Модели онлайн–сообществ как основа взаимодействия учасников колаборативного документирования/ Гетманюк П. О., Форкун Ю. В. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.85–90. – Bibliogr.:16. – ISSN 2079-5459

Models of online–communities as a communicational basis in collaborative documentation/ Getmanyk P., Forkun Y. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.85–90. – Bibliogr.:16. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Гетманюк Павло Олександрович – Аспірант, Кафедра інженерії програмного забезпечення, Хмельницький національний університет, вул. Інститутська 11, Хмельницький, Україна, 29000, E–mail: gornnaemnik@gmail.com.

Форкун Юрій Вікторович – Кандидат технічних наук, доцент, Кафедра інженерії програмного забезпечення, Хмельницький національний університет, вул. Інститутська 11, Хмельницький, Україна, 29000, E–mail: forkun@ridne.net.

Гетманюк Павел Александрович – Аспирант, Кафедра инженерии програмного обеспечения, Хмельницкий национальный університет, вул. Институтская 11, Хмельницкий, Украина, 29000,

Форкун Юрий Викторович – кандидат технических наук, доцент, Кафедра инженерии програмного обеспечения, Хмельницкий национальный університет, вул. Институтская 11, Хмельницкий, Украина, 29000,

Getmanyuk Pavlo – postgraduated student, Department Software Engineering, Khmelnitskiy national university, str. Institutska 11, Khmelnitskiy, Ukraine, 29000, e–mail: gornnaemnik@gmail.com.

Forkun Iurii – PhD., associate professor, Department Software Engineering, Khmelnitskiy national university, str. Institutska 11, Khmelnitskiy, Ukraine, 29000, e–mail: forkun@ridne.net.

УДК 681.3

Р. В. СКУРАТОВСКИЙ, Е. О. ОСАДЧИЙ, Д. М. КВАШУК

ДЕЛЕНИЕ ТОЧКИ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НА ДВА И ЕГО ПРИМЕНЕНИЕ В КРИПТОГРАФИИ

Большинство криптосистем современной криптографии естественным образом можно реализовать на эллиптических кривых. Мы рассматриваем алгебраические кривые в форме Эдвардса над простым полем, F_p, которые сейчас являются одними из наиболее перспективных носителей групп, используемых в асимметричных криптосистемах. Показано, что проективная кривая Эдвардса $E_{a,d}$ не является эллиптической. Исследовано некоторые интересные свойства группы точек этих кривых. Найдено род скрученной кривой Эдвардса и ее особые точки. Показано возможность построения генератора случайных крипто стойких последовательностей на этой кривой. Предложена нормализация скрученной кривой Эдвардса. Исследованы условия делимости на два элемента из группы точек скрученной кривой Эдвардса над полем F_{p^n} . Целью роботы есть поиск критерия делимости точки кривой напополам над полем F_{p^n} и анализ свойств скрученной кривой Эдвардса необходимых для построения генератора псевдослучайных крипто стойких последовательностей.

Ключевые слова: конечное поле, алгебраическая кривая, группа точек эллиптической кривой, делимость точки кривой пополам.

Більшість криптосистем сучасної криптографії природним чином можна реалізувати на еліптичні криві. Ми розглядаємо алгебраїчні криві Едвардса над скінченним полем F_{p^n} , які на даний час є одним з найбільш перспективних носіїв множин точок, що використовують для швидких групових операцій, які наявні в асиметричних криптосистемах, зокрема для побудови випадкових криптостійких послідовностей. Показано, що проективна крива $E_{a,d}$ не є еліптичною. Досліджено умови існування подільності навпіл елемента з групи точок скрученої кривої Едвардса $E_{a,d}$, що є важливим в алгоритмах. Знайдено рід скрученої кривої Едвардса. Метою роботи є пошук критерію подільності точки кривої навпіл над полем F_{p^n} і аналіз властивостей скрученої кривої Едвардса необхідних для побудови генератора псевдовипадкових криптостійких послідовностей і побудова односторонньої функції для нього.

Ключові слова: скінчене поле, алгебраїчна крива, група точок еліптичної кривої, подільність точки кривої навпіл.

Most cryptosystems of modern cryptography can be naturally transformed into elliptic curves. We review Edwards algebraic curves over a finite field, which at the present time is one of the most promising carriers of sets of points that are used for fast group operations. These are found in asymmetric cryptosystems. In particular, for constructing random crypto-stable sequences. It is shown that the projective curve is not elliptic.

The conditions of the existence of divisibility in half an element from the group of points of the twisted curve of Edwards $E_{a,d}$, which is important in algorithms, are investigated. The type of twisted curve Edwards is found. The purpose of the work is to find the criterion of the divisibility of the point of the curve in half over the field and to analyze the properties of the twisted curve of Edwards necessary for constructing a generator of pseudo-random crypto-stable sequences and constructing a one-way function F_{p^n} for it.

Keywords: finite field, elliptic curve, Edwards curve, order of a curve, finite field, algebraic curve, group of points of an elliptic curve, order of a point, torsion curves.

Введение. Электронно цифровая подпись из средств защиты информации наиболее широко обеспечивает защиту от всех возможных атак. Причиной этого является наличие в ней хешфункции и закрытого ключа шифрования. Наиболее прогрессивной схемой является схема цифровой подписи эллиптической кривой (ECDSS - Elliptic Curve Digital Signature). Благодаря вышеупомянутым возможностям решается проблема управления и распределения ключей шифрования. Мы исследуем еще одно семейство кривых пригодных для создания ECDSS.

Впервые кривые Эдвардса E_d были представлены Эдвардсом в работе Бернстейна и Ланге [1]. В эллиптической криптографии очень важно знать, те кривые которые являются суперсингулярными (имеющие нулевой j-инваривант), поскольку они являются крипографично слабыми и период построенного на их основе генератора псевдослучайных чисел является меньшим.

Известно, что супер сингулярные кривые, в отличие от несуперсингулярных, над алгебраически замкнутым полем, не имеют коммутативное кольцо эндоморфизмов. Кривые в форме Эдвардса над простым полем сегодня являются одним из наиболее перспективных носителей множеств точек, использующих для быстрых групповых операций, что используются в асимметричных криптосистемах. Их важнейшие преимущества: рекордная производительность, универсальность закона сложения, симметричность точек и представления нейтрального элемента группы точек в аффинных координатах. Эти свойства были замечены и обоснованные в работах известных специалистов по криптографии [1–7].

Данные кривые удовлетворяют самым сильным требованиям по устойчивости к MOV-атаки, о чем неоднократно отмечалось в трудах отечественных и зарубежных ученых [2]: невозможность применения этого метода обеспечивается через отсутствие возможности вложить группу точек кривой в мультипликативную группу поля достаточно малого порядка. Для этого достаточно, чтобы минимальное натуральное t, $p^t \equiv 1 mod \mid N_E \mid$, было достаточно большим. Для скрученных кривых Эдвардса $t = \mid N_E \mid -1$, что является максимально возможным. Большим преимуществом является возможность построения скрученной кривой Эдвардса порядка $4p,\ p \in \mathbf{P}$, поэтому не может быть использована атака подмены точки, принадлежащей рекомендованной кривой на точку из скрученной кривой, то есть так называемой кривой кручения. Также не дает противнику использовать китайскую теорему об остатках для определения секретного ключа [2, 8–13], так как имеем большой множитель p в $\mid N_E \mid$. С точки зрения алгебраической геометрии, кривая не является эллиптической, потому что она сингулярная.

Кривые Эдвардса также как и скрученные кривые Эдвардса имеют аффинное представление изоморфное, некоторой аффинной части эллиптической кривой, имеющей в порядке группы кривой множитель. Интересной является возможность построения скрученной кривой порядка Эдвардса $4p,\ p \in \mathbf{P}$, то есть такой, которая имеет минимальный кофактор. Поэтому естественно исследовать такие кривые и класс кривых, который обобщает эти кривые – скрученные кривые Эдвардса. Частично, изложенные результаты представлены в тезисах [7] и предыдущие исследования есть в статье автора [3].

С точки зрения алгебраической геометрии, кривая Эдвардса не является эллиптической, потому что она сингулярная. Кривые Эдвардса также как и скрученные кривые Эдвардса имеют аффинное представление изоморфное, некоторой аффинной части эллиптической кривой, имеющей в порядке группы кривой множитель. Как указано в работе В. Фултона [8] для построения "elliptic curve power generator" генератора и генератора "Naor-Reingold "используют не супер сингулярную эллиптическую кривую и ее точку P большого простого порядка, если же порядок l точки P не простой, то выбирают начальное заполнение e такое, что $(e,l)=1$.

Нашей целью является исследование свойств этих кривых, необходимых для ее применения в асимметричной криптографии, а также в криптоанализе, в частности исследования этой кривой на предмет сингулярности.

Постановка проблемы заключается в выявлении ресурсов математического аппарата, что позволит максимально быстро осуществлять групповую операцию связанную с сложением точки к собой либо обратную к удвоению точки – деление точки на 2 то есть с обратной операций к удвоению точки. То есть операция экспоненцирования точки кривой, которая лежит в основе проблемы дискретного логарифма.

Анализ особенностей скрученной кривой Эдвардса. Рассмотрим скрученную кривую Эдвадрса $E_{a,d}$

$$\begin{aligned} &ax^2 + y^2 = 1 + dx^2y^2,\ a,d \in F_p^*, \\ &ad(a-d) \neq 0,\ d \neq 1,\ p \neq 2,\ a \neq d, \end{aligned} \qquad (1)$$

При $a = d$ преобразуем кривую $ax^2 + y^2 = 1 + ax^2y^2$ к виду $ax^2 - ax^2y^2 - 1 + y^2 = 0$ или $ax^2(1-y^2) - (1-y^2) = 0$. Таким образом, кривая раскладывается в произведение двух пар прямых $(ax^2-1)(y^2-1) = 0$. Если $a = 1$, то $E_{a,\mathrm{d}}$ превращается в кривую E_{d}. Из условия гладкости находим особые точки аффинной кривой.

Обозначим $F(x,y) = ax^2 + y^2 = 1 + dx^2y^2$, a,d $\in \mathrm{F_p}^*$, $\mathrm{d} \neq 1,\ \mathrm{p} \neq 2,\ a \neq d$.

$$\begin{cases} \dfrac{\mathrm{F}(x,y)}{\partial x} = 0 \\ \dfrac{\mathrm{F}(x,y)}{\partial y} = 0 \end{cases}, \quad \begin{cases} 2ax = 2dxy^2 \\ 2y = 2dx^2y \end{cases},$$

$$\begin{cases} ax - dxy^2 = 0 \\ y - dx^2y = 0 \end{cases} \quad \begin{cases} x(a - dy^2) = 0 \\ y(1 - dx^2) = 0 \end{cases}$$

$$\left[\begin{cases} x=0 \\ y=0 \end{cases} \begin{cases} (a-dy^2)=0 \\ (1-dx^2)=0 \end{cases} \begin{matrix} (0,0) \\ \left(\pm\sqrt{\frac{1}{d}},\pm\sqrt{\frac{a}{d}}\right) \end{matrix}\right.$$

Но точка $(0,0)$ кривой $E_{a,\mathrm{d}}$ не принадлежит не зависимо от поля. Таким образом, получили аж 4 точки, согласно условию, что при этом для F_p коэффициенты a и d из F_p должны быть такими, что $\left(\frac{d}{p}\right)=1$ и $\left(\frac{ad}{p}\right)=1$, то есть $\left(\frac{d}{p}\right)=1$ и $\left(\frac{a}{p}\right)=1$. Таким образом, наявные 4 особенные точки с учетом того, что точка $(0,0)$ кривой не принадлежит.

Подсчитаем род кривой согласно Риду

$$\rho^*(C)=\rho_\alpha(\mathrm{C})-\sum_{p\in E}\delta_p=\frac{(n-1)(n-2)}{2}-\sum_{p\in E}\delta_p=3-2=1$$

или $n=4$. де $\rho_\alpha(C)$ – арифметический род кривой C, параметр $n=degC=4$.

Поскольку кривая имеет род 1, то она изоморфна плоской кубической кривой но не есть эллиптической, так как имеет особенности в проективной части. Кривая Эдварса как и скрученная кривая Эдаварса изоморфна некоторой аффинной части эллиптической кривой. Нормализация кривой Эдвардса – кривая E_M в форме Веерштрасса, которая предложена Монтгомери получена путем бирационального отображения $u=(1+y)/(1-y)$, $v=u/x$ в [9], и уже являющаяся эллиптической, что показано в теореме 3. 2 из [9]. Однако при анализе этой теоремы авторы–Бессалов А. В. и Цыганкова О. В. [12] путают бирациональную эквивалентность с изоморфизмом [11], зря критикуя теорему 3.2 из [9], где анализируется эта бирациональная эквивалентность. Также ими в [12] допущено неточность в конце раздела 1, где указан случай наявной корректной арифметики при четных d хотя нужно было указать квадратичность вычета $\left(\frac{d}{p}\right)=1$.

Свойства скрученной кривой Эдвардса. Лемма 1. Если (x,y) точка кривой $E_{a,d}$, тогда имеет место равенство $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$.

Доказательство. Из уравнения скрученной кривой Эдвардса $ax^2+y^2=(1+dx^2y^2)$ получаем $y^2-dx^2y^2=1-ax^2$ $y^2-dx^2y^2=1-ax^2$ откуда $y^2(1-dx^2)=(1-ax^2)$. А поскольку квадратичность левой части определяется лишь множителем $(1-dx^2)$, то имеет место конгруэнция $\left(\frac{1-dx_1^2}{p}\right)=\left(\frac{1-ax_1^2}{p}\right)$.

Лемма 2. Если (x,y) точка кривой $E_{a,d}$, тогда имеет место равенство $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$.

Доказательство. Из уравнения скрученной кривой Эдвардса $ax^2+y^2=(1+dx^2y^2)$ имеет $ax^2-dx^2y^2=1-y^2$ откуда $x^2(a-dy^2)=1-y^2$. А поскольку квадратичность левой части определяется лишь множителем $a-dy^2$, то имеет место конгруэнтность $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$.

Утверждение 1. Для произвольной не фундаментальной точки (x_1,y_1) кривой (1) при $e=1$ выполняется равенство $\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right)$.

Доказательство. Для точки $P=(x_1,y_1)$ удовлетворяющей уравнение кривой (1) рассмотрим произведение

$$(a-dy_1^2)(1-ax_1^2)=a+adx_1^2y_1^2-a^2x_1^2-dy_1^2=$$
$$=ay_1^2-dy_1^2=(a-d)y_1^2.$$

Согласно лемме 2 имеем $\left(\frac{a-dy_1^2}{p}\right)=\left(\frac{1-y_1^2}{p}\right)$ подставив это в последнее равенство вместо $(a-dy_1^2)$ получаем новое равенство вычетов $\left(\frac{1-ax_1^2}{p}\right)\left(\frac{1-y_1^2}{p}\right)=\left(\frac{a-d}{p}\right)$ что и нужно было доказать.

Ответ на вопрос о делимости точки на два для кривой E_d изучался в работах известных криптографов [9, 14].

Возможность выполнения обратной к удвоению точки операции до сих пор не исследована полностью для скрученной кривой Эдвардса, один из критерием был ранее предложен в работе автора [3] однако более удобным с вычислительной точки зрения является следующий критерий.

Возможность выполнения обратной операции к операции удвоения точки еще и до сих пор не исследовав для скрученной кривой Эдвардса, следующая теорема дает ответ на этот вопрос.

Под делимостью точки (*X*; *Y*) напополам понимает нахождения ее прообраза то есть точки (*x*; *y*), которая при применении формулы удвоения точки [1].

Теорема. Необходимым и достаточным условием существования точек деления на 2 для произвольной точки $G=(X,Y)$ скрученной кривой Эдвардса (1), которая не есть точкой 2-го или 4-го порядка, является условие

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

Доказательство. Для скрученной кривой Эдвардса закон удвоения имеет форму [2,9]

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

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

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

Рассмотрим уравнение $\frac{2x_1y_1}{1+dx_1^2y_1^2}=X$ равносильное $dXx^2y^2-2xy+X=0$ и применим замену $t=x_1y_1$ после чего получим уравнение

$dXt^2-2t+X=0$,

решение, которого существует тогда и только тогда когда $\left(\frac{1-dX^2}{p}\right)=1$ (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

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

.

Сделав замену $u=\frac{y}{x}$ получим $\frac{2u}{u^2+a}=X$ или $2u=X(u^2+a)$, переписав как квадратное уравнение относительно u имеем $Xu^2-2u+Xa=0$ с определителем $D_2=4(1-aX^2)$. Поэтому, согласно Лемме 1 уравнения $dXt^2-2t+X=0$ и $Xu^2-2u+Xa=0$ решения которых существуют или не существуют одновременно, что дает выражения для координат точки $P_j=(x_j,y_j)$: $x_j=\sqrt{t_ju_j^{-1}}, y_j=\sqrt{t_ju_j}$ $j\in\{0,1\}$.

Приравнивая левые части равности $\frac{2x_1y_1}{1+dx_1^2y_1^2}=X$ и $\frac{2x_1y_1}{y^2+ax_1^2}=X$ получаем $ax_1^2+y_1^2=1+dx_1^2y_1^2$, то есть полученные пара координат (x_i,y_j) удовлетворяет уравнению кривой, что также следует с замкнутости групповой операции. Заметим, что вместе с (x_1,y_1) выше указанные уравнения удовлетворяют точки $(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$.

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 $x=x_1,\ y=y_1$, имеем

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

$$=\frac{(y^2+ax^2)^2-4at^2}{(1+dt^2)^2-4dt^2}=\frac{(y^2-ax^2)^2}{(1-dt^2)^2}=\frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}$$

Поэтому, получили уравнение, которое задает вторую координату полученную в результате удвоения точки (x_1,y_1), возведенное в квадрат. Это уравнение мы используем для выбора правильного из дополнительных корней

$(-x_1,-y_1),(-y_1,-x_1),(y_1,x_1)$ 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 $y_1^2(1-dx_1^2)=1-ax_1^2$, и получаем

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

Из равенства (2) для второй координаты имеем определяющее уравнение

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

Поскольку мы ввели уравнение связи между переменными $t=x_1y_1$, то последнее уравнение примет вид $y_1^2-ax_1^2=Y(1-dt^2)$. Откуда, учитывая $t=x_1y_1$, получаем

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

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

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

Откуда

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

Которое после подстановки $t_{1,2}=\frac{1\pm\sqrt{1-dX^2}}{dX}$ даст

$$x_{1,2}^2=\frac{Y(\mathrm{d}(\frac{1\pm\sqrt{1-dX^2}}{dX})^2-1)}{2d}\pm$$
$$\pm\frac{\sqrt{Y^2(1-\mathrm{d}\frac{1\pm\sqrt{1-dX^2}}{dX})^2+4d(\frac{1\pm\sqrt{1-dX^2}}{dX})^2}}{2d} \quad (5)$$

Поскольку эти корни есть сопряженными иррациональностями, то точка $(\pm x,\pm y)$ удовлетворяют одновременно уравнение, 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 (9), должен быть квадратическим вычетом в $\mathbb{F}_p$. Заметим, что оба корни уравнений (4) и (5) есть 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 его удовлетворяют. Поэтому все найденные координаты удовлетворяют уравнению кривой (1) и уравнению операции удвоения точки.

Рассмотрим условия существования точек 8-го порядка которые тесно связаны с кофактором кривой.

Утверждение. Кривая Эдвардса содержит точку порядка 8 тогда и только тогда, когда

$$\left(\frac{1-d}{p}\right)=1.$$

Правильность утверждения следует из того, что точки 8-го порядка удовлетворяют уравнение $2Q=F$, где $F=(\pm1,0)$ – точек 4-го порядка. То, что точка Q имеет вид (x,x) следует из формул сложения точек [9] и из уравнения кривой (1) следует. Отсюда и из уравнения кривой имеем $2(x,x)=(\pm1,0)$, где $(\pm1,0)=F$ это координаты точки 4-го порядка. Значит, точка Q лежит на диагонали, т.е, другими словами $|x|=|y|$. Отсюда и из уравнения кривой имеем биквадратное уравнение $2x^2=1+dx^4$, $dx^4-2x^2+1=0$.

Дискриминант которого является следующим $D=4-4d=4(1-d)$. Поэтому, что бы решение существовало необходимо и достаточно, что бы $\left(\frac{1-d}{p}\right)=1$.

Замечание. Вместе с точкой $P=(x_1,y_1)$ уравнения (2), (3) а также уравнение самой кривой удовлетворяет также точка $Q=P+D=(x_2,y_2)$.

Доказательство следует из коммутативности группы точек, поэтому выполняется следующее тождество $Q+Q=P+D+P+D=2P+O$, так как точка D имеет порядок 2.

Теорема. Для существования точки 8-го порядка на скрученной кривой Эдвардса $E_{a,d}$ необходимо и достаточно чтобы следующие выражения

$$a,\ (1-\frac{d}{a}),\ (\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}})),\ \frac{a}{d}(1\pm\sqrt{1-\frac{d}{a}}),$$

были квадратичными вычетами над F_p.

Доказательство. Для исследования условий существования точки 8-го порядка на скрученной кривой Эдвардса возьмем такой класс этих кривых, где есть точка 4-го порядка - используем формулы координаты удвоенной [12] точки:

$$2(x,y)=(\frac{2xy}{1+dx^2y^2},\frac{y^2-ax^2}{1-dx^2y^2})$$

.

Подставим, в нее координаты точки 4-го порядка $2(x,y)=(\frac{1}{\pm\sqrt{a}},0)$ [9] и найдем координаты точки (x,y), которая удовлетворит условиям этого уравнения

$$(\frac{2xy}{1+dx^2y^2},\frac{y^2-ax^2}{1-dx^2y^2})=(\pm\frac{1}{\sqrt{a}},0)$$

.

Покоординатное соответствие дает систему

$$\begin{cases}\frac{2xy}{1+dx^2y^2}=\frac{1}{\sqrt{a}}\\ \frac{y^2-ax^2}{1-dx^2y^2}=0\end{cases}$$

Для координаты $-\frac{1}{\sqrt{a}}$ в правой части уравнения первого уравнения система аналогична.

С другого равенства имеем $ax^2=y^2$, $y=\pm\sqrt{a}x$.

Подставив $y=\pm\sqrt{a}x$ в первое равенство, имеем

$$\frac{2x\sqrt{a}x}{1+dx^2ay^2}=\frac{1}{\sqrt{a}}$$

откуда $2ax^2=1+adx^4$. Решим это уравнение $adx^4-2ax^2+1=0$:

$$x^2=\frac{a\pm\sqrt{a^2-ad}}{ad}=\frac{1}{d}\pm\frac{\sqrt{1-\frac{d}{a}}}{d}=\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}}).$$

Выполним проверку для чего преобразуем

$$x^2=\frac{a\pm\sqrt{a^2-ad}}{ad}=\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}}),$$

$$x^4=\frac{1}{d^2}(1\pm\sqrt{1-\frac{d}{a}})^2=\frac{1}{d^2}(1+1-\frac{d}{a}\pm2\sqrt{1-\frac{d}{a}}),\ \text{тогда}$$

$$adx^4-2ax^2+1=\frac{a}{d}(2-\frac{d}{a}\pm2\sqrt{1-\frac{d}{a}})-\frac{2a}{d}(1\pm\sqrt{1-\frac{d}{a}})+1=$$

$$=\frac{2a}{d}-1\pm\frac{2a}{d}\sqrt{1-\frac{d}{a}}-\frac{2a}{d}\pm\frac{2a}{d}\sqrt{1-\frac{d}{a}}+1=0$$

Таким образом, выполняется.

Использовав уравнение скрученной кривой Эдвардса, находим $y^2=\frac{a}{d}(1\pm\sqrt{1-\frac{d}{a}})$. Значит правая часть последнего выражения должна быть квадратичным вычетом.

Проверим условие принадлежности кривой (1) точек с координатами $x^2=\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}})$, $y^2=\frac{a}{d}(1\pm\sqrt{1-\frac{d}{a}})$: $\frac{2a}{d}(1\pm\sqrt{1-\frac{d}{a}})=$

$$=\frac{(y^2-ax^2)^2}{(1-dx^2y^2)^2}1+\frac{a}{d}(1+1-\frac{d}{a}\pm2\sqrt{1-\frac{d}{a}})=$$

$$=\frac{2a}{d}(1\pm\sqrt{1-\frac{d}{a}})=1\pm\frac{2a}{d}-1\pm\frac{2}{d}\sqrt{1-\frac{d}{a}}=\frac{2a}{d}(1\pm\sqrt{2-\frac{d}{a}}).$$

Проверим удовлетворяет ли первая (вторая аналогично) координата уравнения формуле удвоения

$$\frac{2\sqrt{a}x}{1+dx^2y^2}=\frac{2\sqrt{a}\,\frac{1}{d}(1\pm\sqrt{1-\frac{d}{a}})}{1+d\,\frac{a}{d^2}(1\pm\sqrt{1-\frac{d}{a}})^2}=$$

$$=\frac{\frac{2\sqrt{a}}{d}(1\pm\sqrt{1-\frac{d}{a}})}{1+\frac{a}{d}(1+1-\frac{d}{a}\pm\sqrt{1-\frac{d}{a}})}=\frac{-1}{\sqrt{a}}.$$

Критерии делимости точки на 2 могут быть использованы для построения метода выбора и тестирования случайной точки $T = (a, b)$ на максимальность порядка как это сделано в для обычной кривой Эдвардса [15]. Там для получения точки максимального порядка производится тестирование величины $(1 – dx^2)$ на квадратичность, что как показано в [15] напрямую связано с делимостью на 2 точки (x, y). В силу того, что точка максимального порядка не делится на 2 получение критерия делимости точки на 2 есть необходимым условием для максимальности порядка точки скрученной кривой Эдвардса.

Также в работе [15] показано, что условие деления точки на два может быть использовано для определения порядка случайной точки кривой Эдвардса, поэтому полученные нами критерии для скрученной кривой Эдвардса имеют туже значимость.

Выводы. Исследование позволило найти критерии делимости точки на два, что может быть применено как в крипто анализе, так и при построении генератора псевдослучайных криптостойких последовательностей и электронно-цифровой подписи на эллиптической кривой.

Список литературы:

1. *Edwards, H. M.* A normal form for elliptic curves [Text] / *H. M. Edwards* // Bulletin of the American Mathematical Society. – 2007. – Vol. 44, Issue 03. – P. 393–423. doi: 10.1090/s0273-0979-07-01153-6
2. *Hisil, H.* Twisted Edwards Curves Revisited [Text] / *H. Hisil, K. K.-H. Wong, G. Carter, E. Dawson* // Lecture Notes in Computer Science. – 2008. – P. 326–343. doi: 10.1007/978-3-540-89255-7_20
3. *Скуратовський, Р.* Нормалізація скрученої кривої Едвардса та дослідження її властивостей над Fp [Текст]: Матер. XIV Всеукр. наук.-практ. конф. / *Р. Скуратовський, А. Мовчан* // Теоретичні і прикладні проблеми фізики, математики та інформатики. Секція: Теоретичні та прикладні проблеми криптографічного захисту інформації. – Київ: НТУУ «КПІ», 2016. – С. 102–104.
4. *Скуратовський, Р.* Дослідження властивостей скрученої кривої Едвардса [Електронний ресурс] / *Р. Скуратовський* // Конференція державної служби спеціального звязку та захисту інформації. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?showHidden=1artid=252312catid=240232ctime=1464080781894
5. *Сергієнко, І. В.* Елементи загальної теорії оптимальних алгоритмів та суміжні питання [Текст] / *І. В. Сергієнко, В. К. Задірака, О. М. Литвин*. – К.: Наук. думка, 2012. – 400 с.
6. *Skuratovskii, R. V.* Twisted Edwards curve and its group of points over finite field Fp [Text] / *R. V. Skuratovskii, U. V. Skruncovich* // XI Літня школа "Алгебра, Топологія, Аналіз". – 2016. – С. 122–124.
7. *Skuratovskii, R. V.* Twisted Edwards curve and its group of points over finite field Fp [Text] / *R. V. Skuratovskii, U. V. Skruncovich* // Conference. Graphs and Groups, Spectra and Symmetries. – 2016. – Available at: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf
8. *Fulton, W.* Algebraic curves. An Introduction to Algebraic Geometry [Text] / *W. Fulton* // Third Preface. – 2008. – 121 p.
9. *Bernstein, D. J.* IST Programme under Contract IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498 [Text] / *D. J. Bernstein, P. Birkner, M. Joye, T. Lange, C. Peters, T. E. Curves* // 2008. – P. 1–17.
10. *Долгов, В. И.* Эллиптические кривые в криптографии [Текст] / *В. И. Долгов* // Системи обробки інформації. – 2008. – Вип. 6 (73). – С. 3–10.
11. *Скуратовский, Р. В.* Метод быстрого таймерного кодирования текстов [Текст] / *Р. В. Скуратовский* // Кибернетика и системный анализ. – 2013. – Т. 49, № 1. – С. 154–160.
12. *Бессалов, А. В.* Производительность групповых операций на скрученной кривой Эдвардса над простым [Текст] / *А. В. Бессалов, О. В. Цыганкова* // Радиотехника. – 2015. – Вып. 181. – С. 58–63.
13. *Алексеев, Е. К.* О перспективах использования скрученных эллиптических кривых Эдвардса со стандартом ГОСТ Р 34.10-2012 и алгоритмом ключевого обмена на его основе [Текст] / *Е. К. Алексеев, И. Б. Ошкин, В. О. Попов, С. В. Смышляев, Л. А. Сонина* // Материалы XVI международной конференции "РусКрипто'2014". – 2014.
14. *Bruce, S.* Applied Cryptography: Protocols, Algorithms, and Source Code in C [Text] / *S. Bruce*. 2nd ed. – 2002. – 816 p.
15. *Бессалов, А. В.* Удвоение точки и обратная задача для кривой Эдвардса над простым полем. Условие деления точки на два для определения порядка случайной точки кривой Эдвардса [Текст] / *А. В. Бессалов, Д. Б. Третьяков* // Сучасний захист інформації. – 2013. – № 3. – С. 56–58.

Bibliography (transliterated):

1. Edwards, H. M. (2007). A normal form for elliptic curves. Bulletin of the American Mathematical Society, 44 (03), 393–423. doi: 10.1090/s0273-0979-07-01153-6
2. Hisil, H., Wong, K. K.-H., Carter, G., Dawson, E. (2008). Twisted Edwards Curves Revisited. Lecture Notes in Computer Science, 326–343. doi: 10.1007/978-3-540-89255-7_20
3. Skuratovskyi, R., Movchan, A. (2016). Normalizatsiya skruchenoi kryvoi Edvardsa ta doslidzhennia yii vlastyvostei nad Fp. Teoretychni i prykladni problemy fizyky, matematyky ta informatyky. Sektsiya: Teoretychni ta prykladni problemy kryptohrafichnoho zakhystu informatsiyi. Kyiv: NTUU «KPI», 102–104.
4. Skuratovskyi, R. Doslidzhennia vlastyvostei skruchenoi kryvoi Edvardsa. Konferentsiya derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsiyi. Available at: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article? showHidden=1artid=252312catid=240232ctime=1464080781894
5. Serhiienko, I. V., Zadiraka, V. K., Lytvyn, O. M. (2012). Elementy zahalnoi teoriyi optymalnykh alhorytmiv ta sumizhni pytannia. Kyiv: Nauk. dumka, 400.
6. Skuratovskii, R. V., Skruncovich, U. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. XI Litnia shkola "Alhebra, Topolohiya, Analiz", 122–124.
7. Skuratovskii, R. V., Skruncovich, U. V. (2016). Twisted Edwards curve and its group of points over finite field Fp. Conference. Graphs and Groups, Spectra and Symmetries. Available at: http://math.nsc.ru/conference/g2/g2s2/exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf
8. Fulton, W. (2008). Algebraic curves. An Introduction to Algebraic Geometry. Third Preface, 121.
9. Bernstein, D. J., Birkner, P., Joye, M., Lange, T., Peters, C., Curves, T. E. (2008). IST Programme under Contract IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498, 1–17.

10. Dolgov, V. I. (2008). Ellipticheskie krivye v kriptografii. Systemy obrobky informatsiyi, 6 (73), 3–10.
11. Skuratovskiy, R. V. (2013). Metod bystrogo taymernogo kodirovaniya tekstov. Kibernetika i sistemnyy analiz, 49 (1), 154–160.
12. Bessalov, A. V., Cygankova, O. V. (2015). Proizvoditel'nost' gruppovyh operaciy na skruchennoy krivoy Edvardsa nad prostym. Radiotekhnika, 181, 58–63.
13. Alekseev, E. K., Oshkin, I. B., Popov, V. O., Smyshlyaev, S. V., Sonina, L. A. (2014). O perspektivah ispol'zovaniya skruchennyh ellipticheskih krivyh Edvardsa so standartom GOST R 34.10-2012 i algoritmom klyuchevogo obmena na ego osnove. Materialy XVI mezhdunarodnoy konferencii "RusKripto'2014".
14. Bruce, S. (2002). Applied Cryptography: Protocols, Algorithms, and Source Code in C, 816.
15. Bessalov, A. V., Tret'yakov, D. B. (2013). Udvoenie tochki i obratnaya zadacha dlya krivoy Edvardsa nad prostym polem. Uslovie deleniya tochki na dva dlya opredeleniya poryadka sluchaynoy tochki krivoy Edvardsa. Suchasnyi zakhyst informatsiyi, 3, 56–58.

Поступила (received) 06.12.2017

Бібліографічні описи / Библиографические описания / Bibliographic descriptions

Ділення точки скручених кривих Едвардса на два та його застосування у криптографії/ Скуратівський Р. В., Осадчий Є. О., КвашукД. М. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.90–96. – Bibliogr.:15. – ISSN 2079-5459

Деление точки скрученных кривой Эдвардса на два и его применение в криптографии/ Скуратовский Р. В., Осадчий Е. А., КвашукД. М. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.90–96. – Bibliogr.:15. – ISSN 2079-5459

Halving of twisted Edwards curve points and its application in cryptography/ Skuratovskii R., Osadchy E., Kvashuk D. //Bulletin of NTU "KhPI". Series: Mechanical-technological systems and complexes. – Kharkov: NTU "KhPI", 2017. – № 44 (1266).– P.90–96. – Bibliogr.:15. – ISSN 2079-5459

Відомості про авторів / Сведения об авторах / About the Authors

Скуратовский Руслан Вячеславович – преподаватель, кафедра информационной безопасности, Межрегиональная Академия управления персоналом, ул. Фрометовская, 2, г. Киев, Украина, 03039.

Осадчий Евгений Александрович – кандидат технических наук, заведующий НИЛ высокопроизводительных систем обработки информации, Киевский национальный университет имени Тараса Шевченко, ул. Владимирская, 60, г. Киев, Украина, 01601.

Квашук Дмитрий Михайлович – доцент, кафедра экономической кибернетики Национальный авиационный университет, просп. Космонавта Комарова, 1, г. Киев, Украина, 03058.

Скуратовський Руслан В'ячеславович – викладач, кафедра інформаційної безпеки, Міжрегіональна Академія управління персоналом, вул. Фрометівська, 2, м. Київ, Україна, 03039.

Осадчий Євген Олександрович – кандидат технічних наук, завідувач НДЛ високопродуктивних систем обробки інформації, Київський національний університет імені Тараса Шевченка, вул. Володимирська, 60, м. Київ, Україна, 01601.

Квашук Дмитро Михайлович – доцент, кафедра економічної кібернетики Національний авіаційний університет, просп. Космонавта Комарова, 1, м. Київ, Україна, 03058.

Skuratovskii Ruslan – teacher, Department of information security, Interregional Academy of Personnel Management, Frometovskaya, str., 2, Kiev, Ukraine, 03039.

Osadchy Evgeny – PhD, Head of NIL of high-performance information processing systems, Kyiv National Taras Shevchenko University, Vladimirskaya, str., 60, Kiev, Ukraine, 01601.

Kvashuk Dmitry – Associate Professor, Department of Economic Cybernetics National Aviation University, Cosmonaut Komarov, ave., 1, Kiev, Ukraine, 03058.