимой точки. Исследованы необходимые и достаточные условия существования 4 разных прообразов точки $G=(X,Y)$ при делении ее на два. Спаривание на дружественных эллиптических кривых простого порядка или почти простого порядка есть очень существенным во многих криптографических протоколах вида короткой цифровой подписи длительного использования.

Ключевые слова: *конечное поле, эллиптическая кривая, кривая Эдвардса, порядок кривой, порядок точки эллиптической кривой, символ Лежандра, квадратичный вычет, квадратичный невычет.*

Введение. Мы рассматриваем алгебраические кривые в форме Эдвардса [1] над простым полем F_p, которые сейчас являются одними из наиболее перспективных носителей групп, используемых в асимметричных криптосистемах.

Цель роботы — получение новых [2, 3] и уточнение старых критериев делимости точки кривой не только напополам, но и на 4 над полем F_{p^n}. Важность операции делимости точки на 2 при криптоанализе уже частично описана в работе А. В. Бессалова [4]. Наша цель найти эти условия и исследовать возможности их применения для скрученной кривой Эдвардса. Пусть E — единичный элемент в группе точек кривой $E_{a,d}$.

Основной результат. Скрученная кривая Эдвардса $E_{a,d}$ имеет вид

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

Под делимостью точки (X; Y) пополам понимается нахождение ее прообраза, то есть точки (x; y), которая при применении формулы удвоения точки [1] дает в результате точку (X; Y).

Теорема 1. Пусть G = (X; Y) — точка скрученной кривой Эдвардса. Тогда необходимым условием делимости точки G на 2 является условие

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

Доказательство. Для скрученной кривой Эдвардса закон удвоения [4, 9] имеет форму

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

отсюда, воспользовавшись уравнением кривой, мы выводим модифицированную формулу сложения точки с собой:

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

Рассмотрим уравнение $\frac{2x_1 y_1}{1 + dx_1^{\,2} y_1^{\,2}} = X$ равносильное $dXx^2 y^2 - 2xy + X = 0$, при $1 + dx_1^2 y_1^2 \neq 0$, и применим замену $t = x_1 y_1$, после чего получаем уравнение $dXt^2 - 2t + X = 0$, решение, которого существует тогда и только тогда, когда $\left(\frac{1 - dX^2}{p} \right) = 1$ (или если $1 - dX^2 \equiv 0 (\mathrm{mod}\ p)$). Решения имеют вид $t_{1,2} = \frac{1 \pm \sqrt{1 - dX^2}}{dX}$, они существуют если $\left(\frac{1 - dx_1^2}{p} \right) = 1$. Согласно с леммой 1 имеем $\left(\frac{1 - dx_1^2}{p} \right) = \left(\frac{1 - ax_1^2}{p} \right)$. Из уравнения (2) имеем для первой координаты одно уравнение

$$\frac{2x_1 y_1}{y_1^2 + ax_1^{\,2}} = X \ .$$

Сделав замену $u = \frac{y}{x}$, корректность которой следует из не делимости точек $D_{0,1} = (0, \pm 1)$ второго порядка на 2 а также 2 особых точек [3] ввиду того, что это точки для которых задача деления на 2 не имеет смысла а других точек вида $(0, y)$ не существует, получаем $\frac{2u}{u^2 + a} = X$ или $2u = X(u^2 + a)$. Переписав последнее уравнение как квадратное относительно u получаем $Xu^2 - 2u + Xa = 0$, где определитель $D_2 = 4(1 - aX^2)$. Поэтому, согласно лемме 1, имеем уравнения $dXt^2 - 2t + X = 0$, и $Xu^2 - 2u + Xa = 0$ решения которых существуют или не существуют одновременно. Это дает выражения для координат точки $P_j = (x_j, y_j)$: $x_j = \sqrt{t_j u_j^{-1}}, y_j = \sqrt{t_j u_j}$ $j \in \{0,1\}$.

Приравнивая левые части равенств $\frac{2x_1y_1}{1+dx_1^2y_1^2}=X$ и $\frac{2x_1y_1}{y_1^2+ax_1^2}=X$, получаем $ax_1^2+y_1^2=1+dx_1^2y_1^2$, то есть полученные пары координат (x_1,y_1) удовлетворяют уравнению кривой. Заметим, что вместе с (x_1,y_1) выше указанные уравнения удовлетворяют точки $(-x_1,-y_1),\left(-\frac{y_1}{\sqrt{a_1}},-x_1\right),\left(\frac{y_1}{\sqrt{a_1}},x_1\right)$.

Проанализируем, какие из полученных точек удовлетворяют уравнение удвоения точки по 2-ой координате

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

Преобразуем уравнение кривой (1) как $Y^2=\frac{1-aX^2}{1-dX^2}$, подставим полученные $X=\frac{2x_1y_1}{1+dx_1^2y_1^2}$ и обозначим $x=x_1,\ y=y_1$, тогда

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

$$=\frac{(y^2-ax^2)^2}{(1-dt^2)^2}=\frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}\ .$$

Поэтому получили уравнение, которое задает вторую координату полученную в результате удвоения точки (x_1,y_1). Это уравнение мы используем для выбора правильного из дополнительных корней $(-x_1,-y_1),\left(-\frac{y_1}{\sqrt{a_1}},-x_1\right),\left(\frac{y_1}{\sqrt{a_1}},x_1\right)$ к истинному корню (x_1,y_1). Таким образом, второе уравнение удовлетворяют точки (x_1,y_1) и $(-x_1,-y_1)$. Заметим, что $(-x_1,-y_1)=(x_1,y_1)+D$. Учитывая, что $y_1^2-dx_1^2y_1^2=1-ax_1^2$ откуда $y_1^2(1-dx_1^2)=1-ax_1^2$ получаем

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

Из равенства (2) для второй координаты имеем

$$\frac{y_1^2 - a{x_1}^2}{1 - d{x_1}^2 y_1^2} = Y .$$

Поскольку мы ввели замену переменных $t = x_1 y_1$, то последнее уравнение примет вид $y_1^2 - a{x_1}^2 = Y(1 - dt^2)$. Откуда, получаем

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

$$t^2 - ax^4 = Y(1 - dt^2)x^2,$$

$$ax^4 + Y(1 - dt^2)x^2 - t^2 = 0 .$$

Откуда

$$x^2 = \frac{Y(dt^2 - 1) \pm \sqrt{Y^2(1 - dt)^2 + 4dt^2}}{2d} . \qquad (4)$$

После подстановки $t_{1,2} = \frac{1 \pm \sqrt{1 - dX^2}}{dX}$ имеем

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

Заметим, что знаки $\pm$ перед выражениями $\sqrt{1 - dX^2}$ одинаковы. Поскольку эти корни являются сопряженными иррациональностями, то точка $(\pm x, \pm y)$ удовлетворяют одновременно уравнению кривой, чего достаточно для выполнения условий теоремы. Кроме того, $y^2 = \frac{t^2}{x^2} = \frac{(1 + \sqrt{1 - dx^2})^2}{dx^3}$, то есть элемент dx, где x определяется условием (4), должен быть квадратическим вычетом в $\mathbb{F}_p$. Заметим, что оба корни уравнений (4) и (5) являются сопряженными иррациональностями, поэтому если один из них удовлетворяет уравнению над Z или над $\mathbb{F}_p$, то элементы полученные в результате операций сложения, умножения и возведения его в натуральную степень тоже все ему удовлетворяют. Поэтому все найденные координаты удовлетворяют уравнению кривой (1) и уравнению операции удвоения. Операция деление точки требует 4 умножения и 2 извлечения корня в поле и 1 инверсии.

Обозначим $Y^2(1 - \mathrm{d}\frac{1 \pm \sqrt{1 - dX^2}}{dX})^2 + 4d(\frac{1 \pm \sqrt{1 - dX^2}}{dX})^2$ как g. При этом знаки «+» или «–» подставляются в обеих дробях одинако-

вым образом. А полученные выражения обозначаем как g_1 для «+» и как g_2 для знака «–».

Теорема 2. Для любой точки *A*, допускающей деление надвое, существует столько же точек со свойством $2B = A$, сколько существует на кривой точек D, для которых $2D = E$.

Доказательство. Пусть D_i, $i \in 2,4$ семейство точек удовлетворяющих условию $2D = E$. Тогда каждая из них удовлетворяет и уравнению $2(B + D_i) = A$, которое по сути есть уравнение (2), где точка $B + D_i = (x_1, y_1)$ и удовлетворяет условию $2(x_1, y_1) = \left(\frac{2x_1 y_1}{y_1^2 + a x_1^2}, \frac{y_1^2 - a x_1^2}{1 - d x_1^2 y_1^2} \right) = (X, Y)$. Действительно $2(x_1, y_1) = 2(B + D_i) = 2B + 2D_i = A + E = A.$ Поэтому совокупное количество решений уравнения (2) равно количеству решений $2D = E$.

Замечание. Необходимыми и достаточными условиями делимости точки $G = (X, Y)$ кривой $E_{a,d}$ на 2 является условия

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

Доказательство. Поскольку полученное в результате деление на 2 точку (x_1, y_1) не обязательно лежит на исходной кривой. Хотя она и удовлетворяет уравнениям удвоения точки (2) и (3), покуда мы можем получить такую пару (*X*; *Y*), которая не на кривой $E_{a,d}$ в силу того, что мы не потребовали выполнения $(X, Y) \in E_{a,d}$. Ввиду того, что группа точек кривой $E_{a,d}(F_{p^n})$ не является ограничено делимой [8] т. е. не для любого $n \in N$, $n < m$ и $g \in G$ уравнение $x^n = h$ имеет решение $h \in G$, то это не выполняется автоматически. Именно поэтому сформулированное в теореме 3 условие является лишь необходимым. Дополнив его условием $(x_1, y_1) \in E_{a,d}$ мы получим следующий критерий. Деление точки требует 4M, 2S и I в F_{p^n}.

Следствие 1. Необходимым и достаточным условием существования 4 разных точек, для которых результат удвоения равен *G,* является: $(\frac{1 - dX^2}{p}) = 1$ и $(\frac{g}{p}) = 1$.

Следствие 2. Если $(\frac{1 - dX^2}{p}) = 1$ но $(\frac{g_1}{p}) = 0$ и $(\frac{g_2}{p}) = 0$, то для точки *A* = (*X*, *Y*) существует либо 2, либо 4 прообраза в зависимости

от количества точек D, со свойством $2D = E$. Последнее определяется условием $\left(\frac{ad}{p}\right) = 1$ [2, 3, 7].

Следствие 3. Если $\left(\frac{1 - aX^2}{p}\right) \neq -1$ и $(x, y) \in E_{a,d}$, то существует 2 прообраза при $\left(\frac{ad}{p}\right) = -1$, либо 4 при $\left(\frac{ad}{p}\right) = 1$.

Доказательство основывается на теореме 2 и условии существования особых точек 2-го порядка записанного как $\left(\frac{ad}{p}\right) = 1$ [2, 3, 7].

Вывод. В работе исследована обратная операция к удвоению точки для скрученной кривой Эдвардса над конечным полем.

Список использованных источников:

1. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane. Twisted Edwards Curves. IST *Programme under Contract IST-2002-507932 ECRYPT*. 2008. P. 1–17.
2. Скуратовський Р. В. Побудова еліптичних кривих з нульовим слідом ендоморфізма Фробеніуса. *Захист інформації*. 2018. Т. 20, № 1, січень-березень 2018. С. 32–45.
3. Скуратовський Р. В. Суперсингулярність еліптичних кривих і кривих Едвардса над F_p^n. Research in mathematics and mechanics. 2018. Т. 31, № 1. С. 17–26.
4. Бессалов А. В., Третьяков Д. Б. Удвоение точки и обратная задача для кривой Эдвардса над простым полем. *Сучасний захист інформаці*ї. 2013. № 3. С. 16–27.
5. Bernstein D. J., Lange Tanja. Faster addition and doubling on elliptic curves. *IST Contract 2002-507932 ECRYPT*. 2007. P. 1–20.
6. Skuratovskii R. V. Employment of Minimal Generating Sets and Structure of Sylow 2-Subgroups of Alternating Groups in Ciphers. *Advances in Computer and Computational Sciences*. P. 351–364.
7. Бессалов А. В. Эллиптические кривые в форме Эдвардса и криптография : монография. Киев : Polytechnika, 2017. 272 с.

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

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 curve point into two is considered to determine the order of a point in a cryptosystem based on discrete logarithm problem.

The necessary and sufficient conditions for the divisibility of a point $G=(X,Y)$ of a curve $E_{a,d}$ by 2 are found. The possibility of using these curves to generate a crypto-resistant sequence of a large period is investigated.

All possible numbers of the result of the division of a point into two and the dependence of these quantities on the dividend point are studied. The necessary and sufficient conditions for the existence of 4 different preimages of a point $G=(X,Y)$ when dividing it into two are investigated. Pairing-friendly curves of prime or near-prime order are absolutely essential in certain pairing-based schemes like short signatures with longer useful life.

Key words: *elliptic curve, twisted Edwards curve, curve order, points order, Legendre symbol, square, non-square.*

Получено 21.01.2019

УДК 519.65
DOI: 10.32626/2308-5878.2019-19.155-160

В. М. Старков, д-р фіз.-мат. наук,
П. М. Томчук, д-р фіз.-мат. наук
Інститут фізики НАН України, м. Київ

ПРО ВПЛИВ ПОХИБОК ВИМІРЮВАНЬ НА ІНТЕРПРЕТАЦІЮ РЕЗУЛЬТАТІВ ЛАЗЕРНИХ ЕКСПЕРИМЕНТІВ

На основі врахування і математичного аналізу незначних апаратних похибок вимірювань розглянуті приклади їх впливу на фізичну інтерпретацію лазерних експериментальних досліджень. Проведений нами аналіз показує, що ігнорування факту наявності похибок може призвести до помилкових висновків щодо фізичної суті розглянутих оптичних явищ.

Ключові слова: *похибки вимірювань, експеримент, інтерпретація, апроксимація.*

Вступ. На принципове значення достовірності інтерпретації результатів фізичних досліджень звертали увагу видатні вчені [1, 2]. Так, в роботі [2, с. 3] сказано: «Будь-яке наукове дослідження в галузі фізики (і не тільки в галузі фізики) безсумнівно, пов'язане з інтерпретацією отриманих результатів. Таку інтерпретацію часто називають «з'ясуванням фізичного сенсу» або досяганням «розуміння» тих явищ, які досліджують. Зазвичай, інтерпретація фізичного явища відображає рівень розвитку науки в даний момент часу, і тому вона не є абсолютною, а може змінюватися з плином часу». До останнього зауваження можна лише додати, що інтерпретація відображає, крім усього іншого, рівень інтелекту, освіти, наукового досвіду і т.д. дослідника, який її реалізує. Інтерпретація результатів наукового фізич-

© В. М. Старков, П. М. Томчук, 2019