УДК 004.051/056 DOI: 10.30748/soi.2017.151.17

М.Г. Ковтун

Национальный авиационный университет, Киев

ПРИМЕНЕНИЕ КРИВЫХ ЭДВАРДСА ДЛЯ ЗАЩИЩЕННОЙ РЕАЛИЗАЦИИ МЕХАНИЗМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ СОГЛАСНО ДСТУ 4145-2002

Рассматривается повышение быстродействия криптографических преобразований при формировании и проверки ЭЦП согласно ДСТУ 4145-2002, за счет использования бирационально эквивалентных кривых Эдвардса над двоичным полем, при выполнении промежуточных преобразований в скалярном умножении.

В работе анализируется операция скалярного умножения на двоичных эллиптических кривых Вейерштрасса из ДСТУ 4145-2002, а также на бирационально эквивалентных им кривых Эдвардса для случая $d_1 \neq d_2$ *и* $d_1 = d_2$. *Сравнивается производительность для кривых Эдвардса для общего случая* $d_1 \neq d_2$ *и* $d_1 = d_2$, *а также производительность выполнения операции, при* d_1, *которое не превышает 64 бита. В результате исследований удалось выяснить, что производительность операции скалярного умножения на кривых Вейерштрасса из ДСТУ 4145-2002 показала лучшее время, нежели на кривых Эдвардса в общем случае* $d_1 \neq d_2$. *Однако, время реализации операции скалярного умножения на двоичных кривых Эдвардса, с условием* $d_1 = d_2$, *в 1.3 раза быстрее для кривых Вейерштрасса, начиная с базового поля* $GF\left(2^{257}\right)$. *Дальнейшие исследования будут посвящены поиску двоичных кривых Эдвардса с* $d_1 = d_2$ *для полей из ДСТУ 4145-2002, что позволит повысить эффективность национальной системы ЭЦП.*

***Ключевые слова**: эллиптические кривые, двоичные кривые Эдвардса, двоичные кривые Вейерштрасса, ЭЦП, ДСТУ 4145-2002, скалярное умножение, лестница Монтгомери.*

Введение

Современное общество переходит к информационной эре, где информация является важной составляющей, и ее объёмы растут с каждым днем. Для массовой автоматизации, необходимо предоставить информационным процессам юридическую значимость, что послужило принятием Закона Украины «Об электронной цифровой подписи» [1] и «Об электронных документах и электронном документообороте» [2]. Процедура формирования и проверки электронной цифровой подписи (ЭЦП) выполняется согласно государственному стандарту ДСТУ 4145-2002 [3].

С целью интеграции Украины в международное сообщество был гармонизирован целый ряд международных стандартов в области криптографии и доверительных услуг.

При формировании и проверке ЭЦП, согласно ДСТУ 4145-2002, используется две операции: это хеширование и скалярное умножение (СУ) точки эллиптической кривой (ЭК) в форме Вейерштрасса. СУ является наиболее важной и в то же время самой трудоемкой, с вычислительной точки зрения, операцией на ЭК. Для авторов интерес представляет именно СУ, а точнее сокращение времени выполнения этой операции, поскольку именно она влияет на время вычисления и проверки ЭЦП, в целом.

Известно множество алгоритмов СУ точки ЭК [8-9;11;15-23]. Среди них выделяют так называемую лестницу Монтгомери, которая устойчива к атакам по побочным каналам (класс атак, направленный на выявление и эксплуатацию уязвимостей в практической реализации криптосистемы), также она является достаточно быстрой [18-19]. Противодействие к уязвимостям по побочным каналам связано с тем, что на каждом шаге лестницы, независимо от текущего обработанного бита скаляра k, выполняется операция удвоения точки, а также операция сложения точки, и изменяется только порядок их выполнения. Лестница Монтгомери широко используется в аппаратных реализациях криптосистем. В контексте программных реализаций противодействие побочным каналам не менее важно.

В ДСТУ 4145-2002 представлены стандартизированные (именованные) ЭК в форме Вейерштрасса. Авторы [8; 14] описали возможность перехода к другому представлению – кривым Эдвардса, которые обладают желаемыми криптографическими свойства и преимуществами [8; 14; 19]:

- групповой закон для кривых Эдвардса – полный и унифицирован;
- более безопасные реализации к атакам по сторонним каналам;
- имеют эффективное сложение и удвоение точек;

- закон сложения точек для кривых Эдварда линеен с точки зрения выполнения операций процессором, т.к. позволяет исключить различные проверки, присущие при сложении точек ЭК в форме Вейерштрасса (например формула сложения идентична для P и P, а также P и $-P$);
- каждая ЭК в форме Вейерштрасса над двоичным полем имеет бирационально эквивалентную кривую Эдвардса E_{B,d_1,d_2} для $m \geq 3$.

Все вышеперечисленное позволяет кривым Эдвардса обеспечивать лучшую платформу для построения криптографических примитивов.

Актуальная научно-техническая задача, решаемая в работе, состоит повышении быстродействия криптографических преобразований при формировании и проверке ЭЦП согласно ДСТУ 4145-2002, за счет использования бирационально эквивалентных кривых Эдвардса над двоичным полем, при выполнении промежуточных преобразований в СУ.

Основная часть

Кривую Вейерштрасса для $GF\left(2^m\right)$ можно записать следующим образом [4; 8-9].

$$E_{W,a,b} : v^2 + uv = u^3 + a \cdot u^2 + b. \qquad (1)$$

При реализации СУ существует ряд неопределенностей: к примеру, сложение $P+Q$ точек невозможно, если:

- точка P является точкой на бесконечности;
- точка Q находится на бесконечности;
- результат $P+Q$ принадлежит бесконечности;
- выполняется условие $P = Q$.

Каждый из описанных случаев должен быть проверен и анализироваться отдельно, что требует дополнительных операций процессора. Алгоритм «полного» сложения получается путем «склеивания» нескольких формул сложения для частных случаев.

В работе [8] описывается переход от кривых Вейерштрасса к кривым Эдвардса, для которых выполняется полнота группового закона и кривые являются унифицированными, что не требует выявлять частные случаи.

Определение 1. Пускай $k = 2$ является характеристикой поля, d_1, d_2 – элементы поля k, такие что $d_1 \neq 0$ и $d_2 \neq d_1^2 + d_1$. Тогда двоичная кривая Эдвардса с коэффициентами d_1 и d_2 в аффинном представлении имеет вид [8]:

$$E_{B,d_1,d_2} : d_1(x+y) + d_2\left(x^2+y^2\right) = \\ = xy + xy(x+y) + x^2y^2. \qquad (2)$$

Каждая кривая (2) является не суперсингулярной, что позволяет противостоять схемам ЭЦП целому ряду атак.

Для двоичной кривой Эдвардса в аффинном представлении существует две точки, которые лежат на бесконечности (1:0) и (0:1).

В проективных координатах, кривую Эдвардса (2) можно записать [6; 8–9; 19]:

$$d_1(X+Y)Z^3 + d_2\left(X^2+Y^2\right)Z^2 = \\ = XYZ^2 + XY(X+Y)Z + X^2Y^2. \qquad (3)$$

В этом случае точки на бесконечности: (1:0:0) и (0:1:0).

В работах [4; 8-9] показано, что каждая кривая Вейерштрасса (1) бирационально эквивалентна двоичной кривой Эдвардса (2) при $d_1 \neq d_2$:

$$v^2 + uv = u^3 + \left(d_1^2 + d_2\right)u^2 + d_1^4\left(d_1^4 + d_1^2 + d_2^2\right). \qquad (4)$$

Бирационально эквивалентное преобразование кривой (4), при условии, что $b \neq 0$ и $d_1 \neq d_2$, осуществляется за счет преобразования [4; 8-10]:

$$u = d_1\left(d_1^2 + d_1 + d_2\right)(x+y)\Big/\left(xy + d_1(x+y)\right)$$

$$v = d_1\left(d_1^2 + d_1 + d_2\right)(x)\Big/\left(xy + d_1(x+y) + d_1 + 1\right).$$

Обратное отображение для $d_1 \neq d_2$ имеет следующий вид:

$$x = \frac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{u + v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)};$$

$$y = \frac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)}.$$

Определение 2. Пускай k – поле с характеристикой 2, d_1, d_2 – элементы поля, для которых $d_1 \neq 0$. Предположим, что ни один элемент $t \in k$ не удовлетворяет условию $t^2 + t + d_2 = 0$. Полная двоичная кривая Эдвардса с коэффициентами d_1 и d_2 в аффинном представлении имеет вид (2) [8].

Полная двоичная кривая Эдвардса, такая же, как и обычная двоичная кривая Эдвардса, но для нее выдвигается дополнительное требование $t^2 + t + d_2 \neq 0$ для всех $t \in k$, даже для $t = d_1$. Это возможно при условии, что $\mathrm{Tr}(d_2) = 1$.

Теорема 1. Пускай m – целое, с условием, что $m \geq 3$. Каждая обычная ЭК над $GF\left(2^m\right)$ является бирационально эквивалентной к полной кривой Эдвардса [8].

Алгоритм бирационально эквивалентного преобразования и доказательство теоремы для $d_1 \neq d_2$, представлены в работах [4; 8; 10].

Для двоичной кривой Эдвардса когда $d_1 = d_2$, в работе [10] описаны условия для бирационального эквивалентного преобразования кривой Вейерштрасса (1) к полной кривой Эдвардса E_{B,d_1,d_1}, при условии, что $\mathrm{Tr}(b) = 1 = \mathrm{Tr}(d_1)$ и с изоморфизмом $v \to v + d_1 u$:

$$v^2 + uv = u^3 + \left(d_1^2 + d_1\right)u^2 + d_1^8. \qquad (5)$$

Сама же кривая Эдвардса имеет вид [10]:

$$d_1\left(x + x^2 + y + y^2\right) = \left(x + x^2\right)\left(y + y^2\right). \qquad (6)$$

Преобразования точки из кривой $E_{W,d_1^2+d_1,b}$ в E_{B,d_1,d_1} и наоборот осуществляются [10]:

$$(x,y) \to (u,v) = \left(\frac{d_1^3(x+y)}{xy + d_1(x+y)}; \frac{d_1^3 x}{\left(xy + d_1(x+y)\right) + d_1 + 1}\right);$$

$$(u,v) \to (x,y) = \left(\frac{d_1\left(u + d_1^2\right)}{u + v + \left(d_1^2 + d_1\right)d_1^2}; \frac{d_1\left(u + d_1^2\right)}{v + \left(d_1^2 + d_1\right)d_1^2}\right).$$

В табл. 1 представлена вычислительная сложность арифметических операций на двоичных кривых Вейерштрасса и бирационально эквивалентным им кривым Эдвардса (БЭК). Из табл. 1 видно, что кривые Эдвардса проигрывают по количеству арифметических операций кривым Вейерштрасса, но не стоит забывать, что для кривых Эдвардса можно опустить операции ветвления (проверок), сравнивая точки перед операцией сложения и удвоения.

Таблица 1

Вычислительная сложность арифметических операций на кривых Вейерштрасса и Эдвардса

Координаты	Условие	Кривые Вейерштрасса	БЭК Эдвардса	
			$d_1 \neq d_2$	$d_1 = d_2$
Сложение точек				
Аффинные		**I**+3**M**+**S**	**I**+10**M**+**D**+4**S**	**I**+10**M**+**D**+4**S**
Проективные	$Z_2 = 1$		13**M**+3**S**+3**D**	13**M**+3**S**+3**D**
Лопес-Дахаб	$Z_2 = 1, a = 1$	8**M**+4**S**+**D**		
Лопес-Дахаб	$Z_2 = 1, a = 0$	8**M**+5**S**+**D**		
Проективное			17**M**+3**S**+6**D**	15**M**+2**S**+4**D**
Лопес-Дахаб	$a = 1$	13**M**+4**S**		
Лопес-Дахаб	$a = 0$	13**M**+4**S**		
Проективные	$Z_2 = Z_1 = 1$		12**M**+3**S**+**D**	12**M**+3**S**+**D**
Лопес-Дахаб	$Z_2 = Z_1 = 1, a = 1$	5**M**+3**S**+**D**		
Лопес-Дахаб	$Z_2 = Z_1 = 1, a = 0$	5**M**+3**S**+**D**		
Удвоение точек				
Аффинные		**I**+3**M**+**S**+**D**	**I**+2**M**+4**D**+2**S**	**I**+**M**+4**D**+2**S**
Проективные			2**M**+3**D**+6**S**	2**M**+2**D**+6**S**
Лопес-Дахаб	$a = 1$	3**M**+5**S**+**D**		
Лопес-Дахаб	$a = 0$	3**M**+5**S**+**D**		
Монтгомери (проективные w-координаты)			6**M**+4**D**+4**S**	5**M**+2**D**+4**S**
Монтгомери (Лопес-Дахаб)		6**M**+4**S**		

Рассматривая быструю реализацию алгоритма Монтгомери, для него применяют дифференциальные формулы сложения и удвоения, которые оперируют только одной координатой точки. Под дифференциальным сложением подразумевается вычисление $Q + P$ с учетом Q, P, $Q - P$: например, вычисление $(2m+1)P$, при условии $(m+1)P$, mP, P или вычисление $2mP$, при условии mP, P, $0P$. В частности, «w-координатное дифференциальное сложение» подразумевает вычисление $w(Q+P)$ при $w(Q)$, $w(P)$, $w(Q-P)$ [8-9; 11].

Алгоритм 1 представляет СУ методом Монтгомери в аффинном и проективном представлении [12].

Алгоритм 1. Скалярное умножение точки методом Монтгомери

Вход: $P = (x_0, y_0) \in GF\left(2^m\right)$, $k = (k_{l-1}, \cdots, k_1, k_0)_2$.

Выход: $Q = kP \in GF\left(2^m\right)$.

1. $A \leftarrow P$, $B \leftarrow 2P$.
2. for $i - 1$ down to 0 do
2.1 if $k_i = 0$ then
2.1.1. $A \leftarrow 2A$, $B \leftarrow A + B$.

2.2. else
2.2.1. $A \leftarrow A + B$, $B \leftarrow 2B$.
3. return $Q \leftarrow A$.

Ниже представлен Алгоритм 2, который использует w -координатное дифференциальное сложение и удвоение, где DiffDBL – дифференциальное удвоение, а MDiffAdd – смешенное дифференциальное сложение [11].

Алгоритм 2. Алгоритм Монтгомери для СУ с использованием w -координат

Вход: $P = (x_0, y_0) \in GF(2^m)$, $k = (k_{l-1}, \cdots, k_1, k_0)_2$.

Выход: $w(Q) = w(kP) \in GF(2^m)$.

1. $w_0 \leftarrow x_0 + y_0$.
1.1. $W_1 \leftarrow w_0$, $Z_1 \leftarrow 1$.
1.2. $(W_2, Z_2) \leftarrow \mathrm{DiffDBL}(W_1, Z_1)$.
2. for $l-2$ down to 0 do
2.1. if $k_i = 1$ then
2.1.1. $(W_1, Z_1) \leftarrow \mathrm{MDiffAdd}(W_1, Z_1, W_2, Z_2, w_0)$.
2.1.2. $(W_2, Z_2) \leftarrow \mathrm{DiffDBL}(W_2, Z_2)$.
2.2. else
2.2.1. $(W_1, Z_1) \leftarrow \mathrm{DiffDBL}(W_1, Z_1)$.
2.2.2. $(W_2, Z_2) \leftarrow \mathrm{MDiffAdd}(W_1, Z_1, W_2, Z_2, w_0)$.
3. return $w(kP) \leftarrow (W_1, Z_1)$ и $w((k+1)P) \leftarrow (W_2, Z_2)$.

После получения результата $w_2 = w(kP)$ и $w_3 = w((k+1)P)$, необходимо осуществить преобразования точки в аффинный вид $Q = (x_2, y_2) = kP$. Для этого следует воспользоваться формулой [8; 11]:

$$x_2^2 + x_2 = \frac{w_3\left(d_1 + w_0 w_2 (1 + w_0 + w_2) + {}^{d_2}\!/_{d_1}\, w_0^2 w_2^2\right)}{w_0^2 + w_0} + \frac{d_1(w_0 + w_2) + \left(y_1^2 + y_1\right)\left(w_2^2 + w_2\right)}{w_0^2 + w_0}.$$

Чтобы найти x_2, решается квадратное уравнение, представленное выше. Для нахождения y_2 при условии, что $d_1 \neq d_2$, следует подставить значение x_2 в уравнение кривой (2). После чего получается результат:

$$y_2^2 + y_2 \cdot \left(\frac{d_1 + x_2 + x_2^2}{d_2 + x_2 + x_2^2}\right) + \frac{d_1 \cdot x_2 + d_2 \cdot x_2^2}{d_2 + x_2 + x_2^2} = 0.$$

Сделав замену $z = y_2 \cdot \left(\frac{d_2 + x_2 + x_2^2}{d_1 + x_2 + x_2^2}\right)$, следует решить квадратное уравнение (7) относительно z:

$$z^2 + z = \frac{\left(d_1 \cdot x_2 + d_2 \cdot x_2^2\right)\left(d_2 + x_2 + x_2^2\right)}{\left(d_1 + x_2 + x_2^2\right)^2}. \qquad (7)$$

После нахождения z, результирующий $y_2 = z \cdot \frac{\left(d_1 + x_2 + x_2^2\right)}{\left(d_2 + x_2 + x_2^2\right)}$.

Если используется кривая, где коэффициенты равны $d_1 = d_2$, тогда, решив квадратное уравнение (8), в результате получаем y_2:

$$y_2^2 + y_2 = \frac{d_1\left(x_2 + x_2^2\right)}{d_1 + x_2 + x_2^2}. \qquad (8)$$

Таблица 2

Сравнение производительности реализации операции СУ в проективных координатах

Поле (m)	Время реализации СУ в мс				
	Вейерштрасс ДСТУ4145-2202		ДСТУ4145-2202		
			Эдвардс $d_1 \neq d_2$	Эдвардс при $d_1 = d_2$	Эдвардс при $d_1 = d_2$
	Алгоритм Монтгомери (проективные координаты Лопеса-Дахаба)	Бинарный алгоритм (смешанные координаты Лопеса-Дахаба)	Алгоритм Монтгомери (проективные w -координаты)		
163	0,2065	0,2228	0,3279		
167	0,209	0,3796	0,3335		
173	0,2293	0,2414	0,3733	0,2752	
173***	0,228	0,2472	0,3705	0,2736	
173#	0,2751	0,2906	0,4417	0,3307	
179	0,2426	0,4177	0,3892		
191	0,2572	0,2816	0,4363		
233	0,4255	00,4487	0,6651		
251					0,4903

Окончание табл. 2

Поле (m)	Время реализации СУ в мс				
	Вейерштрасс ДСТУ4145-2202		ДСТУ4145-2202		
			Эдвардс $d_1 \neq d_2$	Эдвардс при $d_1 = d_2$	Эдвардс при $d_1 = d_2$
	Алгоритм Монтгомери (проективные координаты Лопеса-Дахаба)	Бинарный алгоритм (смешанные координаты Лопеса-Дахаба)	Алгоритм Монтгомери (проективные w - координаты)		
251*					0,4600
251**					0,5986
251***					0,6143
257	0,6927	1,1483	1,0424	0,5277	
257*	0,6488	1,076	0,9771	0,4951	
257**	0,8117	1,3829	1,2552	0,6189	
257***	0,8115	1,3825	1,2589	0,6251	
307	0,7742	1,3205	1,2023		
367	1,1507	1,1668	1,7775		
431	1,7486	2,8938	2,6802		

* – Intel Xeon E3-1270v5 3,60 GHz (Windows Server 2012 R2);
** – Intel Core i7-4702MQ 2,2GHz (Windows 8.1 Pro x64);
*** – Intel Core i5-3570 (Windows 7 x64 Ultimate) 3,40 GHz, (AVX version);
# – Intel® Core™ i5-4670 (Windows 7 x64 Ultimate) 3,40 GHz. (AVX2 version).

Для сравнения эффективности скалярного умножения на двоичных кривых Вейерштрасса из ДСТУ 4145-2002, а также соответствующих им бирационально эквивалентных кривых Эдвардса при $d_1 \neq d_2$ [8] и $d_1 = d_2$ (см. табл. 3), а также для $d_1 = d_2$ с размером d_1 не более 64 бита [10] была выполнена реализация алгоритма СУ по методу Монтгомери на языке высокого уровня C++ в среде Microsoft Visual C++ 2015 Express Edition с учетом фиксированного приведения по модулю [6] и при инвертировании использовался метод [7]. Замеры времени производились как среднее время выполнения 1000 операций, с помощью вычислительной системы с процессором Intel Core i7-6700 2,60 GHz, под управлением ОС Windows 10 x86-64, Intel Xeon E3-1270v5 3,60 GHz (Windows Server 2012 R2), Intel Core i7-4702MQ 2,2GHz (Windows 8.1 Pro x64). В табл. 2 представлены результаты замеров производительности реализации операции СУ для двоичных кривых Вейерштрасса и соответствующих бирационально эквивалентных кривых Эдвардса в проективных w -координатах. Результаты, приведенные в табл. 2, показывают, что производительность операции СУ на кривых Эдвардса преобладает над БЭК Эдвардса с двумя параметрами. Рассматривая время реализации СУ на кривых Эдвардса, при условии $d_1 = d_2$, то производительность реализации СУ растет начиная с поля $GF\left(2^{257}\right)$.

Таблица 3

Бирационально эквивалентное преобразование двоичных кривых Вейерштрасса из ДСТУ 4145-2002 в двоичные кривые Эдвардса с одним параметром

Кривые Вейерштрасса (изоморфные)	**БЭК Эдвардса**
Поле 173	

a=c3b83a9be232fbe1f5012bbaa7b24e9ea1a265a1056;
b=108576c80499db2fc16eddf6853bbb278f6b6fb437d9;
Xw=4d41a619bcc6eadf0448fa22fad567a9181d37389ca;
Yw=19595eda0a1190cd5a1e5e731f03ff94ac5c0d41635a;
	d=e92f31c2f97583b5b079a66498651cff964d4edc1;
	Xe=9c31a259ac014b272a80452b4c50ab08afd833f48f7;
	Ye=18a8bce3975a6c58bc03279c87f7902cbd44b8d6728;

Поле 257	

a=1df8904dcdca731d5b055ba8e258f7927d18c9946d68988e878c7aef3eb1654a8;
b=1cef494720115657e18f938d7a7942394ff9425c1458c57861f9eea6adbe3be10;
Xw=2a29ef207d0e9b6c55cd260b306c7e007ac491ca1b10c62334a9e8dcd8d20fb7;
Yw=6cb64ffdc022976cb9e87d5c70a0a181271ab25eb27ae9da67c875bd7dda7d6d;
	d=1a561c01c65fda18821a29f0299c88c26c8a85c4f5f326bf152b115950e5ab7a6;
	Xe=14f0139b391a9f8dd68a0160b2e1a0e08dd2dfa731e8ce7ffadf5fda4102705d6;
	Ye=5cde2ec44b73aee5413d6aa26219ff673ff206f082b073b6ad3b47d2e7f873f5;

Выводы

1. Выполнена программная реализация СУ для кривых Вейерштрасса и БЭК Эдвардса для двоичного поля из ДСТУ 4145-2002, некоторых полей NIST, а также для кривой Эдвардса с один параметром d_1 с максимальным размером в 64 бита для поля размером 251.

2. Выигрыш в производительности СУ на кривых Эдвардса с одним коэффициентом составил 1,3 раза перед реализацией СУ на соответствующих кривых Вейерштрасса начиная с поля, размером 257. Реализация СУ на кривых Эдвардса, с коэффициентами d_1 и d_2, проигрывает в 1,2 раза перед кривыми Вейерштрасса.

3. Дальнейшая работа нацелена на поиск параметров двоичной кривой Эдвардса для полей из ДСТУ 4145-2002, размером 307, 367, 431, с генерацией параметра d_1 с максимальным размером в 64 бита, что позволит значительно защитить и повысить производительность формирования и проверки ЭЦП на основе фиксированной точки.

Список литературы

1. Закон Украины об электронной цифровой подписи // Ведомости Верховной Рады. – 2003. – №36. – С. 1029-1035.
2. Закон Украины об электронных документах и электронном документообороте // Ведомости Верховной Рады. – 2003. – №36. – С. 1025-1029.
3. ДСТУ 4145–2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка. – К.: Госстандарт Украины, 2002. – 40 с.
4. Kovtun M. Search method development of birationally equivalent binary Edwards curves for binary Weierstrass curves from DSTU 4145-2002 / V. Kovtun., A. Okrimenko, S. Gnatyuk // Conference Paper: PIC S&T 2015, Kharkov, Ukraine, October 13-15, 2015. – P. 5-8. DOI: 10.1109/INFOCOMMST.2015.7357253.
5. Ковтун М.Г. Ускоренное извлечение r -го корня в двоичном поле / М.Г. Ковтун, С.А. Гнатюк, В.И. Трофименко // Международная науч.-практ. конференция «Информационные и телекоммуникационные технологии: образование, наука, практика», 2-4 декабря 2015 г., г. Алматы, Казахстан. – С. 547-551.
6. Kovtun M. Method of Algorithm Building for Modular Reducing by Irreducible Polynomial / A. Okhrimenko, M. Kovtun, T. Gancarczyk, V. Karpinskyi, S. Gnatyuk // Proceedings of the 16th International Conference on Control, Automation and Systems, Oct. 16-19, 2016, Gyeongju, Korea. – P. 1476-1479. DOI: 10.1109/ICCAS.2016.7832498.
7. Булах М.Г. Методы повышения производительности операции инвертирования в двоичном поле / М.Г. Булах, В.Ю. Ковтун // Безпека інформації. – 2014. – Том 20, №1. – С. 55-61.
8. Bernstein D.J. Binary Edwards Curve. Cryptographic Hardware and Embedded Systems - CHES 2008 / D.J. Bernstein, T. Lange, R. Rezaeian Farashahi. – Berlin: Springer, 2008. – ISBN 978-3-540-85052-6. – P. 244-265.
9. Ho Kim K. Binary Edwards Curve Revisiteed / K. Ho Kim, C. Ok Lee, Ch. Negre // Progress in Cryptology -- INDOCRYPT 2014. – P. 393-408.
10. Bernstein D.J. Batch binary Edwards. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677. – Springer, Heidelberg, 2009. – P. 317-336.
11. Li Ming. Fast Algorithm for Converting Ordinary Elliptic Curves into Binary Edward Form / Ming Li, Ali Miri, Daming Zhu // International Journal of Digital Content Technology & its Applications. – Jan 2012, Vol. 6, Issue 1. – P. 405-412.
12. Koziel B. Low-Resource and Fast Binary Edwards Curves Cryptography / B. Koziel, R. Azarderakhsh, M. Mozaffari-Kermani // Progress in Cryptology -- INDOCRYPT 2015. – P. 347-369.
13. Zhang F. Halving of Binary Edwards Curve. [Электронный ресурс] / F. Zhang // Journal of National University of Defense Technology. – 2016. – Режим доступа к статье: https://www.researchgate.net/publication/220336653_Halving_on_Binary_Edwards_Curves.
14. Bernstein D.J. Faster addition and doubling on elliptic curves. In: Kurosawa, K. (ed.) / D.J. Bernstein, T. Lange // ASIACRYPT 2007. LNCS. – Vol. 4833. – Springer, Heidelberg. – P. 29-50.
15. Joye M. Highly Regular Right-to-Left Algorithms for Scalar Multiplication. In Pascal Paillier and Ingrid Verbauwhede, editors / Marc Joye // Cryptographic Hardware and Embedded Systems, 9th International Workshop – CHES 2007, LNCS. – Vol. 4727. – Springer, 2007. – P. 135-147.
16. Morain F. Speeding up the computation on an elliptic curve using addition-subtraction chains / Francois Morain, Jorger Olivos // Information Theory Appl., 24: 531-543, 1990.
17. Hankerson D. Guide to Elliptic Curve Cryptography / Darrel Hankerson, Alfred J. Menezes, Scott Vanstone. – Springer-Verlag, 2003.
18. Peter L. Montgomery. Speeding the Pollard and Elliptic Curve Methods of Factorization / L. Peter // Mathematics of Computation. – 1987. – No. 48(177). – P. 243-264.
19. База данных явных формул. [Электронный ресурс]. – Режим доступа к ресурсу: http://www.hyperelliptic.org/EFD.
20. Brier E. Weierstrass elliptic curves and side-channel attacks. In David Naccache and Pascal Paillier, editors / Eric Brier, Marc Joye // Public Key Cryptography – PKC 2002, LNCS. – Vol. 2274. – Springer, 2002. – P. 335-345.
21. Izu T. A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks / Tetsuya Izu, Tsuyoshi Takagi // Public Key Cryptography – PKC 2002, LNCS. – Vol. 2274, Springer, 2002. – P. 280-296.
22. M¨oller B. Securing Elliptic Curve Point Multiplication against Side-Channel Attacks / B. M¨oller // Information Security, G.I. Davida and Y. Frankel, Eds., LNCS 2200. – Springer-Verlag, 2001. – P. 324-334.

23. Shah P.G. Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes / P.G. Shah, X. Huang, D. Sharma // Proceeding in international conference on wireless communication and sensor computing. – 2010. – P. 1-6.

References

1. (2003), "Zakon Ukrainyi ob elektronnoy tsifrovoy podpisi" [The Law of Ukraine on Electronic Digital Signature], *Vedomosti Verhovnoy Radyi*, No. 36, pp. 1029-1035.

2. (2003), "Zakon Ukrainyi ob elektronnyih dokumentah i elektronnom dokumentooborote" [The Law of Ukraine on Electronic Documents and Electronic Document Management], *Vedomosti Verhovnoy Radyi*, No. 36, pp. 1025-1029.

3. (2002) "*DSTU 4145–2002. Informatsionnyie tehnologii. Kriptograficheskaya zaschita informatsii. Tsifrovaya podpis, osnovannaya na ellipticheskih krivyih. Formirovanie i proverka*" [*DSTU 4145-2002. Information Technology. Cryptographic protection of information. Digital signature based on elliptical curves. Formation and verification*], Gosstandart Ukrainyi, Kiev, 40 p.

4. Kovtun, M., Kovtun, V., Okrimenko, A. and Gnatyuk, S. (2015), "Search method development of birationally equivalent binary Edwards curves for binary Weierstrass curves from DSTU 4145-2002", *Conference Paper: PIC S&T 2015*, Kharkov, October 13-15, pp. 5-8, DOI: 10.1109/INFOCOMMST.2015.7357253.

5. Kovtun, M., Gnatyuk, S. and Trofimenko, V. (2015), "Uskorennoe izvlechenie r -go kornya v dvoichnom pole" [Accelerated extraction of the r -th root in the binary field], *International Scientific Practical Conference "Information and telecommunication technologies: education, science, practice"*, Almaty, Kazakhstan, pp. 547-551.

6. Kovtun, M., Okhrimenko, A., Gancarczyk, T., Karpinskyi, V. and Gnatyuk, S. (2016), Method of Algorithm Building for Modular Reducing by Irreducible Polynomial, *16th International Conference on Control, Automation and Systems*, Gyeongju, Korea, pp. 1476-1479, DOI: 10.1109/ICCAS.2016.7832498.

7. Bulakh, M.G., Kovtun, V.Yu. (2014), "Metodyi povyisheniya proizvoditelnosti operatsii invertirovaniya v dvoichnom pole" [Methods for increasing the performance of an inverting operation in a binary field], *Information security*, Vol. 20, No. 1, pp. 55-61.

8. Bernstein, D.J., Lange, T. and Rezaeian Farashahi, R. (2008), Binary Edwards Curve, *Cryptographic Hardware and Embedded Systems - CHES 2008"*, Berlin, pp. 244-265.

9. Ho Kim, K., Ok Lee, C. and Negre, Ch. (2014), Binary Edwards Curve Revisiteed, *INDOCRYPT 2014*, pp. 393-408.

10. Bernstein, D.J. (2009), Batch binary Edwards, *CRYPTO 2009*, LNCS, Vol. 5677, Heidelberg, pp. 317-336.

11. Li, M., Miri, A. and Zhu, D. (2012), Fast Algorithm for Converting Ordinary Elliptic Curves into Binary Edward Form, *International Journal of Digital Content Technology & its Applications*, Vol. 6 (1), pp. 405-412.

12. Koziel, B., Azarderakhsh, R. and Mozaffari-Kermani, M. (2015), Low-Resource and Fast Binary Edwards Curves Cryptography, *Progress in Cryptology -- INDOCRYPT 2015*, pp. 347-369.

13. Zhang, F. (2016), Halving of Binary Edwards Curve, *Journal of National University of Defense Technology*. URL:https://www.researchgate.net/publication/220336653_Halving_on_Binary_Edwards_Curves.

14. Bernstein, D.J. and Lange, T. (2007), Faster addition and doubling on elliptic curves, *ASIACRYPT 2007*, LNCS, Vol. 4833, Heidelberg, pp. 29-50.

15. Joye, M. (2007), Highly Regular Right-to-Left Algorithms for Scalar Multiplication, *Cryptographic Hardware and Embedded Systems, 9th International Workshop – CHES 2007*, LNCS, Vol. 4727, pp. 135-147.

16. Morain, F. and Olivos, J. (1990), Speeding up the computation on an elliptic curve using addition-subtraction chains, *Information Theory Appl.*, Vol. 24, pp. 531-543.

17. Hankerson, D., Menezes, A.J. and Vanstone, S. (2003), *Guide to Elliptic Curve Cryptography*, Springer-Verlag.

18. Montgomery, P.L. (1987), Speeding the Pollard and Elliptic Curve Methods of Factorization, *Mathematics of Computation*, No. 48(177), pp. 243-264.

19. *Explicit-Formulas Database*, http://www.hyperelliptic.org/EFD.

20. Brier, E. and Joye, M. (2002), Weierstrass elliptic curves and side-channel attacks, *Public Key Cryptography – PKC 2002*, LNCS, Vol. 2274, Springer, pp. 335-345.

21. Izu, T. and Takagi, T. (2002), A Fast Parallel Elliptic Curve Multiplication Resistant against Side Channel Attacks, *Public Key Cryptography – PKC 2002*, LNCS, Vol. 2274, Springer, pp. 280-296.

22. M¨oller, B. (2001), Securing Elliptic Curve Point Multiplication against Side-Channel Attacks, *Information Security*, LNCS 2200, Springer-Verlag, pp. 324-334.

23 Shah, P.G., Huang, X. and Sharma, D. (2010), Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes, *proceeding in International Conference on Wireless Communication and Sensor Computing*, pp. 1-6, DOI:10.1109/ICWCSC.2010.5415874.

Поступила в редколлегию 14.09.2017
Одобрена к печати 2.11.2017

Відомості про автора:

Ковтун Марія Григорівна
аспірант кафедри Національного авіаційного університету,
Київ, Україна
https://orcid.org/0000-0002-3021-2659
e-mail: mg.kovtun@gmail.com

Information about the author:

Kovtun Mariya
Postgraduate student of National Aviation university,
Kyiv, Ukraine
https://orcid.org/0000-0002-3021-2659
e-mail: mg.kovtun@gmail.com

ЗАСТОСУВАННЯ КРИВИХ ЕДВАРДСА ДЛЯ ЗАХИЩЕНОЇ РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ ЗГІДНО ДСТУ 4145-2002

М.Г. Ковтун

Розглядається підвищення швидкодії криптографічних перетворень при формуванні та перевірки ЕЦП згідно ДСТУ 4145-2002, за рахунок використання біраціональних еквівалентних кривих Едвардса над двійковим полем, при виконанні проміжних перетворень в скалярному множенні.

В роботі аналізується операція скалярного множення на довічних еліптичних кривих Вейерштрасса з ДСТУ 4145-2002, а також на біраціональних еквівалентних їм кривим Едвардса для випадку $d_1 \neq d_2$ *і* $d_1 = d_2$ *. Порівнюється продуктивність для кривих Едвардса для загального випадку* $d_1 \neq d_2$ *і* $d_1 = d_2$ *, а також продуктивність виконання операції, при розмірі, що не перевищує 64 біта. В результаті досліджень вдалося з'ясувати, що продуктивність операції скалярного множення на кривих Вейерштрасса з ДСТУ 4145-2002 показала найкращий час, ніж на кривих Едвардса в загальному випадку* $d_1 \neq d_2$ *. Однак, час реалізації операції скалярного множення на двійкових кривих Едвардса, з умовою* $d_1 = d_2$ *, в 1.3 рази краще часу на стандартизованих кривих Вейерштрасса починаючи з поля* $GF\left(2^{257}\right)$ *. Подальші дослідження будуть присвячені пошуку довічних кривих Едвардса з* $d_1 \neq d_2$ *для полів з ДСТУ 4145-2002, що дозволить підвищити ефективність національної системи ЕЦП.*

Ключові слова*: еліптичні криві, двійкові криві Едвардса, двійкові криві Вейерштрасса, ЕЦП, ДСТУ 4145-2002, скалярне множення, сходи Монтгомері.*

USING EDWARDS CURVES FOR THE PROTECTED IMPLEMENTATION OF DIGITAL SIGNATURE MECHANISMS ACCORDING TO DSTU 4145-2002 STANDARD

M. Kovtun

The speed increasing of the cryptographic transformations during the generation and verification of digital signatures according to DSTU 4145-2002 is considered, by using birationally equivalent Edwards curves over binary field, when performing intermediate transformations in scalar multiplication.

The operation of scalar multiplication on binary elliptic Weierstrass curves from DSTU 4145-2002 is analyzed, as well as on the birationally equivalent Edwards curves for the case $d_1 \neq d_2$ *and* $d_1 = d_2$ *. It compares the performance for Edwards curves for the general case* $d_1 \neq d_2$ *and* $d_1 = d_2$ *, as well as the performance of the operation with* $d_1 = d_2$ *, where* d_1 *has bit length near 64 bits. As a results of the research, is that the performance of scalar multiplication on Weierstrass curves from DSTU 4145-2002 showed a better time than on Edwards curves in the general case.* $d_1 \neq d_2$ *However, the time of execution of scalar multiplication on Edwards binary curves, with a condition* $d_1 = d_2$ *, is 1.3 times better than the time on the standardized Weierstrass curves beginning from* $GF\left(2^{257}\right)$ *. Further research will be devoted to finding the binary Edwards curves with* $d_1 = d_2$ *for fields from DSTU 4145-2002, which will improve the efficiency of the national digital signature system.*

Keywords*: elliptic curves, binary Edwards curves, binary Weierstrass curves, digital signature, DSTU 4145-2002, scalar multiplication, Montgomery ladder.*