

ПРОИЗВОДИТЕЛЬНОСТЬ ГРУППОВЫХ ОПЕРАЦИЙ НА СКРУЧЕННОЙ КРИВОЙ ЭДВАРДСА НАД ПРОСТЫМ ПОЛЕМ

Введение

Эллиптические кривые в форме Эдвардса над простым полем являются наиболее быстрыми и перспективными для использования в асимметричных криптосистемах. Важнейшие их преимущества: рекордная производительность, универсальность закона сложения и аффинные координаты нейтрального элемента группы. Эти свойства были обнаружены и обоснованы в работе [1].

Симметрия точек кривых Эдвардса относительно обеих координатных осей влечет за собой интересные и удобные свойства этих кривых. Исключая бесполезные изоморфные кривые, в кривых Эдвардса достаточно использовать один параметр d вместо обычных двух параметров a и b классической кривой в канонической форме.

В работе [2] авторы обобщили и расширили класс кривых Эдвардса введением нового параметра a и снятием ограничения на неквадратичность параметра d кривой. Они назвали этот класс скрученными кривыми Эдвардса. Дальнейший прогресс в изучении новых свойств этого класса скрученных кривых Эдвардса получен в работе [3], в которой найдены альтернативные формулы для закона сложения точек кривой, определены особые точки для этого закона и предложен метод расчета координат суммы точек в расширенных проективных координатах. Авторам удалось снизить число операций при сложении разных точек с $10M+2S+2U$ до $9M+1U$ (M – одно умножение в поле, S – возведение в квадрат, U – умножение на параметр кривой).

В данной работе дан критический анализ свойств скрученных кривых Эдвардса и производительности вычисления скалярного произведения точек на такой кривой. Обсуждается и обосновывается некорректность формулировки теоремы 3.2 [2] и предлагаются формулировки, обходящие особые точки кривых. Доказано, что введение нового параметра a не расширяет класс кривых и не дает новых свойств для кривой Эдвардса, а лишь замедляет вычисления. Вместе с тем, снятием ограничения на неквадратичность параметра d кривой Эдвардса можно вдвое расширить класс этих кривых. При этом нет необходимости в термине «скрученная кривая Эдвардса». Приведена сравнительная оценка производительности вычисления скалярного произведения точек кривых в форме Эдвардса и в канонической форме при выполнении операций в проективных координатах [1], и в расширенных проективных координатах [3]. Мы показываем, что полученный авторами [3] выигрыш в вычислении суммы точек практически компенсируется проигрышем при удвоении точки, в итоге общий выигрыш очень незначителен. Средний показатель выигрыша кривых Эдвардса по сравнению с кривыми в канонической форме приблизительно равен 1,5.

1. Скрученные кривые Эдвардса

В работе [2] скрученные кривые Эдвардса (twisted Edwards curves) определены как обобщение кривых Эдвардса $x^2 + y^2 = 1 + dx^2y^2$ путем ввода нового параметра a в уравнение

$$E_{E,a,d}: ax^2 + y^2 = 1 + dx^2y^2, a \neq d, a, d \in \mathbb{F}_p^*, d \neq 1, p \neq 2. \quad (1)$$

Наряду с вводом параметра a авторы сняли ограничения на пару параметров a и d , предполагая любой из них квадратичным вычетом или невычетом. Для скрученной кривой (1) нейтральный элемент группы точек $O = (0,1)$ и точка второго порядка $D = (0,-1)$ не отличаются от кривой Эдвардса. Если обратной точке $P = (x_1, y_1)$ точку определить как $-P = (-x_1, y_1)$, то универсальный закон сложения точек кривой (1) имеет вид

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_2 + x_2 y_1}{1 + d x_1 x_2 y_1 y_2}, \frac{y_1 y_2 - a x_1 x_2}{1 - d x_1 x_2 y_1 y_2} \right). \quad (2)$$

Отсюда, в частности, $P + (-P) = (0, 1) = O$. Кривая Эдвардса является частным случаем скрученной кривой (1) при $a = 1$. В работе [1] доказано (теорема 3.3), что закон сложения (2) является полным, т.е. при любых входах знаменатели в (2)

$$1 + d x_1 x_2 y_1 y_2 \neq 0, \quad 1 - d x_1 x_2 y_1 y_2 \neq 0,$$

если параметр d есть квадратичный невычет: $\left(\frac{d}{p}\right) = -1$.

Изоморфизм между кривыми в форме Монтгомери

$$E_{M,A,B}: Bv^2 = u^3 + Au^2 + u, \quad A = 2\frac{a+d}{a-d}, \quad B = \frac{4}{a-d}, \quad a = \frac{A+2}{B}, \quad d = \frac{A-2}{B}, \quad A \neq \{0, \pm 2\} \quad (3)$$

и скрученными кривыми Эдвардса (1) основан на замене координат с помощью рациональных функций

$$u = \frac{1+y}{1-y}, \quad v = \frac{u}{x} \Rightarrow \quad x = \frac{u}{v}, \quad y = \frac{u-1}{u+1}. \quad (4)$$

В работе [2] доказывается теорема 3.2: *любая скрученная кривая Эдвардса (1) бирационально эквивалентна кривой (3) в форме Монтгомери*. Нам представляется доказательство этой теоремы в общем случае некорректным.

В этом разделе мы даем анализ всевозможных четырех выборов вычет-невычет для пар параметров a и d кривой (1) и обосновываем некорректность утверждения теоремы 3.2 [2].

1. Пусть $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = -1$. Согласно (1) и (2) в этом случае на кривой (1) имеется единственная точка $D = (0, 1)$ второго порядка и две точки 4-го порядка $\pm F = (\pm 1/\sqrt{a}, 0)$. В соответствии с (4) им отвечают точки кривой Монтгомери (3) $D_M = (0, 0)$ и $\pm F_M = (1, \pm\sqrt{a})$. Это наиболее прозрачный случай, при котором заменой $(x, y) \rightarrow (X/\sqrt{a}, Y)$ получаем изоморфную кривой (1) кривую Эдвардса $X^2 + Y^2 = 1 + d'X^2Y^2$, $d' = d/a \Rightarrow \left(\frac{d'}{p}\right) = -1$. Этот изоморфизм делает бесполезным введение избыточного параметра a , лишь тормозящего вычисления.

2. Пусть $\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = 1$. Здесь также нет неожиданностей, так как параметры a и d просто меняются местами. С помощью замены $(x, y) \rightarrow (X, 1/Y)$ можно получить скрученную кривую $dX^2 + Y^2 = 1 + aX^2Y^2$ или, как и в п.1, изоморфную ей кривую Эдвардса $\bar{x}^2 + \bar{y}^2 = 1 + \left(\frac{a}{d}\right)\bar{x}^2\bar{y}^2$. Так как переход от параметра d к обращенному параметру d^{-1} дает кривую кручения [1, 4, 7], пара кривых в п.1 и п.2 образует пару кривых кручения.

3. Пусть $\left(\frac{a}{p}\right) = -1, \left(\frac{d}{p}\right) = -1$. Согласно (3) имеем $(Bad)^2 = (A+2)(A-2)$ и, следовательно, дискриминант квадратного уравнения в правой части (3) $(A^2 - 4)$ является квадратом. Кубическое уравнение $u^3 + Au^2 + u = 0$ имеет три корня в поле F_p : $\{0, -(A \pm \sqrt{A^2 - 4})/2\}$, а кривая Монтгомери содержит три точки 2-го порядка: $D_{M1} = (0, 0)$, $D_{M2,3} = (-(A \pm \sqrt{A^2 - 4})/2, 0)$, с координатами $v_{1,2,3} = 0$. Преобразованием координат (4) точка D_{M1} кривой (3) переходит в точку $D = (0, -1)$ кривой (1), а две другие точки $D_{M2,3}$ трансформируются в две точки 2-го порядка с y -координатами $(\pm\sqrt{A^2 - 4} - A - 2)/(\pm\sqrt{A^2 - 4} - A + 2)$ и с делением на 0 x -координаты $x = u/v$. Так как при $y = 0$ из (1) следует $ax^2 = 1$, решения для x -координаты нет и точки 4-го порядка для этого случая не существуют. Итак, этот случай характеризуется двумя особыми точками 2-го порядка (две точки на бесконечности) и отсутствием точек 4-го порядка.

4. Пусть $\left(\frac{a}{p}\right) = 1, \left(\frac{d}{p}\right) = 1$. Как и в предыдущем случае, дискриминант уравнения (3) $(A^2 - 4) = (Bad)^2$ является квадратом, и вновь имеем три точки 2-го порядка с теми же координатами.

натами, что и в п.3. Две из них преобразованием (4) переходят в особые точки 2-го порядка кривой Эдвардса. В отличие от п.3 здесь появляются также точки 4-го порядка, в частности точки $\pm F = (\pm 1/\sqrt{a}, 0)$ кривой (1). Кроме того, кривая Монтгомери (3) содержит две точки 4-го порядка с координатой $u_1 = -1$, которые отображением (4) порождают особые точки кривой Эдвардса (1). Действительно, из уравнения касательной к кривой (3) в точке 4-го порядка $P_M = (u_1, v_1)$, проходящей через точку $(0,0)$ 2-го порядка, имеем

$$\left. \frac{dv}{du} \right|_{u=u_1} = \frac{3u_1^2 + 2Au_1 + 1}{2Bv_1} = \frac{v_1}{u_1}.$$

Тогда с учетом (3) получим $u_1^2 = 1 \Rightarrow u_1 = \pm 1$. Одна из пар точек 4-го порядка имеет координаты $\pm F_M = (-1, \pm \sqrt{(A-2)/B})$. Как следует из (4), эти две точки кривой Монтгомери с координатой $u_1 = -1$ преобразуются в особые точки 4-го порядка кривой (1) с x -координатами $(\pm \sqrt{(A-2)/B})$, и с делением на 0 y -координаты $y = (u_1 - 1)/(u_1 + 1)$. В итоге в рассматриваемом случае получили четыре особые точки (на бесконечности): по две точки 2-го и 4-го порядков. Как и в п.3, в этом случае нарушается полнота закона сложения (2) [1].

Так как групповая операция (2) для скрученной кривой Эдвардса (1) определена в конечном поле F_p , в котором нет деления на 0, то для бесконечно удаленных точек 2-го и 4-го порядков в случаях п.3 и 4 групповая операция не определена. Следовательно, при существовании группы точек $E_{M,A,B}$ группа точек $E_{E,a,d}$ в рассматриваемых случаях в целом не существует, а утверждение теоремы 3.2 [2] следует признать некорректным. Так как эта теорема справедлива для всех точек в условиях п.1 и 2 и локально справедлива для подгрупп нечетных порядков в условиях п.3 и 4, мы предлагаем ее формулировку в следующих двух теоремах:

Теорема 1. При $\left(\frac{ad}{p}\right) = -1$ любая скрученная кривая Эдвардса (1) изоморфна кривой (3) в форме Монтгомери.

Теорема 2. При $\left(\frac{ad}{p}\right) = 1$ любая подгруппа скрученной кривой Эдвардса (1) нечетного порядка изоморфна соответствующей подгруппе кривой (3) в форме Монтгомери.

Их доказательство можно провести аналогично [2] с учетом ограничений, исключающих особые точки скрученной кривой Эдвардса (1), рассмотренные в случаях п.3 и 4.

Обращаясь к примеру кривой $E_{M,9,1} : v^2 = u^3 + 9u^2 + u, p = 17$, приведенному в [2] и отвечающему согласно (3) условиям п.3, получаем уравнение скрученной кривой $E_{E,11,7} : 11x^2 + y^2 = 1 + 7x^2y^2$ (здесь параметры $a = 11$ и $d = 7$ являются квадратичными невычетами по модулю 17). Кривая Монтгомери $v^2 = u(u+3)(u+6)$ имеет порядок 20, содержит три точки 2-го порядка и не имеет точек 4-го порядка. Она является нециклической и представляется прямой суммой циклических подгрупп 2-го и 10-го порядков. Ясно, что она содержит две различные подгруппы простого порядка 5 (всего имеется восемь точек 5-го и восемь точек 10-го порядков). Если уравнение $E_{E,11,7}$ записать как $x^2 = (y^2 - 1)/(7y^2 - 11)$, то и числитель, и знаменатель обращаются в ноль при соответственно $y^2 = 1$ и $y^2 = 4$. Особые точки для координаты x возникают при $y = \pm 2$. Согласно (4) $y = (u-1)/(u+1)$, и эти значения отвечают корням $u_{2,3} \in \{-3, -6\}$ кубического уравнения в $E_{M,9,1}$, т.е. особым точкам 2-го порядка $D_{2,3} = (\infty, \pm 2)$. Для этих точек операция (2) не определена и нельзя построить всю группу точек $E_{E,11,7}$, ни даже подгруппы точек, включающие эти особые точки. Вместе с тем, закон сложения (2) будет работать для подгрупп, не включающих особые точки. Например, примем $P = (1, 8)$, тогда $2P = (-5, 3)$, $4P = (6, -4)$, $8P = (5, 3)$. Так как $8P = -2P$, то $10P = O$ и $\text{Ord} P = 10$. Но в подгруппу $\langle P \rangle$ входит особая точка 2-го порядка $5P = 4P + P = (\infty, 2)$, операция с которой не определена. Однако, приняв генератором подгруппы 5-го порядка

точку $G = 2P$, можно в подгруппе точек $\langle G \rangle$, не включающей особых точек, пользоваться групповой операцией (2). Этот же вывод справедлив для случая п. 4 для всех подгрупп, порядок которых не кратен 2 и 4. Можно утверждать, что такие подгруппы для кривых Монтгомери и скрученной кривой Эдвардса изоморфны при любом выборе пары a и d , $a \neq d$.

Как видим, с конструктивной точки зрения нельзя исключать применение в криптографии, в которой используются подгруппы $\langle G \rangle$ простого порядка n , любые выборы вычет-невычет для пары параметров a и d . Это вдвое расширяет множество всех кривых Эдвардса.

Заметим, что введение нового параметра a в определение скрученной кривой Эдвардса практически не дает новых полезных свойств и не расширяет множество кривых Эдвардса, так как эти кривые изоморфны. Более того, в групповой операции появляется дополнительная операция умножения на a , что лишь замедляет вычисления. Расширение вдвое множества всех приемлемых кривых Эдвардса ($a = 1$) можно осуществить снятием ограничения с параметра d как квадратичного невычета, но с корректной арифметикой при четных d лишь в подгруппах $\langle G \rangle$ точек нечетных порядков. Далее обсудим возможность повышения производительности групповой операции.

2. Производительность групповой операции на скрученной кривой Эдвардса

Авторы [3], изыскивая возможности ускорения групповых операций на скрученных кривых Эдвардса, нашли интересный резерв для решения этой задачи. Выразив параметры a и d через координаты складываемых точек, они получили альтернативные формулы для законов сложения, в частности

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1 y_1 + x_2 y_2}{y_1 y_2 + a x_1 x_2}, \frac{x_1 y_1 - x_2 y_2}{x_1 y_2 - x_2 y_1} \right) = (x_3, y_3). \quad (5)$$

Хотя модифицированный закон (5) уже в общем случае не является полным (существуют особые точки, обращающие знаменатели в 0), для точек нечетного порядка особых точек нет и формула (5) вполне конструктивна. Обсудим этот вопрос в разд. 3.

Вводя расширенные проективные координаты $(X:Y:T:Z)$, авторам [3] удалось сократить число полевых операций при сложении двух разных точек до $9M + 1U$ (M – умножение в поле, S – возведение в квадрат, U – умножение на параметр кривой) в сравнении со сложностью $10M + 1S + 2U$ при реализации сложения по формуле (2) [1]. Рассмотрим их метод.

При $Z \neq 0$ зададим четырехмерные проективные координаты $(X:Y:T:Z)$ подстановкой в (5) $x = X/Z$, $y = Y/Z$, $t = xy/Z$, $T = XY/Z$. Тогда

$$\frac{x_3}{z_3} = \frac{(t_1 z_2 + z_1 t_2)}{(y_1 y_2 + a x_1 x_2)}, \quad \frac{y_3}{z_3} = \frac{(t_1 z_2 - z_1 t_2)}{(x_1 y_2 - y_1 x_2)}$$

Отсюда

$$\begin{aligned} X_3 &= (X_1 Y_2 - Y_1 X_2)((T_1 Z_2 + Z_1 T_2), \\ Y_3 &= (Y_1 Y_2 + a X_1 X_2)((T_1 Z_2 - Z_1 T_2), \\ T_3 &= (T_1 Z_2 + Z_1 T_2)((T_1 Z_2 - Z_1 T_2), \\ Z_3 &= (Y_1 Y_2 + a X_1 X_2)((X_1 Y_2 - Y_1 X_2). \end{aligned} \quad (6)$$

Пусть $A = X_1 X_2$, $B = Y_1 Y_2$, $C = T_1 Z_2$, $D = Z_1 T_2$, $E = C + D$, $F = C - D$,

$G = B + aA$, $H = (X_1 - Y_1)(X_2 + Y_2) - A + B \Rightarrow$

$X_3 = EH$, $Y_3 = GF$, $T_3 = EF$, $Z_3 = GH$.

Мы видим, что сложность групповой операции сложения разных точек составляет $V_{ED} = 9M + 1U$. Если параметр $a = \pm 1$ или мал, сложность оценивается как $9M$. При удвоении точки кривой Эдвардса в трехмерных проективных координатах сложность минимальна и составляет $W_{ED} = 3M + 4S + 1U$ [1]. В работе [3] в расширенных проективных координатах сложность удвоения возрастает на одну операцию $W_{ED} = 4M + 4S + 1U$.

Оценим выигрыш в производительности при вычислении скалярного произведения на скрученной кривой Эдвардса в расширенных проективных координатах по сравнению с аналогичной процедурой на канонической кривой в проективных координатах.

Расчет числа операций при вычислении суммы точек канонической кривой E дает сложность $V_E = 12M + 2S$. Аналогичный расчет для удвоения точек приводит к результату $W_E = 7M + 5S$ [6].

Принимая вычислительную сложность возведения в квадрат $1S = 0.67M$, а умножения на параметр кривой $1U = 0.5M$, получим оценки сложности сложения и удвоения на кривой Эдвардса $V_{ED} = 9.5M$, $W_{ED} = 4M + 4S + 1U = 7.17M$. Удвоение, как видим, значительно быстрее сложения. Для канонической эллиптической кривой имеем $V_E = 13.33M$, $W_E = 10.35M$.

При вычислении скалярного произведения rQ точки Q число r представляется в двоичной форме, тогда работает алгоритм последовательного сложения-удвоения, а приведенный результат для γ справедлив при равновероятных 0 и 1 в числе r . Пусть v – относительная частота знаков 1 в двоичной последовательности r ; тогда в общей форме выигрыш

$$\gamma = \frac{W_E + vV_E}{W_{ED} + vV_{ED}}. \quad (7)$$

В среднем при равновероятных 0 и 1 в двоичной записи числа r ($v \rightarrow 0.5$) получаем среднее значение выигрыша $\bar{\gamma} = 1.426$. Если использовать кривые Эдвардса с параметром $a = \pm 1$, то $V_{ED} = 9M$, $W_{ED} = 6.67M$ и средний выигрыш достигает значения $\bar{\gamma} = 1.521$.

В работе [5] была проведена сравнительная оценка быстродействия операций на кривой Эдвардса ($a = 1$) с результатами, полученными в [1] на основе закона сложения (2) в проективных координатах $(X:Y:Z)$, и канонической кривой. В [1] сложность сложения точек $V_{ED} = 10M + 1S + 1U \approx 11.17M$ несколько выше, чем в [3], зато сложность удвоения точек $W_{ED} = 3M + 4S = 5.67M$ меньше на одну операцию умножения. В итоге по формуле (7) при $a = 1$ получаем среднее значение выигрыша $\bar{\gamma} = 1.51$.

Итак, использование закона сложения (5) и расширенных проективных координат дает весьма незначительный прирост производительности вычислений на кривой Эдвардса по сравнению с полным универсальным законом сложения (2). Вместе с тем, по сравнению с каноническими кривыми обе арифметики дают прирост быстродействия приблизительно в 1,5 раза.

Если использовать вместо двоичного представления числа k произведения kP троичное NAF(k) $k_i \in \{0, 1, -1\}$ [6], то можно снизить среднее число ненулевых компонент в числе k до $1/3$. По формуле (7) при $v = 1/3$ это даст максимальное значение среднего выигрыша $\bar{\gamma} = 1.531$.

3. Особые точки модифицированного закона сложения

Из формулы (5) для y -координаты видно, что при удвоении точки знаменатель обращается в 0. Поэтому при удвоении точки следует пользоваться законом (2). Но и при сложении разных точек возникают особые пары точек, обращающие знаменатели x -координаты и y -координаты в ноль. В [3] доказана теорема:

Теорема 3. Пусть имеем скрученную кривую Эдвардса $E_{E,a,d}$ (1). Для фиксированной точки кривой $P = (x_1, y_1)$ найдется такая точка $Q = (x_2, y_2)$, для которой:

1) $y_1y_2 + ax_1x_2 = 0$ тогда и только тогда, когда $Q \in S_x$, где

$$S_x = \left\{ \left(\frac{y_1}{\sqrt{a}}, -x_1\sqrt{a} \right), \left(-\frac{y_1}{\sqrt{a}}, x_1\sqrt{a} \right), \left(\frac{1}{x_1\sqrt{ad}}, -\frac{\sqrt{a}}{y_1\sqrt{d}} \right), \left(\frac{-1}{x_1\sqrt{ad}}, \frac{\sqrt{a}}{y_1\sqrt{d}} \right) \right\};$$

2) $x_1y_2 - y_1x_2 = 0$ тогда и только тогда, когда $Q \in S_y$, где

$$S_y = \left\{ (x_1, y_1), (-x_1, -y_1), \left(\frac{1}{y_1\sqrt{d}}, \frac{1}{x_1\sqrt{d}} \right), \left(\frac{-1}{y_1\sqrt{d}}, \frac{-1}{x_1\sqrt{d}} \right) \right\}.$$

Рассмотрим наиболее распространенный случай $\left(\frac{a}{p}\right) = 1$, $\left(\frac{d}{p}\right) = -1$. Тогда в каждом из множеств S_x, S_y остается по две первых точки. Их координаты для множества S_x определяются как $Q = P \pm F$, где $\pm F = (\pm \frac{1}{\sqrt{a}}, 0)$ – точки 4-го порядка. Тогда здесь возникает особенность при $Q + P = 2P \pm F$. Координаты точек для множества S_x определяются как $Q = P$ и $Q = P + D$, где $D = (0, 1)$ – точка 2-го порядка. Здесь особенность возникает при $Q + P = 2P$ и при $Q + P = 2P + D$. Мы видим, что все особые случаи порождаются удвоением точки P с возможным суммированием с ним точек 4-го или 2-го порядков.

Если P – точка нечетного порядка n , то $\text{Ord}(2P) = n$, так как $n2P = O$. Отсюда следует, что $\text{Ord}(2P \pm F) = 4n$ и $\text{Ord}(2P + D) = 2n$. Другими словами, особенности в рассматриваемом случае могут возникать лишь при сложении разных точек четных порядков (мы исключаем удвоение для закона (5)). При вычислении скалярного произведения kP при больших значениях k для каждой точки P большого порядка (возможно четного) может существовать всего три точки Q таких, что сумма $Q + P$ не определена, а вероятность такого события ничтожна. В криптосистеме с генератором G простого порядка n суммирование любых разных точек из группы $\langle G \rangle$ с помощью формулы (5) особенностей не порождает. Это всегда справедливо для всех точек нечетного порядка (см. **Теорема 2**).

В заключение заметим, что обобщение кривых Эдвардса с помощью скрученных кривых Эдвардса можно считать конструктивным лишь в плане снятия ограничения с параметра d (он может быть квадратичным вычетом и невычетом), а параметр a является избыточным (в силу изоморфизма) и лишь замедляет вычисления. Модифицированный закон сложения (5) полезен при сложении разных точек нечетного порядка и дает очень незначительный выигрыш в быстродействии при расчете скалярного произведения. По сравнению с канонической формой эллиптической кривой быстродействие операций на кривой Эдвардса возрастает приблизительно в 1,5 раза.

Список литературы: 1. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves // IST Programme under Contract IST-2002-507932 ECRYPT, 2007. – Pp. 1–20. 2. 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, 2008. – Pp. 1–17. 3. Hisil Huseyin, Koon-Ho Wong Kenneth, Carter Gary, and Dawson Ed. Twisted Edwards Curves Revisited. ASIACRYPT 2008, LNCS 5350. – Pp. 326 – 343. 4. Бессалов А.В. Число изоморфизмов и пар кручения кривых Эдвардса над простым полем // Радиотехника. – 2011. – Вып. 167. – С. 203 – 208. 5. Бессалов А.В., Дихтенко А.А., Третьяков Д.Б. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем // Сучасний захист інформації. – 2011. – №4. – С.33 – 36. 6. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых : учеб. пособие. – К. : ІВЦ «Політехніка», 2004. – 224с. 7. Бессалов А.В. Построение кривой Эдвардса на базе изоморфной эллиптической кривой в канонической форме // Прикладная радиоэлектроника. – 2014. – Т. 13, №3. – С.286 – 289.

Национальный технический университет «КПИ»

Поступила в редколлегию 12.04.2015