УДК 004.051/056 Гнатюк С.А., Ковтун В.Ю., Ковтун М.Г. (НАУ)

Ускоренное мультипликативное инвертирование в двоичном поле для ДСТУ 4145-2002

Аннотация: В работе авторы представляют модифицированные алгоритмы мультипликативного инвертирования Ито-Тцуджи для двоичных полей приведенных в ДСТУ 4145-2002 и рекомендованных Госспецсвязью Украины. Предложенная модификация позволяет на современных процессорах с поддержкой специальных инструкций CLMUL, существенно повысить производительность операций с ЭЦП согласно ДСТУ 4145-2002.

Ключевые слова: защита информации, эллиптическая кривая, ДСТУ 4145-2002, электронная цифровая подпись, конечные поля, алгоритм инвертирования Ито-Тцуджи.

В современном глобальном мире большую роль играет время реакции на те или иные события, разворачивающиеся в его отдаленных уголках. Другими словами, скорость передачи информации и ее обработка становится одним из наиболее приоритетных задач в современных автоматизированных системах управления. Однако не следует забывать и о злоумышленниках, желающих нарушить контур управления. В связи с чем, в современных автоматизированных системах управления важную роль играет система защиты информации, причем на подсистему криптографической защиты информации ложится задача обеспечения конфиденциальности, целостности, авторства, аутентичности и т. д. информации. Указанные задачи могут быть успешно решены с помощью криптографических преобразований с открытым ключом: выработки общего секрета, электронной цифровой подписи (ЭЦП).

В Украине действует Закон «Об электронной цифровой подписи» [6] и национальный стандарт ЭЦП ДСТУ 4145-2002 [4] «Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых».

Не смотря на высокую эффективность алгоритмов формирования и проверки ЭЦП, в связи с ростом объемов обрабатываемой информации, актуальность быстродействия этих операций не вызывает сомнения. Стойкость и скорость преобразований зависит от длины ключа, т.к. от двоичной длины элементов базового поля $\mathbf{GF}(2^m)$ – степени расширения m.

В самом стандарте ДСТУ 4145-2002 приводится большое число полей $\mathbf{GF}(2^m)$, однако регулятор в области защиты информации – Госспецсвязь Украины, дала соответствующие рекомендации в виде приказа от 20.08.2012 № 1236/5/453 [3]: $\mathbf{GF}(2^m)$, $m \in \{163, 173, 179, 191, 233, 257, 307, 367, 431\}$.

<table>
<tr><td>Криптопреобразования</td><td colspan="3">Зашифровывание/ расшифровывание</td><td colspan="3">Формирование и проверка цифровой подписи</td><td colspan="2">Обмен ключами</td></tr>
<tr><td rowspan="2">Арифметика в группе точек эллептической кривой</td><td colspan="6">Скалярное умножение точек эллиптической кривой</td><td colspan="2" rowspan="2">Генерация случайной точки</td></tr>
<tr><td colspan="4">Сложение точек</td><td colspan="2">Удвоение точки</td></tr>
<tr><td>Арифметика в поле GF(p), GF(2^m)</td><td>Умножение</td><td>Сложение</td><td>Деление</td><td colspan="2">Возведение в квадрат</td><td>Приведение по модулю</td><td>Инвертирование</td><td>Извлечения квадратного корня</td></tr>
<tr><td>Операции над массивами</td><td colspan="2">Сдвиг</td><td colspan="2">Сравнение</td><td>Сложение</td><td>Вычитание</td><td colspan="2">Умножение</td></tr>
<tr><td>Команды CPU</td><td colspan="8">mov, mul, shr, shl, add, sub</td></tr>
</table>

Рис. 1. Иерархия операций при выполнении криптографических преобразований на ЭК

На рис. 1 показана иерархия операций при выполнении криптографических преобразований на ЭК. Проведенный анализ показал, что среди операций в поле $\mathbf{GF}(2^m)$, наиболее трудоемкой операцией является мультипликативное инвертирование. В связи с этим, авторы сосредоточились на задаче повышения производительности именно операции мультипликативного инвертирования в поле $\mathbf{GF}(2^m)$.

Анализ исследований в области мультипликативного инвертирования в $\mathbf{GF}(2^m)$, позволил выделить следующие алгоритмы:

1. Расширенный алгоритм Евклида (РАЕ) [8][5].

2. Алгоритмы на основе свойства циклических групп – теорема Лагранжа. Алгоритм Ито-Тцуджи (ИТА) [1] принадлежит именно к этому классу.

Предыдущие исследования [5] были посвящены переносимой эффективной реализации РАЕ, в которой показан значительный выигрыш РАЕ над ИТА. Однако анонс в 2010 и выход в 2012 году процессоров Intel Westmere нового поколения, поддерживающих специальную инструкцию CLMUL (умножение в поле $\mathbf{GF}(2^m)$) позволил сделать более привлекательным именно ИТА для вычислительных систем на современных процессорах Intel. С выходом процессоров Intel Haswell, с существенно оптимизированной инструкцией CLMUL, эффективность ИТА стала бесспорной [7].

В связи с этим, представляет интерес в оптимизации ИТА для полей $\mathbf{GF}(2^m)$ рекомендованных Госспецсвязью Украины.

Алгоритм мультипликативного инвертирования ИТА

Особенность цикличных групп, которые используются в мультипликативной инверсии базируются на теореме Лагранжа. Теорема утверждает, что порядок каждой подгруппы H и любой конечной группы G делит порядок группы; порядок любого элемента также делит порядок группы. Порядком элемента a является наименьшее целое число n, что удовлетворяет условие $a^n = e$, где e - единица группы. Таким образом, для любого члена a циклической группы G, следует что $a^{|G|} = e$ и $a^{|G|-1} = a^{-1}$. Таким образом, обратный элемент $a(x) \in \mathbf{GF}(2^m)$ может быть вычислен следующим образом

$$a^{-1}(x) = a^{2^m-2}(x) = \left(a^2\right)^{2^{m-1}-1}(x) \bmod f(x) \quad (1)$$

Впервые, ИТА использовался для полей $\mathbf{GF}(2^m)$, с оптимальным нормальным базисом представления элементов. Алгоритм носит общий характер и может быть использован для других базисов, в том числе и полиномиальный. Существует и обобщенная версия алгоритма для полей $\mathbf{GF}(p^m)$.

Наиболее трудоемкой, с вычислительной точки зрения, является операция возведения в степень. Это одна из причин, почему ИТА хорошо подходит для нормального базиса, поскольку возведения в квадрат и возведения в степень относительно быстрые. С появлением специальных инструкций CLMUL для умножения полиномов, стало возможно применение алгоритма ИТА и для полиномиального базиса.

Декомпозиция порядка группы

Перейдем к более подробному рассмотрению декомпозиции порядка группы. Пускай $a(x), b(x) \in \mathbf{GF}(2^m)$. Из уравнения (1) следует:

$$a^{-1}(x) = \left(a^2\right)^{2^{m-1}-1}(x) = b^{2^{m-1}-1}(x) = b^{1+2+2^2+\ldots+2^{m-2}} \bmod f(x) \quad (2)$$

где каждый «+» в степени b, по сути, является умножением. Таким образом, задача состоит в том, чтобы найти разложение цепи $1+2^1+2^2+\ldots+2^{2^{m-2}}$ с наименьшим количеством операций умножения. Общая рекурсивная формула для получения цепочки может быть задана как [2]:

$$1+2^n+2^{2n}+\ldots+2^{(k-2)n} = \begin{Bmatrix} \left(1+2^n\right)\times\left(1+2^{2n}+\ldots 2^{(k-3)n}\right) & | \text{k -1} \equiv 0 \bmod 2 \\ 1+2^{\text{n}}\times\left(1+2^n\right)\times\left(1+2^{2n}+\ldots+2^{(k-4)n}\right) & | \text{k -1} \equiv 1 \bmod 2 \end{Bmatrix} \quad (3)$$

В таблице 1 представлены следующие разложения для полей с рекомендованных Госспецсвязью.

Таблица 1. Декомпозиция в поле $\mathbf{GF}(2^m)$

Поле	Декомпозиция
$\mathbf{GF}(2^{163})$	$(1+2)(1+2^2(1+2^2)(1+2^4)(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})))$
$\mathbf{GF}(2^{167})$	$(1+2)(1+2^2(1+2^2)(1+2^4(1+2^4)(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}))))$
$\mathbf{GF}(2^{173})$	$(1+2)(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}))))$
$\mathbf{GF}(2^{179})$	$(1+2)(1+2^2(1+2^2)(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}))))$
$\mathbf{GF}(2^{191})$	$(1+2)(1+2^2(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})))))$
$\mathbf{GF}(2^{233})$	$(1+2)(1+2^2)(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}(1+2^{64}))))$
$\mathbf{GF}(2^{257})$	$(1+2)(1+2^2)(1+2^4)(1+2^8)(1+2^{16})(1+2^{32})(1+2^{64})(1+2^{128})$
$\mathbf{GF}(2^{307})$	$(1+2)(1+2^2(1+2^2)(1+2^4)(1+2^8)(1+2^{16}(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})(1+2^{128}))))$
$\mathbf{GF}(2^{367})$	$(1+2)(1+2^2(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64}(1+2^{64})(1+2^{128})))))$
$\mathbf{GF}(2^{431})$	$(1+2)(1+2^2(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})(1+2^{128}(1+2^{128})(1+2^{256}))$

Для большей наглядности, рассмотрим более подробно два примера декомпозиций цепочки с наименьшим числом умножений.

Пример 1. Для поля $\mathbf{GF}(2^{173})$.

Известно, $k=173$, тогда согласно (3), .разложение цепи будет иметь вид $1+2^1+2^2+\ldots+2^{(173-2)\cdot 1}$. В Таблица 2 приводятся все итерации рекурсивного формирования цепочки.

Таблица 2. Пример декомпозиции для поля $\mathbf{GF}(2^{173})$

№ итер.	Цепь	Параметры	Условие
1	$1+2^1+2^2+\ldots+2^{(173-2)\cdot 1}$	$k=173, n=1$	$k-1\equiv 0 \bmod 2$
2	$(1+2)(1+2^2+\ldots+2^{(173-3)\cdot 1})$	$k=87,\ n=2$	$k-1\equiv 0 \bmod 2$
3	$\ldots(1+2^2)(1+2^4+\ldots+2^{(87-3)\cdot 2})$	$k=44,\ n=4$	$k-1\equiv 1 \bmod 2$
4	$\ldots(1+2^4(1+2^4)(1+2^8+\ldots+2^{(44-4)\cdot 4}))$	$k=22,\ n=8$	$k-1\equiv 1 \bmod 2$
5	$\ldots(1+2^8(1+2^8)(1+2^{16}+\ldots+2^{(22-4)\cdot 8}))$	$k=11,\ n=16$	$k-1\equiv 0 \bmod 2$
6	$\ldots(1+2^{16})(1+2^{32}+\ldots+2^{(11-3)\cdot 16})$	$k=6,\ n=32$	$k-1\equiv 1 \bmod 2$
7	$\ldots(1+2^{32}(1+2^{32})(1+2^{64}))$		

Таким образом декомпозиция цепочки может быть представлена следующим образом:

$1+2^1+2^2+\ldots+2^{(173-2)\cdot 1}=$
$(1+2)(1+2^2)(1+2^4(1+2^4)(1+2^8(1+2^8)(1+2^{16})(1+2^{32}(1+2^{32})(1+2^{64})))).$

Пример 2. Для поля $\mathbf{GF}(2^{431})$.

Известно, $k=431$, тогда согласно (3), .разложение цепи будет иметь вид $1+2^1+2^2+\ldots+2^{(431-2)\cdot 1}$. В Таблица 3 приводятся все итерации рекурсивного формирования цепочки.

Таблица 3. Пример декомпозиции для поля $\mathbf{GF}(2^{431})$

№ итер.	Цепь	Параметры	Условие
1	$1+2^1+2^2+\ldots+2^{(431-2)\cdot 1}$	$k=431, n=1$	$k-1\equiv 0 \bmod 2$
2	$(1+2)(1+2^2+\ldots+2^{(431-3)\cdot 1})$	$k=216,\ n=2$	$k-1\equiv 1 \bmod 2$

3	$\ldots\left(1+2^2\left(1+2^2\right)\left(1+2^4+\ldots+2^{(216-4)\cdot 2}\right)\right)$	$k=108,\ n=4$	$k-1\equiv 1 \bmod 2$
4	$\ldots\left(1+2^4\left(1+2^4\right)\left(1+2^8+\ldots+2^{(108-4)\cdot 4}\right)\right)$	$k=54,\ n=8$	$k-1\equiv 1 \bmod 2$
5	$\ldots\left(1+2^8\left(1+2^8\right)\left(1+2^{16}+\ldots+2^{(54-4)\cdot 8}\right)\right)$	$k=27,\ n=16$	$k-1\equiv 0 \bmod 2$
6	$\ldots\left(1+2^{16}\right)\left(1+2^{32}+\ldots+2^{(27-3)\cdot 16}\right)$	$k=14,\ n=32$	$k-1\equiv 1 \bmod 2$
7	$\ldots\left(1+2^{32}\left(1+2^{32}\right)\left(1+2^{64}+\ldots+2^{(14-4)\cdot 32}\right)\right)$	$k=7,\ n=64$	$k-1\equiv 0 \bmod 2$
8	$\ldots\left(1+2^{64}\right)\left(1+2^{128}+2^{(7-3)\cdot 64}\right)$	$k=4,\ n=128$	$k-1\equiv 1 \bmod 2$
9	$\ldots\left(1+2^{128}\left(1+2^{128}\right)\left(1+2^{256}\right)\right)$		

Таким образом декомпозиция цепочки может быть представлена следующим образом:

$1+2^1+2^2+\ldots+2^{(431-2)\cdot 1}=$
$(1+2)\left(1+2^2\left(1+2^2\right)\left(1+2^4\left(1+2^4\right)\left(1+2^8\left(1+2^8\right)\left(1+2^{16}\left(1+2^{32}\left(1+2^{32}\right)\left(1+2^{64}\left(1+2^{128}\left(1+2^{128}\right)\left(1+2^{256}\right)\right)\right)\right)\right)\right)\right)\right)$

Ранее описанные декомпозиции, позволили разработать авторами соответствующие алгоритмы инвертирования для рекомендованных полей.

Алгоритм 1. Инверсия в поле $\mathbf{GF}\left(2^{163}\right)$.

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

Выход: $a^{-1}(x)=a^{2^{m-1}-1}$

1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$.
3. $t_1 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.
5. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.
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. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_1$.
13. **return** $t_0 = a^{-1}(x)$.

Алгоритм 2. Инверсия в поле $\mathbf{GF}\left(2^{167}\right)$.

Вход: $a(x)\in \mathbf{GF}\left(2^{167}\right)$.

Выход: $a^{-1}(x)=a^{2^{m-1}-1}$

1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$.
3. $t_1 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.
5. $t_2 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.
7. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$.
9. $t_3 \leftarrow t_0$.
10. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.
12. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_3$.
13. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_2$.
14. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_1$.
15. **return** $t_0 = a^{-1}(x)$.

Алгоритм 3. Инверсия в поле $\mathbf{GF}\left(2^{173}\right)$.

Вход: $a(x)\in \mathbf{GF}\left(2^{173}\right)$.

Выход: $a^{-1}(x)=a^{2^{m-1}-1}$

1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$. $t_1 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$. $t_2 \leftarrow t_0$
5. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.

Алгоритм 4. Инверсия в поле $\mathbf{GF}\left(2^{179}\right)$.

Вход: $a(x)\in \mathbf{GF}\left(2^{179}\right)$.

Выход: $a^{-1}(x)=a^{2^{m-1}-1}$

1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$. $t_1 \leftarrow t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.
5. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$. $t_2 \leftarrow t_0$.

6. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$. $t_3 \leftarrow t_0$.
7. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.
9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_3$.
10. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_2$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_1$.
12. **return** $t_0 = a^{-1}(x)$.

Алгоритм 5. Инверсия в поле $\mathbf{GF}\left(2^{191}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{191}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^{1} \times t_0$. $t_1 \leftarrow t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_0$. $t_2 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_0$. $t_3 \leftarrow t_0$.
5. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_0$. $t_4 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$. $t_5 \leftarrow t_0$.
7. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.
9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_5$.
10. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_4$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_3$.
12. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_2$.
13. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_1$.
14. **return** $t_0 = a^{-1}(x)$.

Алгоритм 6. Инверсия в поле $\mathbf{GF}\left(2^{233}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{233}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^{1} \times t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_0$.
5. $t_1 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_0$.
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. $t_3 \leftarrow t_0$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.
12. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_3$.
13. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_2$.
14. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_1$.
15. **return** $t_0 = a^{-1}(x)$.

Алгоритм 7. Инверсия в поле $\mathbf{GF}\left(2^{257}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{257}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^{1} \times t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_0$.
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. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.

Алгоритм 8. Инверсия в поле $\mathbf{GF}\left(2^{307}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{307}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^{1} \times t_0$. $t_1 \leftarrow t_0$.
3. $t_0 \leftarrow \left(t_0^{\,2}\right)^{2} \times t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^{4} \times t_0$.
5. $t_0 \leftarrow \left(t_0^{\,2}\right)^{8} \times t_0$. $t_2 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$. $t_3 \leftarrow t_0$.
7. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.

9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{128} \times t_0$.
10. **return** $t_0 = a^{-1}(x)$.

Алгоритм 9. Инверсия в поле $\mathbf{GF}\left(2^{367}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{367}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$.
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$.
3. $t_1 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.
5. $t_2 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.
7. $t_3 \leftarrow t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.
9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$.
10. $t_4 \leftarrow t_0$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
12. $t_5 \leftarrow t_0$.
13. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$.
14. $t_0 \leftarrow \left(t_0^{\,2}\right)^{128} \times t_0$.
15. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_5$.
16. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_4$.
17. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_3$.
18. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_2$.
19. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_1$.
20. **return** $t_0 = a^{-1}(x)$.

9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{128} \times t_0$.
10. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_3$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_2$.
12. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_1$.
13. **return** $t_0 = a^{-1}(x)$.

Алгоритм 10. Инверсия в поле $\mathbf{GF}\left(2^{431}\right)$.
Вход: $a(x) \in \mathbf{GF}\left(2^{431}\right)$.
Выход: $a^{-1}(x) = a^{2^{m-1}-1}$
1. $t_0 \leftarrow a^2$.
2. $t_0 \leftarrow \left(t_0^{\,2}\right)^1 \times t_0$.
3. $t_1 \leftarrow t_0$.
4. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_0$.
5. $t_2 \leftarrow t_0$.
6. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_0$.
7. $t_3 \leftarrow t_0$.
8. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_0$.
9. $t_0 \leftarrow \left(t_0^{\,2}\right)^{16} \times t_0$.
10. $t_4 \leftarrow t_0$.
11. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_0$.
12. $t_0 \leftarrow \left(t_0^{\,2}\right)^{64} \times t_0$. $t_5 \leftarrow t_0$.
13. $t_0 \leftarrow \left(t_0^{\,2}\right)^{128} \times t_0$.
14. $t_0 \leftarrow \left(t_0^{\,2}\right)^{256} \times t_0$.
15. $t_0 \leftarrow \left(t_0^{\,2}\right)^{128} \times t_5$.
16. $t_0 \leftarrow \left(t_0^{\,2}\right)^{32} \times t_4$.
17. $t_0 \leftarrow \left(t_0^{\,2}\right)^8 \times t_3$.
18. $t_0 \leftarrow \left(t_0^{\,2}\right)^4 \times t_2$.
19. $t_0 \leftarrow \left(t_0^{\,2}\right)^2 \times t_1$.
20. **return** $t_0 = a^{-1}(x)$.

Количество машинных циклов для операций инвертирования, для процессора Intel Core i7-3770 полученных авторами с помощью компилятора gcc 4.7.0 представлены в таблице 4.

Таблица 4. Количество машинных циклов для операций инвертирования

Поле	Инверсия	Поле	Инверсия
$\mathbf{GF}\left(2^{163}\right)$	4,811	$\mathbf{GF}\left(2^{233}\right)$	6,956
$\mathbf{GF}\left(2^{167}\right)$	4,789	$\mathbf{GF}\left(2^{257}\right)$	6,814
$\mathbf{GF}\left(2^{173}\right)$	4,823	$\mathbf{GF}\left(2^{307}\right)$	9,732

$\mathbf{GF}(2^{179})$	4,834	$\mathbf{GF}(2^{367})$	10,345
$\mathbf{GF}(2^{191})$	4,785	$\mathbf{GF}(2^{431})$	15,876

Выводы

1. Проведенный анализ показал возможность применения алгоритма ИТА для инвертирования элементов поля $\mathbf{GF}(2^m)$ в полиномиальном базисе, поскольку в современных процессорах появились специальные инструкции умножения в поле $\mathbf{GF}(2^m)$.
2. Рассчитаны цепочки разложений пордяков рекомендованных полей $\mathbf{GF}(2^m)$ для алгоритма ИТА с наименьшим количеством операций умножения для эффективной программной реализации ДСТУ 4145-2002.
3. Разработаны алгоритмы мультипликативного инвертирования ИТА для рассчитанных цепочек разложения порядка поля $\mathbf{GF}(2^m)$.
4. Приведены результаты в машинних циклах программной реализации разработанных алгоритмов ИТА для соответствующих полей $\mathbf{GF}(2^m)$.

Литература

[1] T. Itoh and S. Tsujii, A fast algorithm for computing multiplicative inverses in $\mathbf{GF}(2^m)$using normal bases, Inf. Comput., 78 (1988), pp. 171–177.

[2] 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.

[3] Вимоги до структури об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами. Мін'юст України, Держспецзв'язку України; Наказ, Вимоги від 20.08.2012 № 1236/5/453. URL: http://zakon4.rada.gov.ua/laws/show/z1399-12.

[4] Національний стандарт України ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – К.: Держ. комітет України з питань технічного регулювання та споживчої політики, 2003.

[5] Ковтун В. Методы повышения производительности операции инвертирования в двоичном поле / В. Ковтун, М. Булах // Безпека інформації . - 2014. - Т. 20, № 1. - С. 55-61. - URL: http://nbuv.gov.ua/j-pdf/bezin_2014_20_1_11.pdf.

[6] Закон України від 22.05.2003 р. № 852-IV «Про електронний цифровий підпис».

[7] J. Maitin-Shepard: Optimal software-implemented Itoh-Tsujii inversion for $\mathbf{GF}(2^m)$. IACR Cryptology ePrint Archive 2015: 28 (2015).

[8] D. Hankerson, J. Hernandez, A. Menezes. Software implementation of Elliptic Curve Cryptography over binary fields. Proceedings of Workshop on Cryptographic Hardware and Embedded System. –LNCS 1965. –2000. –pp. 1-24.