DOI: 10.18372/2410-7840.20.13101
УДК 681.3, 512.742.72 +514.135(0.034)

ПСЕВДОСЛУЧАЙНЫЕ КРИПТОСТОЙКИЕ ПОСЛЕДОВАТЕЛЬНОСТИ И ДЕЛЕНИЕ ТОЧКИ ДЛЯ СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМИ И СОСТАВНЫМИ ПОЛЯМИ

Руслан Скуратовский

Получены оценки сложности операции деления точки кривой в форме Эдвардса на два и их сравнение с удвоением точки. Рассмотрено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме. Показана криптостойкость генератора псевдослучайных последовательностей, предложенного автором, на основе кривой в форме Эдвардса. Показано возможность применения данных кривых для генерации криптостойкой последовательности большого периода. Предложена новая схема генерирования и новая односторонняя функция псевдослучайной криптостойкой последовательности на основе этих кривых. Исследована степень погружения этих кривых в конечное поле для спаривания на дружественных эллиптических кривых простого порядка или почти простого порядка. Последнне есть очень существенным во многих криптографических протоколах вида короткой цифровой подписи длительного использования. Для этой цели мы нашли дружественные кривые на основе семейства скрученных кривых Эдвардса. Найдено возможность построения скрученной кривой порядка Эдвардса $4p,\ p \in \mathbf{P}$*, то есть такой, которая имеет минимальный кофактор 4. Получено решение задачи обратной к удвоению для квази-эллиптических кривых, представленных в скрученной форме Эдвардса и ее применение к обоснование криптостойкости генератора псевдослучайных последовательностей. Она дает возможность обосновать стойкость разработанного нами генератора псевдослучайных криптостойких последовательностей.*

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

Введение

Одним из основных свойств генератора криптоскойкой псевдослучайной последовательности. (ГПСЧ) есть его надежность даже в случае, когда часть или все его состояния стали известны (или были корректно вычислены). Это значит, что не должно быть возможности получить случайную последовательность, созданную генератором, предшествующую получению этого знания криптоаналитиком. Т.е. попытка вычислить знание о входных данных должна быть вычислительно невозможна. Также одной из уязвимостей ГПСЧ является свойство генератора псевдослучайных последовательностей называемое: предсказуемое начальное значение генератора. Именно для обоснования экспонциальности функции роста сложности для задачи нахождения начального значения ГПСЧ мы исследуем обратную задачу к удвоению точки – деление точки на 2.

Большинство криптосистем современной криптографии естественным образом можно реализовать на эллиптических кривых. 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. Найдено возможность построения генератора случайных криптостойких последовательностей на этой кривой. Целью роботы есть получение новых [2, 3] и уточнение старых критериев делимости точки кривой не только напополам, но и на 4 над полем F_{p^n} и анализ свойств скрученной кривой Эдвардса необходимых для построения генератора псевдослучайных криптостойких последовательностей.

Важность операции делимости точки на 2 при криптоанализе уже частично описана в работе А. В. Бессалова [4]. Мы также подчеркнем ее значимость для определения порядка случайной точки кривой Эдвардса, которая рассматривается в качестве кандидата на инициальную точку криптостойкой последовательности. Этому вопросу также уделялось внимание в пункте 3 статьи [4], где исследовались условия делимости точки обычной кривой Эдвардса. Наша цель найти эти условия и исследовать возможности их применения для скрученной кривой Эдвардса.

Основной результат

Напомним, что скрученная кривая Эдвадрса $E_{a,d}$ имеет вид:

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

Определение 1. Несингулярная эллиптическая кривая над F_p называется дружественно-спаривающей, если она содержит подгруппу порядка

r, степень вложения которой k не слишком велика, что означает, что быстрые вычисления в поле F_{p^k} возможны.

Определение 2. Натуральное число k называется степенью вложения эллиптической кривой E (относительно r), если k - наименьшее целое число такое, что $r \mid p^k - 1$ и k – порядок p в мультипликативной группе Z_r^*.

Теорема 1. Если кривая $E_{1,d}$ над F_p (F_{p^n}), где $p \equiv 7(mod 8)$, $n \equiv 1 \bmod 2$ и выполнено условие $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\bmod p)$, $(\frac{d}{p}) = 1$, при этом $p = 8q - 1$ ($p^n + 1 = 8q$), где $p, q \in \mathrm{P}$, то группа всех ее точек имеет кофактор 8.

Доказательство. Напомним теорему доказанную автором в [2], где найдено порядок, как количество аффинных точек, суперсингулярной кривой над F_p, который для $p \equiv 7(mod 8)$ равен $p - 3$. Поэтому из наложенного условия $p + 1 = 8q$ получим, что группа всех точек, включая особые точки (существование которых обеспечивается условием $(\frac{d}{p}) = 1$ [20], кривой имеет порядок $8q$. Согласно теореме Кели, она имеет циклическую подгруппу порядка q. Поэтому ее кофактор равен 8.

Заметим, что если для кривой $E_{a,d}$ выполнено условие $(\frac{a}{p}) = 1$, то мы имеем изоморфизм кривых $E_{a,d}$ и $E_{1,d}$, который задается форулой $(\bar{x}, \bar{y}) \mapsto (x, y) = \left(\bar{x}, \frac{1}{\bar{y}}\right)$ [1], где коэффициент изоморфной кривой $E_{1,D}$ как $D = \frac{d}{a}$. Поэтому мы получаем следствие из теоремы 1.

Следствие 1. Если кривая $E_{a,d}$ над F_p (F_{p^n}), где $p \equiv 7(mod 8)$, $p = 8q - 1$ и $n \equiv 1 \bmod 2$ $p, q \in \mathrm{P}$, где $p, q \in \mathrm{P}$, а также выполнено условие $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 D^j \equiv 0(\bmod p)$ и $(\frac{a}{p}) = 1, (\frac{D}{p}) = 1$, то группа всех ее точек имеет имеет кофактор 8.

Доказательство. Поскольку, как сказано выше, в случае $(\frac{a}{p}) = 1$ кривые $E_{a,d}$ и $E_{1,D}$ изоморфны, то проанализируем кривую $E_{1,d}$. Из теоремы о суперсингулярности доказанной автором в [2], где найдено порядок, как количество афинных точек, суперсингулярной кривой над F_p, который для $p \equiv 7(mod 8)$ равен $p - 3$. Поэтому из наложенного условия $p = 8q - 1$ получим, что группа всех точек, включая особые точки (существование которых обеспечивается условием $(\frac{ad}{p}) = 1$ [20], оно равносильно условию теоремы $(\frac{D}{p}) = 1$, кривой имеет порядок $8q$. Согласно теореме Кели, она имеет циклическую подгруппу порядка q. Поэтому ее кофактор равен 8.

Теорема 2. Если кривая задана над полем F_p, $p \equiv 3(mod 8)$ и выполнено условие $\sum_{j=0}^{\frac{p-1}{2}} (C_{\frac{p-1}{2}}^{j})^2 d^j \equiv 0(\bmod p)$, при этом $p + 1 = 4q$, где $p, q \in \mathrm{P}$, то она имеет минимальный кофактор 4.

Доказательство имеет аналогичную структуру с доказательством предыдущей теоремы.

Делимость точек скрученной кривой Эдвардса

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

Теорема 3. *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

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

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 $dXx^2y^2 - 2xy + X = 0$, при $1 + dx_1^2y_1^2 \neq 0$, и применим замену $t = x_1y_1$, после чего получим уравнение $dXt^2 - 2t + X = 0$, решение, которого существует тогда и только тогда, когда $\left(\frac{1 - dX^2}{p}\right) = 1$ (или если $1 - dX^2 \equiv 0(\bmod p)$).

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, 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 $P_j=(x_j,y_j)$: $x_j=\sqrt{t_ju_j^{-1}}, y_j=\sqrt{t_ju_j}\quad j\in\{0,1\}$.

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 $x=x_1,\ y=y_1$, 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). 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 $y_1^2(1-dx_1^2)=1-ax_1^2$, 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 замену 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

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

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

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

Заметим, что знаки $\pm$ перед выражениеми $\sqrt{1-dX^2}$ 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 (9), 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 точки.

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 одинаковым образом. А полученные выражения обозначаем как g_1 для "+" и как g_2 для знака "–". Обозначим E – единичный элемент в группе точек кривой $E_{a,d}$.

Теорема 4. Для любой точки A, допускающей деление надвое, существует столько же точек со свойством $2B=A$, сколько существует на кривой точек D, для котрих $2D=E$.

Доказательство. Пусть D_i, $i\in 2,4$ семейство точек удовлетворяющих условию $2D=E$. Тогда каждая из них удовлетвоеряет и уравнение $2(B+D_i)=A$, которое по сути есть уравнение (2), где точка $B+D_i=(x_1,y_1)$ и удовлетворяет условию $2(x_1,y_1)=\left(\frac{2x_1y_1}{y_1^2+ax_1^2},\frac{y_1^2-ax_1^2}{1-dx_1^2y_1^2}\right)=(X,Y)$. Действительно $2(x_1,y_1)=2(B+D_i)=2B+2D_i=A+E=A$. Таким, образом совокупное количество решений уравнения (2) равно I, где I – количество прообразов в группе точек $E_{a,d}$.

Следствие 2. Необходимым и достаточным условием существования 4 разных точек, для которых результат удвоения равен *G,* является:

$$(\frac{1-dX^2}{p})=1 \text{ и } (\frac{g}{p})=1.$$

Следствие 3. 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 $\left(\frac{ad}{p}\right)=1$ [Mon].

Данное утверждение равносильно следующему.

Следствие 4. Если $\left(\frac{1-aX^2}{p}\right)\neq -1$ и $(x,y)\in E_{a,d}$, то $A=(X,Y)$ существует либо 2 прообраза при делении ее на два если $\left(\frac{ad}{p}\right)=-1$, либо 4 прообраза если $\left(\frac{ad}{p}\right)=1$ [20, 3].

Доказательство основывается на **Теореме 2 и условия существования особых точек 2-го порядка записанного как** $\left(\frac{ad}{p}\right)=1$ [Mon, Sk]. Таким образом количество точек от деления точки A на 2 определяется количеством точек D, со свойством $2D=E$. Количество таких точек определяется условием $\left(\frac{ad}{p}\right)=1$ [Mon, Sk=2, 3].

Более очевидными есть ниже изложенные следствия, которые не требуют доказательства.

Следствие 4. Если $(\frac{\sqrt{1-dX^2}}{p})=1$ и $(\frac{g}{p})=1$ при подстановке в g каждого корня из $\sqrt{1-dX^2}$, то существует 4 прообраза.

Если $(\frac{\sqrt{1-dX^2}}{p})=1$ и $(\frac{g}{p})=1$ при подстановке в g одного корня из $\sqrt{1-dX^2}$ и $(\frac{g}{p})=0$ при подстановке в g второго корня, то существует 2 прообраза при делении точки G.

Если $(\frac{\sqrt{1-dX^2}}{p})=1$ и $(\frac{g}{p})=1$ при подстановке в g каждого корня из $\sqrt{1-dX^2}$, то существует 4 прообраза у точки G.

Если $(\frac{\sqrt{1-dX^2}}{p})=0$ и $(\frac{g}{p})=1$ при подстановке в g единственного корня из $\sqrt{1-dX^2}$, то существует 2 прообраза у точки G.

Свойство 1. Степень погружения [9] группы суперсингулярной кривой $E_{1,d}$ равна 2.

Действительно порядок группы суперсингулярной кривой $E_{1,d}$ равен p^k+1, это число делит $p^{2k}-1$ и не делит выражения $p^{2k}-1$ с меньшими значениями k в силу разложения выражения $p^{2k}-1=(p^k-1)(p^k+1)$. Поэтому, согласно определению, из [9], степень погружения равна 2. Конец доказательства.

Построение генератора случайной криптостойкой последовательности

Рассмотрим построение генератора псевдослучайных последовательностей на основе удвоения точки скрученной кривой Эдвардса

При использовании кривых Эдвардса над простым полем порядок кривой $N_E = 4n$, где n – большое простое число. После нахождения случайной точки $Q = (x_Q, y_Q)$ кривой генератор криптосистемы порядка n нетрудно найти как точку $G = (x_G, y_G) = 4Q$, для чего потребуется два удвоения (т.е. две групповые операции).

Пусть $\left(m, \left|E_{1,d}\right|\right) = 1$, где $e \in \mathbb{N}$, тогда в качестве функции генерации псевдослучайных последовательностей над полем $\mathbb{F}_{p^n}$ возьмем $P_i = m^i P_0$, $P_i \in E_{1,d}$, P_0 – образующий группы точек кривой $E_{1,d}$. Труднообратимость этой операции основывается па проблеме дискретного логарифма. Пусть бит сложности это 0, если $Tr(x_i) < \frac{p-1}{2}$ и 1, если $Tr(x_i) \geq \frac{p-1}{2}$. Эта схема подобна той, что в PBSG генераторе [11], но предикат односторонней функции другой, кроме того и период последовательности этого генератороа гарантовано велик. Опереция удвоення точки на кривой $E_{1,d}$ есть **более быстрой чем опереция** eP, $e \in \mathbb{N}$ на обычной эллиптической кривой в форме Вейерштрасса, которая рассмотрена как основа для построения генератора в [11].

Известно, что скалярное произведение для точек кривой Эдвардса вычисляется минимальным числом операций в поле, сравнимо с другим известным представлением эллиптических кривых [4, 12]. согласно схеме Горнера, вычисление скалярного произведения kP на кривой Эдвардса WED = 4M + 4S + 1U= 7.17M. Что для эллиптической кривой в канонической форме составляет WE = 10.35M. Аналогично сложности добавлений VED = 9.5M и VE = 13.33M.

Мы используем схему генераци степенного генератора эллиптической кривой $P_i = m^i P$. В нашем случае период тоже будет мультипликативным порядком m по модулю n, где $n = \left|E\right|$ порядок группы эллиптичной кривой. Для максимизации периода T генератора выберем секретный множитель $m : \left(m, n\right) = 1$, тогда величина T будет равна $T = HCK(n, m)$. Вместе с тем операция генерирования следующего элемента последовательности станет проще и быстрее чем в генераторе Калиски [11]. А учитывая скорость удвоения точки суперсингулярних кривых описанную в [3], где есть схема Горнера для исчисления скалярного произведения методом аддитивных цепочек kP.

При использовании нормальных базисов для вычисления степеней, необходимых при формировании аддитивной цепочки в скалярном произведении kP, остаются только операции сложения, так удвоениями можно пренебречь. Поэтому оценка вычисления kP є $O(A2^{m-1} + A\frac{n}{m})$ [17], где m – степень обраной симетризованной системы счисления для представления k нам удобнее брать $m = 3$, A – сложность сложения и отнимания, $n = \left[\log_2 k\right] + 1$. Поэтому использование именно кривой Эдвардса дает наибольшее быстродейсвие генератора, так как на ней операция kP наиболее быстрая.

Известно, что вычисления порядка кривой является не простой задачей [3] но для суперсингулярних кривых порядки известны и метод их построения указано в нашей теореме. пусть $\left|E_{1,d}\right| = n = p^k + 1$ и $n = mq$, $q \in \mathbb{P}$ при этом q большое. Пусть G – генератор группы кривой $E_{1,d}$.

Возьмем эллиптическую кривую заданного большого простого порядка [3], при этом $p \neq q$. В качестве односторонней функции возьмем функцию: $P_i = f(P_{i-1}) = \phi(P_{i-1})G$, где

$$\phi(P_{i-1}) = \begin{cases} x, & P_{i-1} = (x, y) \\ p, & P_{i-1} = O \end{cases}.$$

Применим формулу генерации $P_i = f(P_{i-1}) = \phi(P_{i-1})G$. Тогда сложность обращения этой функции равносильна задаче дискретного логарифма.

Битом сложности этой односторонней функци есть предикат $\mathrm{P}(P_{i-1}) = (\frac{\phi(P_{i-1})}{p})$ альтернативой ему есть предикат

$$\mathrm{P}(P_{i-1}) = \begin{cases} 1, & x_i \geq \frac{p-1}{2} \\ 0, & x_i < \frac{p-1}{2} \end{cases}.$$

Сложность вычисленияя произведения $P_i = f(P_{i-1}) = \phi(P_{i-1})G$ согласно с методом удвоенияя и сложения $O((\log_2 \phi(P) - 1)(\mathrm{W}(\phi(P) - 1)))$ [17].

Для максимизации периода последовательности генератора мы можем использовать циклическую группу кривой $E_{1,d}$ не простого порядка. Что бы образующий G этой группы C_n отобразисля в образующий этой же группы будем применять

сложение его с собой такое количество раз которое взаимно простое с порядком групы. То есть $P_i = f(P_{i-1}) = \frac{\phi(P_{i-1})}{(\phi(P_{i-1}),|E_d|)}G$, где $|E_d|-$ порядок группы кривой $E_{1,d}$. Возможной модификацией есть выбор той координаты точки P_i у которой НОД с $|E|$ есть наименьшим. То есть зададим $t := \underset{z\in\{x,y\}}{\text{Argmin}}\left(\gcd(x,|E|),\gcd(y,|E|)\right)$ тогда в качестве множителя возьмем:

$$\phi(P_{i-1}) = \begin{cases} t, & P_{i-1} = (x,\ y); \\ p, & P_{i-1} = O. \end{cases}$$

Вывод

В работе построен генератор псевдослучайных последовательностей большего периода на основе данных кривых.

Построенный нами генератор криптостойких случайных последовательностей на скрученной кривой Эдвардса имеет большее быстродействие чем генератор Калисски. Благодаря исследованию удалось показать наличие надежности генератора при атаке вычисления входных данных т.е. зерна генератора. Было показано что даже если часть состояний генратора стали известны (или были корректно вычислены), то попытка вычислить знание о входных данных должна быть вычислительно невозможна. Именно для обоснования экспонциальности функции роста сложности для задачи нахождения начального значения ГПСЧ была исследована обратная задача.

Полученный нами критерий делимости точки распосраняется на произвольную скрученную кривую Эдвардса в отличии от того который был сформулирован авторами ранее лишь для обычной кривой Эдварса являющейся частным случаем скрученной кривой Эдвардса .

В работе исследована операция к удвоению точки для скрученной кривой Эдвардса над простыми и составными полями. Получены оценки сложности операции деления на два в сравнении с удвоением точки. Рассмотрено одно из приложений свойств делимости точки на два для определения порядка точки в криптосистеме.

Найдено возможность построения скрученной кривой порядка Эдвардса с минимальным кофактором 4.

Благодарность: автор выражает благодарность А. Рыбаку за полезные знания.

ЛИТЕРАТУРА

[1]. Bernstein Daniel J., Birkner Peter, Joye Marc, Lange Tanja, Peters Christiane, *Twisted Edwards Curves. IST Programme under Contract* IST-2002-507932 ECRYPT, and in part by the National Science Foundation under grant ITR-0716498, pp. 1-17, 2008.

[2]. Р. Скуратовський, "Побудова еліптичних кривих з нульовим слідом ендоморфізма Фробеніуса", *Захист інформації*, т. 20, №1, С. 32-45, 2018.

[3]. Р. Скуратовський, "Суперсингулярність еліптичних кривих і кривих Едвардса над F_{p^n}", *Research in mathematics and mechanics*, т. 31, №1, С. 17-26, 2018.

[4]. А. Бессалов, Д. Третьяков, "Удвоение точки и обратная задача для кривой Эдвардса над простым полем", *Сучасний захист інформації,* № 3, С. 16-27, 2013.

[5]. D. Bernstein, "Lange Tanja. Faster addition and doubling on elliptic curves", *IST Programme Contract 2002-507932 ECRYPT*, pp. 1-20, 2007.

[6]. A. Menezes, T. Okamoto, S. Vanstone, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", *IEEE Transactions On Information Theory*, vol. 39, no. 5, pp. 1603-1646, 1993.

[7]. N. Koblitz, "Eliptic Curve Cryptosystems", *Mathematics of Computation*, vol. 48, no. 177, pp. 203-209, 1987.

[8]. Yu. Drozd, *Vstup do alhebrayichnoyi heometriyi,* 2004, 251 p.

[9]. S. Paulo, M. Barreto, M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order", *International Workshop on Selected Areas in Cryptography SAC,* pp. 319-331, 2005.

[10]. P. Deepthi, P. Sathidevi, "New stream ciphers based on elliptic curve point multiplication", *Computer Communications*, no. 32, pp. 25-33, 2009.

[11]. B. Kaliski, "Elliptic Curves and Cryptography: A Pseudorandom Bit Generator and Other Tools", *PhD thesis*, MIT, Cambridge, MA, USA, 1988, 121 p.

[12]. А. Бессалов, О. Цыганкова, "Производительность групповых операций на скрученной кривой Эдвардса", *Радиотехника*, вып. 181, С. 58-63, 2015.

[13]. А. Белецкий, "Симметричный блочный криптоалгоритм", *Захист інформації,* № 2, С. 42-51, 2006.

[14]. Р. Скуратовский, Е. Осадчий, Д. Квашук, *Деление точки скрученной кривой Эдвардса на два и ее применение в криптографии.*

[15]. Н. Глазунов, Ф. Карпинский, В. Корняк, "Решение некоторых задач алгебры, анализа и математической физики с помощью систем аналитических вычислений на ЭВМ", *Кибернетика и системный анализ*, № 2, С. 23, 1990.

[16]. R. Skuratovskii, U. Skruncovich,. "Twisted Edwards curve and its group of points over finite field F_p", *Akademgorodok, Novosibirsk, Russia. Conference. Graphs and Groups, Spectra and Symmetries.* [Electronic resource]. Online: http:// math. nsc. ru/ conference/ g2/ g2s2/ exptext/SkruncovichSkuratovskii-abstract-G2S2.pdf.

[17]. А. Болотов, С. Гашков, А. Фролов, А. Часовских, "Элементарное введение в эллиптическую криптографию", М.: КомКника, 2006, 328 с.

[18]. S. Paulo, M. Barreto, M. Naehrig, "Pairing-Friendly Elliptic Curves of Prime Order", *SAC 2015: Selected Areas in Cryptography,* pp. 319-331. [Electronic resource]. Online: https://link.springer.com/chapter/10.1007/11693383_22.

[19]. О. Коссак, Я. Холявка, "ОТ-протокол з використанням еліптичної кривої Едварса", *Вісник Львівського університету. Серія прикладна математика та інформатика*, вип. 23, С. 82-88, 2015.

[20]. А. Бессалов, *Эллиптические кривые в форме Эдвардса и криптография: монография*, 2017, 272 с.

PSEUDO-RANDOM CRYPTOLOGICAL SECURITY SEQUENCES AND THE HALVING OF A POINT OF A TWISTED EDWARDS CURVE OVER PRIME AND EXTENDED FIELDS

Estimates of the complexity of the point division operation into two for twisted Edwards curve 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 cryptological security of the pseudo-random sequence generator proposed by the author is shown on the basis of a curve in the form of Edwards. A new generation scheme and a new one-sided function of a pseudo-random cryptological security sequence based on these curves are proposed. The degree of embedding of these curves into a finite field for pairing on friendly elliptic curves of prime order or almost prime order is 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. For this goal we construct friendly curves on base of family of twisted Edwards curves. The possibility of constructing a twisted Edwards order curve, that is, one that has a minimal cofactor 4, has been found. A solution for the inverse doubling problem is obtained for quasi-elliptic curves that represented in the twisted Edwards form. Also its application to the proving of cryptographic pseudo-random sequence generator. It makes it possible to prove the cryptological security of the pseudo-random sequence we developed.

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

ПСЕВДОВИПАДКОВІ КРИПТОСТІЙКІ ПОСЛІДОВНОСТІ І ПОДІЛЬНІСТЬ ТОЧКИ СКРУЧЕНОЇ КРИВОЇ ЕДВАРДСА НАВПІЛ НАД ПРОСТИМИ І СКЛАДЕНИМИ ПОЛЯМИ

Отримано оцінки складності операції ділення на два в порівнянні з подвоєнням точки скрученої кривої Едвардса. Розглянуто один з додатків властивостей подільності точки на два для визначення порядку точки в криптосистемі. Запропоновано нову схему генерування і нова одностороння функція псевдослучайной крипостійкість послідовності на основі цих кривих. Показано криптостійкість генератора псевдовипадкових послідовностей, який був запропонований автором, на основі кривої в формі Эдвардса. Показано можливість застосування даних кривих для генеруваеея криптійкої послідовності великого періода. Запропонована нова схема генерування і нова одностороння функція для псевдовипадкової криптостійкої послідовності на основі цих кривих. Досліджено ступінь занурення цих кривих в скінченне поле для спарювання на дружніх еліптичних кривих простого порядку або майже простого порядку. Останнє є дуже суттєвим в багатьох криптографічних протоколах виду короткого цифрового підпису тривалого використання. Для цієї мети ми знайшли дружні криві на основі сімейства скручених кривих Едвардса. Знайдено можливість побудови скрученої кривої порядку Едвардса, тобто такої, що має мінімальний кофактор 4. Отримано розв'язок зворотної задачі до подвоєння точки квазі-еліптичної кривої, представленої у формі скрученої кривої Едвардса. Він дає можливість обгрунтувати стійкість розробленого нами генератора псевдовипадкових криптоскійких послідовностей.

Ключові слова: скінченні поля, еліптична крива, крива Едвардса, порядок кривої, порядок точки еліптичнох кривої, символ Лежандра, квадратичний лишок, квадратичный нелишок, криві кручення.

Скуратовський Руслан Вячеславович, викладач кафедри інформаційної безпеки, МАУП, ФКІТ.
E-mail: ruslcomp@mail.ru.
Скуратовский Руслан Вячеславович, преподаватель кафедры информационной безопасности, МАУП, ФКИТ.
Skuratovskii Ruslan, lecturer, MAUP, FKIT.