Разработка метода поиска кривых Эдвардса над двоичным полем бирационально эквивалентных кривым Вейерштрасса приведенным ДСТУ 4145-2002

Мария Ковтун, Андрей Охрименко, Владислав Ковтун, Сергей Гнатюк

В работе анализируются известные алгоритмы поиска эллиптических кривых в форме Эдвардса, бирационально эквивалентных кривым в форме Вейерштрасса. Рассматриваются практические аспекты эффективной программной реализации алгоритма поиска бирационально эквивалентных кривых, которые позволили предложить модифицированный алгоритм. Разработанная программная реализация модифицированного алгоритма, позволила найти, среди приведенных в украинском национальном стандарте ДСТУ 4145-2002, такие кривые, для которых существуют бирационально эквивалентные кривые в форме Эдвардса.

В настоящее время человечество переживает новый этап своего развития – переход от индустриального к постиндустриальному информационному обществу, в котором информация становится важнейшим ресурсом. Этот процесс носит глобальный характер, поэтому вхождение нашей страны в мировое информационное пространство носит неизбежный характер. Для успешного вхождения Украины в число технологически и экономически развитых стран требуются значительные усилия по нормативному регулированию, повышению уровня образования, научно-технического и культурного развития, внедрению новых информационных систем для обработки, хранения и передачи информации. Зрелость процессов информатизации характеризуются степенью обеспечения защиты информации и персональных данных пользователей. С этой целью, в Украине разработаны и успешно эксплуатируются стандарты информационной и криптографической защиты информации, среди которых можно выделить стандарт электронной цифровой подписи (ЭЦП) ДСТУ 4145-2002 [1]. В основе указанного стандарта ЭЦП положены преобразования в группе точек эллиптической кривой (ЭК) в форме Вейерштрассе над полем $\mathbf{GF}\left(2^m\right)$. Перечень допустимых ЭК приводится непосредственно в самом стандарте [1].

Активное использование ЭЦП, согласно ДСТУ 4145-2002, в банковском и государственном секторе, показало невысокую скорость постановки и проверки ЭЦП, что снижало эффективность работы соответствующих информационных систем. Проведенный анализ [2], показал, что наиболее трудоемкой с точки зрения вычислений является математическая операция скалярного умножения точки ЭК на скалярный множитель. Проведенные исследования [2][3] показали, что кривые Вейерштрасса приблизились к пределу своих возможностей с точки зрения скорости скалярного умножения. В качестве перспективных следует рассматривать кривые Эдвардса [3][6], для которых скорость выполнения скалярного умножения существенно выше, чем для кривых Вейерштрасса, за счет более простой операции сложения точек. Следует отметить, что известно о существовании рациональной и бирациональной эквивалентности кривых Вейерштрасса к кривым Эдвардса [5]. Это открывает новые возможности для повышения скорости криптографических преобразований за счет перехода от кривой Вейерштрасса к кривой Эдвардса для выполнения промежуточных вычислений (скалярного умножения) [6]. Другими словами, для существующих стандартов ЭЦП [1][10], с уже рекомендованными кривыми Вейерштрасса, можно существенно повысить скорость формирования и проверки ЭЦП.

Известные алгоритмы [5][8] поиска бирациональных кривых Эдвардса, показывают очень низкую производительность, что не позволяет говорить об их практической эффективности. В связи с этим, ***актуальной научно-технической задачей***, является разработка алгоритма поиска бирациональной эквивалентной кривой в форме Эдвардса для ЭК в форме Вейерштрасса над полем $\mathbf{GF}\left(2^m\right)$ с уменьшенной вычислительной сложностью.

Целью работы является разработка модифицированного алгоритма поиска ЭК в форме Эдвардса бирационально эквивалентных ЭК в форме Вейерштрасса из ДСТУ 4145-2002 с уменьшенной вычислительной сложностью путем выполнения предвычислений, изменения порядка вычислений и использования аддитивных цепочек при извлечении кубического корня из элементов поля $\mathbf{GF}\left(2^m\right)$.

Поиск будет производиться среди ЭК в форме Вейерштрасса из ДСТУ 4145-2002, заданных над полями $\mathbf{GF}\left(2^m\right)$ со степенью расширения $m \in \{163,167,173,179,191,233,257,307,367,431\}$ с представлением в полиномиальном базисе.

Для достижения поставленной цели, необходимо решить следующие подзадачи:

1. Проанализировать известные алгоритмы поиска кривой Эдвардса бирационально эквивалентную заданной кривой Вейерштрасса.

2. Разработать алгоритм поиска кривой Эдвардса бирационально эквивалентную заданной кривой Вейерштрасса или доказать, что такой кривой не существует.

3. Разработать эффективную программную реализацию разработанного алгоритма поиска бирациональной эквивалентной кривой Эдвардса.

4. Произвести поиск кривых Эдвардса бирационально эквивалентных кривым Вейерштрасса из списка рекомендованных ДСТУ 4145-2002 или доказать, что таких кривых не существует.

5. Для найденных эквивалентных кривых произвести отображение рекомендованных базовых точек на кривой Вейерштрасса в точки на кривой Эдвардса.

Пусть, задана ЭК в форме Вейерштрасса над полем $\mathbf{GF}\left(2^m\right)$ в виде [8]:

$$v^2+uv=u^3+au^2+b, \tag{1}$$

где a и b - параметры ЭК.

Необходимо найти бирационально эквивалентную кривую Эдвардса вида [8]:

$$d_1(x+y)+d_2\left(x^2+y^2\right)=xy+xy(x+y)+x^2y^2, \tag{2}$$

где d_1 и d_2 - коэффициенты кривой такие, что $d_1\neq 0$ и $d_2\neq d_1^2+d_1$. Кривая (2) бирационально эквивалентна кривой (1):

$$v^2+uv=u^3+\left(d_1^2+d_2\right)u^2+d_1^4\left(d_1^4+d_1^2+d_2^2\right), \tag{3}$$

где условие $d_1^4\left(d_1^4+d_1^2+d_2^2\right)\neq 0$ обеспечивает не суперсингулярность кривых.

Отображение точки на ЭК в форме Вейерштрасса в точку на кривой в форме Эдвардса $(u,v)\mapsto(x,y)$ определяется следующим образом [8]:

$$x=\frac{d_1\left(u+d_1^2+d_1+d_2\right)}{u+v+\left(d_1^2+d_1\right)\left(d_1^2+d_1+d_2\right)}, \tag{4}$$

$$y=\frac{d_1\left(u+d_1^2+d_1+d_2\right)}{v+\left(d_1^2+d_1\right)\left(d_1^2+d_1+d_2\right)}. \tag{5}$$

Отображение точки на ЭК в форме Эдвардса в точку на кривой в форме Вейерштрасса $(x,y)\mapsto(u,v)$ определяется как [8]:

$$u=d_1\left(d_1^2+d_1+d_2\right)\frac{x+y}{xy+d_1(x+y)}, \tag{6}$$

$$v=d_1\left(d_1^2+d_1+d_2\right)\left(\frac{x}{xy+d_1(x+y)}+d_1+1\right). \tag{7}$$

Разработка алгоритма поиска бирационально эквивалентных кривых Эдвардса

Проведенный анализ публикации **Ошибка! Источник ссылки не найден.**[5][6][8] показал наличие алгоритмов поиска кривой в форме Эдвардса эквивалентной кривой Вейерштрасса, приведенных в виде Алгоритма 1 [6] и Алгоритма 2 [8].

Оба алгоритма являются вероятностными, однако отличие Алгоритма 1 состоит в том, что для получения параметров искомой кривой Эдвардса необходимо сделать значительное число итераций: поскольку $\mathbf{P}\left(\mathrm{Tr}(\mathrm{d}_1)=\mathrm{Tr}(a)+1\right)=1/2$ п.1.1 должен выполняться в среднем 2 раза; а также следует заметить, что если $\mathrm{Tr}\left(\sqrt{b}/d_1^2\right)\neq 1$, то нужно вернуться в п. 1.1. Алгоритм 2 лишен недостатков Алгоритма 1 и позволяет почти всегда на первой итерации получить параметры искомой кривой Эдвардса, причем на каждой итерации алгоритма следует выполнять менее сложные математические операции. С последующими итерациями вероятность получения искомых параметров стремится к 1.

Более подробно остановимся на Алгоритме 1 [6], который можно разбить на несколько стадий:

1. Поиск бирационально эквивалентной кривой Эдвардса.

2. Отображение точки кривой Вейерштрасса в бирационально эквивалентную ей точку кривой Эдвардса.

3. Проверка условия бирациональности, посредством обратного отображения полученной на стадии 2 точки кривой Эдвардса в точку исходной кривой Вейерштрасса.

4. Сравнение точек на кривой Вейерштрасса: исходной и полученной в результате отображения в точку на кривой Эдвардса и обратно.

Алгоритм 1. Поиск бирациональных кривых Эдвардса, с использованием квадратного корня.

Вход: $a,b \in \mathbf{GF}\left(2^m\right),\ X_W = (u,v) \in \mathbf{GF}\left(2^m\right),\ \beta \leftarrow \mathrm{Trace}(a)$.

Выход: $d_1, d_2 \in \mathbf{GF}\left(2^m\right),\ X_E = (x,y) \in \mathbf{GF}\left(2^m\right)$.

I. Пп. 1-5 - поиск параметров бирациональной эквивалентной кривой Эдвардса.

1. Do

1.1. Random (d_1).

1.2. $\alpha \leftarrow \mathrm{Tr}(d_1)$.

1.3. While $(\alpha \neq (\beta + 1))$

2. If $\left(\mathrm{Tr}\left(\sqrt{b}/d_1^2\right) = 1\right)$ then

2.1. $d_2 \leftarrow d_1^2 + d_1 + \sqrt{b} \cdot d_1^2$

3. Else goto 1.1.

4. $a' \leftarrow d_1^2 + d_2$.

5. Решение квадратного уравнения относительно λ: $\lambda^2 + \lambda + a + a' = 0$.

II. Пп. 6-8– нахождение бирациональной точки кривой Эдвардса, если задана точка на кривой Вейерштрасса.

6. $x' \leftarrow \dfrac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{u + v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)}$.

7. $y' \leftarrow \dfrac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)}$.

8. $x \leftarrow x',\ y \leftarrow y' + \lambda x'$.

III. Пп. 9-11 – нахождение бирациональной точки Вейерштрасса, если найдена точка на кривой Эдвардса. (Проверка условия бирациональности).

9. $x' \leftarrow x,\ y' \leftarrow y + \lambda x'$.

10. $u \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\dfrac{x' + y'}{x'y' + d_1(x' + y')}$

11. $v \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\left(\dfrac{x'}{x'y' + d_1(x' + y')} + d_1 + 1\right)$.

IV. Пп. 12-13 – проверка условия бирациональности точек кривой Вейерштрасса.

12. If $\left(X_w(u,v) = (u,v) \right)$ then

12.1. Return $(d_1, d_2, X_E(x,y))$.

13. Return $(0,0, X_E(0,0))$.

Суть Алгоритма 1 состоит в подборе коэффициента кривой Эдвардса d_1 на шагах пп.1-3 таким образом, чтобы $\mathrm{Tr}(d_1) = \mathrm{Tr}(a)+1$ и в то же время $\mathrm{Tr}\left(\sqrt{b}/d_1^2\right)=1$, $\mathrm{Tr}(\cdot)$ - след элемента поля $\mathbf{GF}\left(2^m\right)$. В случае выполнения указанных условий, становится возможным вычисление коэффициента d_2. Далее в п.4 подбирается новый коэффициент кривой Вейерштрасса a'. В п.5 выполняется решение квадратного уравнения относительно λ. Для заданной точки на кривой Вейерштрасса, в пп.6-8 происходит вычисление бирационально эквивалентной точки Эдвардса, для которой в пп. 9-11 проверяется **тождество.** Для проверки условия бирациональности следует точку на полученной кривой Эдвардса снова отобразить в точку на кривой Вейерштрасса в пп. 9-11.

В работе [7] проанализирована вычислительная сложность алгоритма 1 - $7\mathbf{T}+2\mathbf{S}+4\mathbf{I}+17\mathbf{M}+1\mathbf{Sqrt}+1\mathbf{E}$, где $\mathbf{T},\mathbf{S},\mathbf{I},\ \mathbf{M},\mathbf{Sqtr},\mathbf{E},\mathbf{Cubrt}$ - вычисление следа, возведения в степень, инвертирование, умножение, вычисление квадратного корня, решение квадратного уравнения, кубического корня, соответственно.

Далее перейдем к описанию Алгоритма 2 [8]. Авторы Алгоритма 2 [8], выяснили, что необходимым условием существования бирационально эквивалентной кривой Эдвардса для кривой Вейерштрасса, является условие $\mathrm{Tr}\left(a^6/b\right)=0$, согласно Теореме 1 [8].

Теорема 1. В поле $\mathbf{GF}\left(2^m\right)$, ЭК $E_{B,a,b}$ в форме Вейерштрасса имеет эквивалентную двоичную кривую в форме Эдвардса E_{B,d_1,d_2} с $a = d_1^2 + d_2$ и $b = d_1^4\left(d_1^4 + d_1^2 + d_2^2\right)$ тогда, и только тогда, когда $\mathrm{Tr}\left(a^6/b\right)=0$.

В связи с этим, необходимо производить такую проверку на всех итерациях поиска параметра a. В случае выполнения условия $\mathrm{Tr}\left(a^6/b\right)=0$ необходимо решить квадратное уравнение $r^2 + r + a^6/b = 0$. Для вычисления коэффициентов кривой Эдвардса d_1 и d_2 используются корень уравнения r, параметр ЭК b и модифицированный параметр ЭК a. Далее производится отображение точки кривой Вейерштрасса в бирационально эквивалентную на кривой Эдвардса согласно (4) и (5), а также обратное отображение для проверки условия бирациональности согласно (6) и (7).

Алгоритм 2. Поиск бирационально эквивалентных кривых Эдвардса, с использованием кубического корня.

Вход: $a,b \in \mathbf{GF}\left(2^m\right),\ X_W = (u,v) \in \mathbf{GF}\left(2^m\right)$.

Выход: $d_1, d_2 \in \mathbf{GF}\left(2^m\right),\ X_E = (x,y) \in \mathbf{GF}\left(2^m\right)$.

I. Пп.1-4 - поиск параметров бирациональной эквивалентной кривой Эдвардса.

1. $\left(\mathrm{Tr}\left(a^6/b\right)\neq 0\right)$ do

1.1. Random (λ), $\lambda \in \mathbf{GF}\left(2^m\right)$.

1.2. $a \leftarrow a + \lambda + \lambda^2$.

2. Решение квадратного уравнения $r^2 + r + a^6/b = 0$, относительно r.

3. $d_1 \leftarrow \sqrt[3]{\sqrt{b}\cdot r} + \sqrt[3]{\sqrt{b}\cdot(r+1)} + a$.

4. $d_2 \leftarrow d_1^2 + a$.

II. Пп. 5-6– нахождение бирациональной точки кривой Эдвардса, если задана точка на кривой Вейерштрасса.

5. $x' \leftarrow \dfrac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{u + v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)}$.

6. $y' \leftarrow \dfrac{d_1\left(u + d_1^2 + d_1 + d_2\right)}{v + \left(d_1^2 + d_1\right)\left(d_1^2 + d_1 + d_2\right)}$.

7. $x \leftarrow x'$, $y \leftarrow y' + \lambda x'$.

III. Пп. 8-10 – нахождение бирациональной точки Вейерштрасса, если найдена точка на кривой Эдвардса, для проверки условия бирациональной эквивалентности.

8. $x' \leftarrow x$, $y' \leftarrow y + \lambda x'$.

9. $u \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\dfrac{x' + y'}{x'y' + d_1\left(x' + y'\right)}$

10. $v \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\left(\dfrac{x'}{x'y' + d_1\left(x' + y'\right)} + d_1 + 1\right)$.

IV. Пп. 11-12 – проверка условия бирациональности точек кривой Вейерштрасса.

11. If $\left(X_w(u,v) = (u,v)\right)$do

11.1. Return $\left(d_1, d_2, X_E(x,y)\right)$.

12. Return $\left(0,0, X_E(0,0)\right)$.

Для Алгоритма 2 вычислительная сложность имеет вид - $2\mathbf{T} + 4\mathbf{S} + 4\mathbf{I} + 16\mathbf{M} + 1\mathbf{Sqrt} + 1\mathbf{E} + 1\mathbf{Cubrt}$ [7], где $\mathbf{T}, \mathbf{S}, \mathbf{I}, \mathbf{M}, \mathbf{Sqtr}, \mathbf{E}, \mathbf{Cubrt}$ - вычисление следа, возведения в степень, инвертирование, умножение, вычисление квадратного корня, решение квадратного уравнения, кубического корня, соответственно.

Алгоритм 3 отличается от алгоритма 2 меньшим количеством операций за счет предвычислений, а также дополнительной проверкой существования решения квадратного уравнения: если решение квадратного уравнения не существует в п.6.1.3, происходит возврат к пункту 6.1. Так же для извлечения кубического корня предложен модифицированный алгоритм с использованием разложения аддитивных цепочек [14][15].

Перед выполнением непосредственно самого алгоритма, следует произвести предвычисления для константы - параметра b кривой Вейерштрасса.

Алгоритм 3. Поиск бирационально эквивалентных кривых Эдвардса, с использованием кубического корня.

Вход: $a, b \in \mathbf{GF}\left(2^m\right)$, $X_W = (u,v) \in \mathbf{GF}\left(2^m\right)$.

Выход: $d_1, d_2 \in \mathbf{GF}\left(2^m\right)$, $X_E = (x,y) \in \mathbf{GF}\left(2^m\right)$.

Предвычисления:

1. $SR_b \leftarrow \sqrt{b}$.

2. $\gamma \leftarrow 1/b$.

Основной алгоритм:

I. Пп.3-13 - поиск параметров бирациональной эквивалентной кривой Эдвардса.

3. $a_2 \leftarrow a$.

4. $\lambda \leftarrow 0$.

5. $z \leftarrow 1$.

6. While $(z \neq 0)$

6.1. While $\left(\mathrm{Tr}\left(a_2^6 \cdot \gamma\right) \neq 0\right)$

6.1.1. Random (λ), $\lambda \in \mathbf{GF}\left(2^m\right)$.

6.1.2. $a_2 \leftarrow a_2 + \lambda^2 + \lambda$.

6.1.3. Решение квадратного уравнения: $r^2 + r + a_2^6 \cdot \gamma = 0$, относительно r.

6.1.4. If $(\mathrm{IsSolutionExist}(r))$ then $z \leftarrow 0$.

7. $g_1 \leftarrow SR_b \cdot r$.

8. $g_2 \leftarrow SR_b \cdot (r+1)$.

9. $SR_1 \leftarrow \sqrt[3]{g_1}$.

10. $SR_2 \leftarrow \sqrt[3]{g_2}$.

11. $d_1 \leftarrow SR_1 + SR_2 + a_2$.

12. $\delta \leftarrow d_1^2$.

13. $d_2 \leftarrow \delta + a_2$.

II. Пп. 14-19 нахождение бирациональной точки кривой Эдвардса, если задана точка на кривой Вейерштрасса.

14. $\varphi \leftarrow \delta + d_1$.

15. $C_1 \leftarrow \varphi + d_2$.

16. $C_2 \leftarrow (C_1 + u) \cdot d_1$.

17. $C_3 \leftarrow \varphi \cdot C_1 + v$.

18. $x \leftarrow C_2 / (u + C_3)$.

19. $y \leftarrow C_2 / C_3 + \lambda \cdot x$.

III. Пп. 20-22 – нахождение бирациональной точки Вейерштрасса, если найдена точка на кривой Эдвардса, для проверки условия бирациональной эквивалентности.

20. $x' \leftarrow x$, $y' \leftarrow y + \lambda x'$.

21. $u \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\dfrac{x' + y'}{x'y' + d_1(x' + y')}$

22. $v \leftarrow d_1\left(d_1^2 + d_1 + d_2\right)\left(\frac{x'}{x'y' + d_1(x' + y')} + d_1 + 1\right)$.

IV. Пп. 11-12 – проверка условия бирациональности точек кривой Вейерштрасса.

23. If $\left(X_w(u,v) = (u,v)\right)$do

23.1. Return $(d_1, d_2, \{x, y\})$.

24. Return $(0,0, X_E(0,0))$.

Анализ Алгоритма 1, 2 и 3 показывает, что его реализация не является тривиальной, т.к. требует вычисления сложных математических операций, таких как извлечение квадратного и кубического корня из элементов поля $\mathbf{GF}\left(2^m\right)$. Проведенный анализ публикаций [9][16][17][18] по тематике эффективного вычисления квадратного и кубического корня в поле $\mathbf{GF}\left(2^m\right)$, позволил выбрать наиболее производительные. Авторы воспользовались ограничением, которое выдвигается к ЭК над полем $\mathbf{GF}\left(2^m\right)$, m - нечетное. Ниже приведем Алгоритм 4 [10] извлечения квадратного корня в поле $\mathbf{GF}\left(2^m\right)$.

Алгоритм 4. Вычисление квадратного корня в поле $\mathbf{GF}\left(2^m\right)$.

Вход: $\alpha \in \mathbf{GF}\left(2^m\right)$, m - нечетное.

Выход: $s \leftarrow \sqrt{\alpha} \in \mathbf{GF}\left(2^m\right)$.

1. $s \leftarrow \alpha$.

1. For $i \leftarrow 0$, $i < m$, $i{+}{+}$ do

1.1. $s \leftarrow s^2$.

2. Return (s).

После получения квадратного корня необходимо сравнить результат: если $s^2 = \alpha$, тогда считается результат верный, в противном случае – нет.

Для вычисления r-го корня, в нашем случае $r = 3$, необходимо, чтобы $r \mid (q-1)$ и $\left((q-1)/r, r\right) = 1$ для $m > 0$ такого, что $(m, r) = 1$. Учитывая тот факт, что m - нечетное и не делится нацело на 2, можно говорить о применимости данного алгоритма. Ниже представлен Алгоритм 5 вычисления кубического корня. Более подробное обоснование корректности алгоритма приведено в Лемме 3 [9].

Алгоритм 5. Вычисление кубического корня из элемента поля $\alpha \in \mathbf{GF}\left(2^m\right)$.

Вход: $\alpha \in \mathbf{GF}\left(2^m\right)$, где m - нечетное.

Выход: $\beta \leftarrow \sqrt[3]{\alpha}$, $\beta \in \mathbf{GF}\left(2^m\right)$.

1. $v \leftarrow 0$.

2. $p \leftarrow 2^m - 1$.

3. For $i \leftarrow 0$, $i \le \left((m-1)/2\right)$, $i{+}{+}$ do

3.1. $v \leftarrow \left(v + 4^i\right) \bmod p$.

4. $\beta \leftarrow a^v$.

5. Return (β).

После вычисления кубического корня необходимо сравнить результат: если $\beta^3 = \alpha$, тогда результат верный, в противном случае – нет.

В Алгоритме 5 используется возведение в произвольную степень, что говорит о его меньшей эффективности чем алгоритма вычисления квадратного корня. В связи с этим, опишем предложенные авторами методы ускорения Алгоритма 5, посредством изменения порядка вычислений и предвычислений.

При вычислении в п.3.1 показателя степени v, не обязательно приводить по модулю p конечную сумму, полученную в результате выполнения накопления на всех итерация цикла п.3, поскольку она всегда, для наших условий, меньше модуля p [9].

Для повышения скорости возведения в степень, при вычислении кубического корня, можно воспользоваться модификациями, предложенными в работе [14], а также модификациями предложенными авторами для полей из ДСТУ 4145-2002 [15], где идет разложение показателя степени v в аддитивную цепочку посредством декомпозиции.

Кубический корень может быть представлен следующим образом [9]:

$$\sqrt[3]{b(x)} = b^{1+2^2+2^4+\ldots+2^{m-1}}(x) \bmod (f(x)) \tag{8}$$

где $1+2^2+2^4+\ldots+2^{m-1}$ - это разложение в аддитивную цепочку, которую можно представить в виде, который позволяет уменьшить количество операций умножения и возведения в квадрат и тем самым увеличить скорость извлечения кубического корня.

Для большей наглядности, ниже приведен Пример 1 декомпозиции показателя степени v в аддитивную цепочку с уменьшенным числом умножений и возведений в квадрат для поля $\mathbf{GF}\left(2^{163}\right)$.

Пример 1. Декомпозиция показателя степени в аддитивную цепочку.

Известно, $m = 163$, тогда согласно (3) [15], разложение цепи будет иметь вид $1+2^2+2^4+\ldots+2^{162}$. В Таблица 1 приводятся все итерации рекурсивного формирования цепочки.

Таблица 1. Пример декомпозиции для поля $\mathbf{GF}\left(2^{163}\right)$

№ итер.	Цепь	Параметры	Условие
1	$1+2^2+2^4+\ldots+2^{162}$	$k=83, n=2$	$k-1\equiv 0 \bmod 2$
2	$\left(1+2^2\right)\left(1+2^4+\ldots+2^{(83-3)\cdot 2}\right)$	$k=42,\ n=4$	$k-1\equiv 1 \bmod 2$
3	$\ldots\left(1+2^2\right)\left(1+2^4\left(1+2^4\right)\left(1+2^8+\ldots+2^{(42-4)\cdot 4}\right)\right)$	$k=21,\ n=8$	$k-1\equiv 0 \bmod 2$
4	$\ldots\left(1+2^8\right)\left(1+2^{16}+\ldots+2^{(21-3)\cdot 8}\right)$	$k=11,\ n=16$	$k-1\equiv 0 \bmod 2$
5	$\ldots\left(1+2^{16}\right)\left(1+2^{32}+\ldots 2^{(11-3)\cdot 16}\right)$	$k=6,\ n=32$	$k-1\equiv 1 \bmod 2$
6	$\ldots\left(1+2^{32}\left(1+2^{32}\right)\left(1+2^{64}\right)\right)$		

Таким образом, декомпозиция цепочки показателя степени может быть представлена следующим образом:

$$1+2^2+2^4+\ldots+2^{162} = \left(1+2^2\right)\left(1+2^4\left(1+2^4\right)\left(1+2^8\right)\left(1+2^{16}\right)\left(1+2^{32}\left(1+2^{32}\right)\left(1+2^{64}\right)\right)\right).$$

Ниже приведен Алгоритм 6 для извлечения кубического корня, основанное на разложения аддитивных цепей.

При обычном вычислении кубического корня, предложенного в Алгоритме 5 для элементов поля $\mathbf{GF}\left(2^{163}\right)$ при возведении в степень v бинарным методом слева направо происходит $((m-1)/2)\mathbf{M} = 81\mathbf{M}$ умножений и $m\mathbf{S} = 163\mathbf{S}$ - возведений в степень, а у предложенной модификации всего $8\mathbf{M}$ умножений и $6\mathbf{S}$ возведений в квадрат. Данная модификация использует предвычисления.

Алгоритм 6. Извлечение кубического корня в поле $\mathbf{GF}\left(2^{163}\right)$.

Вход: $b(x) \in \mathbf{GF}\left(2^{163}\right)$.

Выход: $\sqrt[3]{b(x)} = b^{\sum_{i=0}^{m-1} 2^{2\cdot i}} \bmod (f(x))$

1. $t_0 \leftarrow b$.

2. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.

3. $t_1 \leftarrow t_0$.

4. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.

5. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.

6. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$.

7. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$.

8. $t_2 \leftarrow t_0$.

9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.

10. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.

11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_2$.

12. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_1$.

13. Return $t_0 = \sqrt[3]{b(x)}$.

При реализации Алгоритмов 1-3, необходимы алгоритмы вычисления других нетривиальных полевых операций, таких как вычисления следа и полу-следа элемента поля $\mathbf{GF}\left(2^m\right)$.

В основе Алгоритма 7 [10] вычисления следа элемента поля $\mathbf{GF}\left(2^m\right)$ лежит факт, что если α элемент $\mathbf{GF}\left(2^m\right)$, то след α можно представить в следующем виде:

$$Tr(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \ldots + \alpha^{2^{m-1}}.$$

Алгоритм 7. Вычисление следа элемента поля $\mathbf{GF}\left(2^m\right)$.

Вход: $\alpha \in \mathbf{GF}\left(2^m\right)$.

Выход: $t = \mathrm{Tr}(\alpha)$, $\mathrm{Tr}(\alpha) \in \{0,1\}$.

1. $t \leftarrow \alpha$.

2. For $i \leftarrow 1$, $i < m$, $i{+}{+}$ do

2.1. $t \leftarrow t^2 + \alpha$.

3. Return (t).

Алгоритм 8 [10] вычисления полу-следа элемента поля $\mathbf{GF}\left(2^m\right)$, основывается на том факте, что если m - нечетное, то полу-след можно представить в следующем виде:

$$\mathrm{HfTr}(\alpha) = \alpha + \alpha^2 + \alpha^{2^4} + \ldots + \alpha^{2^{m-1}}.$$

Алгоритм 8. Вычисление полу-следа элемента поля $\mathbf{GF}\left(2^m\right)$.

Вход: $\alpha \in \mathbf{GF}\left(2^m\right)$.

Выход: $H = \mathrm{HfTr}(\alpha)$.

1. $h \leftarrow \alpha$.

2. For $i \leftarrow 0$, $i \le ((m-1)/2)$, $i++$ do

2.1. $h \leftarrow h^2$.

2.1. $h \leftarrow h^2 + \alpha$.

3. Return (h).

Следующим алгоритмом, используемым при поиске бирациональных эквивалентных кривых, является алгоритм решения квадратного уравнения над полем $\mathbf{GF}(2^m)$. Согласно [10], известно, что если m-нечетное, тогда решением квадратного уравнения (8) является $z = \mathrm{HfTr}(\beta)$. Пусть $\beta \in \mathbf{GF}(2^m)$, тогда квадратное уравнение можно представить в виде, где $\beta \neq 0$.

$$z^2 + z = \beta. \tag{9}$$

После получения z, необходимо проверено тождество $\beta \equiv z^2 + z$. Если тождество выполняется, тогда z - решение уравнения, в противном случае - уравнение не имеет решений.

Поиск бирационально эквивалентных кривых Эдвардса

Для поиска бирациональных кривых Эдвардса среди рекомендованных ЭК из ДСТУ 4145-2002, предлагается:

1. Отбросить все кривые, для которых условие $\mathrm{Tr}(a_2^6/b) = 0$ не выполняется. Необходимость этого этапа обусловлена, возможностью существенно уменьшить объемы вычислений до получения результата об отсутствии эквивалентной кривой.

2. Получить бирациональные кривые Эдвардса.

3. Отобразить рекомендованные [13] базовые точки на кривой Вейерштрасса на кривую Эдвардса.

Для выполнения поиска, авторами была разработана программная реализация в среде Wolfram Mathematica 8.0, которая позволила провести экспериментальные исследования и получить эквивалентные кривые и базовые точки. В основу был положен модифицированный Алгоритм 3, поиска бирационально эквивалентных кривых Эдвардса. Наряду с хорошо известными вспомогательными алгоритмами 4, 7 и 8 был использован модифицированный Алгоритм 6 извлечения кубического корня на основе декомпозиции показателя степени в аддитивные цепочки.

В процессе эксперимента, авторами было проверено условие $\mathrm{Tr}(a_2^6/b) = 0$ для всех рекомендованных кривых [13]. Указанное условие соблюдаются лишь для ЭК: $\mathrm{m163(PB)}$, $\mathrm{m173(PB)}$, $\mathrm{m179(PB)}$, $\mathrm{m257(PB)}$, $\mathrm{m307(PB)}$. Отметим, что в экспериментах элементы поля $\mathbf{GF}(2^m)$ представлены в полиномиальном базисе.

Результаты поиска бирациональных кривых, приведены в Таблице 2, с соответствующими параметрами кривых Эдвардса и Вейерштрасса в полиномиальном базисе. Учитывая тот факт, что для криптографических преобразований на ЭК представляют интерес не только сами кривые, но и соответствующие базовые точки – генераторы группы, которые принадлежат этим ЭК, то для рекомендованных точек [13] в полиномиальном базисе, были полученные эквивалентные им на кривых Эдвардса.

Таблица 2. Эквивалентное преобразование кривых Вейерштрасса к кривым Эдвардса

Параметры кривой Вейерштрасса	**Параметры кривой Эдвардса**
m163(PB) (163,3,6,7)	
A=1; B=5FF6108462A2DC8210AB403925E638A19C1455D21; n=4000000000000000000002BEC12BE2262D39BCF14D;	d1=2cfd2b5ee202a45ddd703a5613477654ce1856a21; d2=619b17743b13c8c2bf09172fd478da4f5f68ba16c;
X=2E2F85F5DD74CE983A5C4237229DAF8A3F35823BE; Y=3826F008A8C51D7B95284D9D03FF0E00CE2CD723A;	X=6b57cccdeecfc90122f4d9a06c8a286a9d759ff9; Y=67168b7dec6c2cd9c0b876c9b36af475c1cdcfc3a;
m173(PB) (173,10,2)	
A=0; B=108576C80499DB2FC16EDDF6853BBB278F6B6FB437D9; n=800000000000000000000189B4E67606E38	d1=1270c0a05cefab3de162c3b30cdddedaff4004562137; d2=1f46525dd9dfb37dee43908b5e72ff2553

25BB2831;	afeee83ed8;
X=4D41A619BCC6EADF0448FA22FAD567A9181D37389CA; Y=10B51CC12849B234C75E6DD2028BF7FF5C1CE0D991A1;	X=bf95ca3e0df1a8ffa6a12a0936b7a78f324268df4a0; Y=19e7c368876e79c903ad174f5b6b7abaf61eb197dbe0;
m179(PB) (179,1,2,4)	
A=1; B=4A6E0856526436F2F88DD07A341E32D04184572BEB710; n=3FFFFFFFFFFFFFFFFFFFFB981960435FE5AB64236EF;	d1=227e1b7649d10d207a03739a67521c21e3155f47fbbc7; d2=2cfb3e893554615aabb20e7e185fad537c6d54c0239db;
X=6BA06FE51464B2BD26DC57F48819BA9954667022C7D03; Y=25FBC363582DCEC065080CA8287AAFF09788A66DC3A9E;	X=2891a5f263a7f8efa5f01a7215ec0c207e8d43f5d5f72; Y=7e9c20eeb83176d7b73b638a15e8c7f495b0bbb680dd5;
m257(PB) (257,12,0,0)	
A=0; B=1CEF494720115657E18F938D7A7942394FF9425C1458C57861F9EEA6ADBE3BE10; n=800000000000000000000000000000006759213AF182E987D3E17714907D470D;	d1=651a38e75ae7b53003eed5d73b31f23f184f8b110b129d92bd8a3f1c546e05fb; d2=18342b0dd40458381aa4781266bf1c3846ff148e6a75501f0bb9a9c7c8abcf7bf;
X=02A29EF207D0E9B6C55CD260B306C7E007AC491CA1B10C62334A9E8DCD8D20FB7; Y=10686D41FF744D4449FCCF6D8EEA03102E6812C93A9D60B978B702CF156D814EF;	X=1f40e77c3aec15fc99ccc4f5e8e87da77c1962973f18d64f1b9298daa46d8b9b3; Y=19ab0c6021428d9eff6a0368946041f3e0123f80ff8d86b5c4e0bb35b8b0b794;
m307(PB) (307,2,4,8)	
A=1; B=393C7F7D53666B5054B5E6C6D3DE94F4296C0C599E2E2E241050DF18B6090BDC90186904968BB; n=3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFC079C2F3825DA70D390FBBA588D4604022B7B7;	d1=5793a5de88e69b4b020ffc634d7b34ab416a70abc280aed0f17dd3fbf9d75796672667563c5c3; d2=66ffa0440824ef471a25f2917f3530575cfdf6151b5b13f41b63e358e163e971b340df0133cf9;
X=216EE8B189D291A0224984C1E92F1D16BF75CCD825A087A239B276D3167743C52C02D6E7232AA; Y=5D9306BACD22B7FAEB09D2E049C6E2866C5D1677762A8F2F2DC9A11C7F7BE8340AB2237C7F2A0;	X=5d910361c2486822bfea48b0af814c53212caf8801f3a7e215c029e6a031df755a882ed3c7bff; Y=64de21ef9c219bc1ebf144fced52d57592819a95f4b2d5380e664d6c18633a78c71c1869a8654;

Выводы

В результате проведения исследований, авторами была достигнута поставленная цель – разработан модифицированный алгоритм поиска бирационально эквивалентных кривых Эдвардса для кривых Вейерштрасса, найдены бирационально эквивалентные ЭК в форме Эдвардса для рекомендованных ДСТУ 4145-2002 ЭК в форме Вейерштрасса:

1. Для поиска эквивалентных кривых Эдвардса, были проанализированы известные алгоритмы, на основе которых, авторами была предложена собственная модификация, в которой были использованы известные алгоритмы извлечения квадратного корня, кубического корня, решения квадратного уравнения, вычисления следа и полуследа для элементов поля $\mathbf{GF}\left(2^m\right)$, где m - нечетное.

2. Для быстрого возведения в степень при вычислении кубического корня, предложена модификация алгоритма возведения в степень $\sum_{j=0}^{(m-1)/2} 2^{2\cdot j}$ посредством разложения показателя степени в аддитивную цепочку. Предложенная модификация позволяет значительно уменьшить количество операций умножения и возведения в степень, тем самым повысить скорость вычисления кубического корня.

3. Для проведения эксперимента по поиску эквивалентных кривых, была разработана программная реализация в среде Wolfram Mathematics 8.0 предложенного Алгоритма 3.

4. С использованием программной реализации, были проанализированы кривые, представленные в стандарте ДСТУ 4145-2002 с расширением поля $m \in \{163, 167, 173, 179, 191, 233, 257, 307, 367, 431\}$, среди

которых лишь для ЭК над полем $\mathbf{GF}\left(2^m\right)$, $m \in \{163, 173, 179, 257, 307\}$ было найдено бирациональные отображения в кривые Эдвардса, для остальных кривых такое отображение отсутствует.

5. Для найденных кривых Эдвардса над полем $\mathbf{GF}\left(2^m\right)$, $m \in \{163, 173, 179, 257, 307\}$ были получены базовые точки эквивалентные рекомендованным [13].

6. Использование найденных параметров кривых Эдвардса позволят повысить скорость скалярного умножения точек ЭК и, как следствие, повысить скорость постановки и проверки ЭЦП согласно ДСТУ 4145-2002 [1] и ECDSA [10]. Применение кривых Эдвардса позволяет упростить программные и аппаратные реализации соответствующих процедур, описанных в ДСТУ 4145-2002, по сравнению с ЭК в форме Вейерштрасса.

Дальнейшее направление исследований будет посвящено эффективной программной реализации криптографических преобразований согласно ДСТУ 4145-2002 с использованием найденных бирационально эквивалентных кривым Эдвардса $\mathrm{m163(PB)}$, $\mathrm{m173(PB)}$, $\mathrm{m179(PB)}$, $\mathrm{m257(PB)}$, $\mathrm{m307(PB)}$.

Список используемых источников

[1]. ДСТУ 4145-2002 «Криптографическая защита информации. Цифровая подпись основанная на эллиптических кривых».

[2]. Kovtun V.Y., Tevyashev A.D., Zbitnev S.I. Algorithms of scalar multiplication in group of elliptic curve points and some of their modifications. // Radiotekhnika: Vseukrainskiy mezhvedomstvenniy nauchno-tekhnicheskiy sbornik. – 2005. –Vol. 141. – Kharkov. -pp. 82–96. In Russian.

[3]. Daniel J. Bernstein, Tanja Lange. Analysis and optimization of elliptic-curve single-scalar multiplication. // Pages 1–19 in Finite fields and applications, edited by Gary L. Mullen, Daniel Panario, Igor E. Shparlinski. Contemporary Mathematics 461, American Mathematical Society, 2008.

[4]. Moloney, R., O'Mahony, A., Laurent, P. Efficient Implementation of Elliptic Curve Point Operations Using Binary Edwards Curves // IACR Cryptology ePrint Archive. –No 208. -2010. URL: http://eprint.iacr.org/2010/208.pdf

[5]. Kwang Ho Kim, Chol Ok Lee, Christophe Negre. Binary Edwards Curves Revisited // Lecture Notes in Computer Science Volume 8885, 2014, pp 393-408.

[6]. Daniel J. Bernstein, Tanja Lange and R. Farashahi. Binary Edwards Curves // Lecture Notes In Computer Science. // Proceedings of the 10th international workshop on Cryptographic Hardware and Embedded Systems, CHESS 2008, vol. 5154,pp. 244-265, 2008.

[7]. Daniel J. Bernstein. Batch Binary Edwards // In Advances in Cryptology – Proceedings of CRYPTO 2009, pp. 317-336, 2009.

[8]. Ming Li; Ali Miri; Daming Zhu. Fast Algorithm for Converting Ordinary Elliptic Curves into Binary Edward Form. // International Journal of Digital Content Technology & its Applications . Jan2012, Vol. 6 Issue 1, p405-412. 8p.

[9]. Paulo S. L. M. Barreto, José Felipe Voloch. Efficient Computation of Roots in Finite Fields. // Designs, Codes and Cryptography. May 2006, Volume 39, Issue 2, pp 275-280.

[10]. IEEE P1363-2000. Standard Specifications for Public Key Cryptography.

[11]. Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange and Christiance Peters. Twisted Edwards curves // In: Vaudenay, S. (ed.), Proceedings of AFRICACRYPT 2008, LNCS, vol. 5023, pp. 389-405, Springer, Heidelberg 2008.

[12]. Daniel J. Bernstein and Tanja Lange. Inverted Edwards coordinates. In Proceedings of AAECC 2007, pp. 20-27, 2007.

[13]. Requirements to object identifiers structure for government standards cryptoalgorithms. Ministry of Justice Of Ukraine. Departmental order from 20.08.2012, #1236/5/453. In Ukraine. URL: http://zakon2.rada.gov.ua/laws/show/z1398-12

[14]. M. Bluhm. Software optimization of binary elliptic curves arithmetic using modern processor architectures. // Department of Mathematics, University of Haifa. Embedded Security Group, Ruhr University Bochum. June 17, 2013.

[15]. Vladislav Kovtun, Mariya Kovtun, Sergey Gnatyuk. Hi-speed Multiplicative Inversion in Binary Fields for DSTU 4145-2002 // Preprint. URL:

[16]. S. M¨uller. On the computation of square roots in finite fields. // Designs, Codes and Cryptography, 31, pp. 301 – 312, 2004.

[17]. Javad Doliskani and Éric Schost. Taking roots over high extensions of finite fields. // Mathematics of Computation. 83 (2014), 435-446.

[18]. Dong-Guk Han, Dooho Choi, Howon Kim. Improved Computation of Square Roots in Specific Finite Fields. // IEEE Transactions on Computers (Impact Factor: 1.47). 02/2009; 58:188-196.