На правах рукописи

Бурцев Алексей Анатольевич

СХЕМЫ ДЛЯ ЦЕЛОЧИСЛЕННОЙ АРИФМЕТИКИ И АРИФМЕТИКИ КОНЕЧНЫХ ПОЛЕЙ

01.01.09 – Дискретная математика и математическая кибернетика

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
кандидата физико-математических наук

Нижний Новгород – 2007

Работа выполнена на кафедре дискретной математики механико-математического факультета Московского государственного университета имени М. В. Ломоносова.

Научный руководитель:	доктор физико-математических наук, профессор С. Б. Гашков.
Официальные оппоненты:	доктор физико-математических наук, профессор В. М. Галкин;
	кандидат физико-математических наук, доцент Н. Ю. Золотых.
Ведущая организация:	Московский энергетический институт (МЭИ).

Защита диссертации состоится 13 декабря 2007 г. в 14 ч. 40 мин. на заседании диссертационного совета Д.212.166.06 в Нижегородском государственном университете имени Н. И. Лобачевского по адресу: 603950, Российская Федерация, г. Нижний Новгород, проспект Гагарина, 23, корпус 2, конференц-зал ННГУ.

С диссертацией можно ознакомиться в фундаментальной библиотеке Нижегородского государственного университета имени Н. И. Лобачевского. С текстом автореферата можно ознакомиться на официальном сайте ННГУ имени Н. И. Лобачевского http://www.unn.ru в разделе «Наука и инновации» - «Объявления о защите диссертаций» - «Физико-математические науки».

Автореферат разослан «__8__» «_____ноября_____» 2007 г.

Ученый секретарь
диссертационного совета
Д.212.166.06
кандидат физико-математических наук,
доцент В. И. Лукьянов

Общая характеристика работы

Актуальность темы

В данной работе изучается реализация арифметических операций в некоторых конечных полях схемами из функциональных элементов.

Конечные поля возникли в исследованиях Гаусса и Галуа. Современное изложение теории появилось в работах Мура и Диксона. Схемы для арифметических операций в конечных полях используются в криптографии, кодировании, цифровой передаче сигналов и других областях. В указанных применениях в основном использовались поля сравнительно малой размерности ($n \leq 32$), но с развитием криптографии с открытым ключом поля большой размерности ($n \geq 1000$) нашли применение в криптографических протоколах, основанных на предположении о трудности задачи дискретного логарифмирования[1,2]. Благодаря развитию криптографии на эллиптических кривых появилась возможность использовать поля размерности порядка двухсот[3,4].

Теория сложности схем для булевых функций была развита в работах К. Э. Шеннона и О. Б. Лупанова. Схемы обычно строятся из элементов, реализующих двухместные булевы функции. Под сложностью схемы понимается количество составляющих схему функциональных элементов. Понятие схемной сложности по существу совпадает с понятием битовой сложности. При конструировании логических схем стремятся уменьшить не только их сложность, но и глубину — максимальное число элементов в любой цепи, соединяющей входы схемы с её выходами, так как практически важно увеличить быстродействие схемы. Операции сложения и вычитания просты, поэтому наибольший интерес представляет умножение и инвертирование ненулевых элементов (инвертирование есть нахождение мультипликативного обратного). Деление сводится к инвертированию и умножению. Умножение элементов конечного поля в стандартном базисе сводится к умножению представляющих эти элементы многочленов по модулю некоторого неприводимого многочлена, поэтому существенное значение имеет разработка эффективных схем для умножения многочленов над конечными полями.

---

[1] Diffie W., Hellman M., *New directions in cryptography*, *IEEE Trans. Inform. Theory*, **IT-22**, (1976).

[2] Coppersmith D., *Fast evaluation of logarithms in fields of characteristic two*, *IEEE Trans.Inform.Theory*, **IT30**, 4,(1984), 587-594.

[3] Miller V., *Uses elliptic curves in cryptography* , *CRYPTO-85*, (1986), 417-426.

[4] Koblitz N., *Elliptic curve cryptosystems* , *Mathematics of computation*, 48 (1987), 203-209.

Цель работы

Получение эффективных верхних оценок сложности и глубины схем из двухвходовых булевых элементов для арифметики в некоторых башнях конечных полей, а также для умножения многочленов в некоторых конечных полях.

Основные методы исследования

В работе используются методы дискретной математики, математической кибернетики и алгебры, в частности, теории синтеза и сложности управляющих систем и теории конечных полей.

Научная новизна

Результаты диссертации являются новыми и состоят в следующем.

1. Показано, что для любых положительного ε и натурального $m > 1$ для любого $n = m^s$, где натуральное $s \geq s_\varepsilon$, можно указать в поле $GF(2^n)$ базис и построить схему умножения в нем сложности, не превосходящей $n^{1+\varepsilon/2}$ и схему инвертирования сложности, не превосходящей $n^{1+\varepsilon}$.

2. Показано, что при $n = 2 \cdot 3^k$ в поле $GF(2^n)$ можно указать базис, для которого можно построить схему для умножения сложности $M(n) = n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}$ и схему для инвертирования сложности $O(M(n))$.

3. Получены новые эффективные рекуррентные верхние оценки сложности и глубины схем из функциональных элементов для умножения и инвертирования в некоторых нормальных базисах полей $GF(2^{4n})$, $GF(2^{8n})$, $GF(2^{6n})$, при нечётном n и n, взаимно простом с 6, соответственно.

4. Построены новые эффективные схемы для умножения в полях вида $GF(7^{14n})$, НОД$(n, 14) = 1$. Построены новые эффективные схемы для умножения многочленов над $GF(7^2)$.

5. Получены новые эффективные рекуррентные верхние оценки сложности умножения в некоторых башнях конечных полей большой характеристики.

6. Получены новые эффективные рекуррентные верхние оценки сложности и глубины умножения и инвертирования в полях вида $GF(p^{2^k})$, $p = 2^{16} + 1$.

Теоретическая и практическая ценность

Работа носит теоретический характер. Построенная в ней схемная реализация арифметики в конечных полях может найти применение в кодировании, криптографии, цифровой обработке сигналов и других областях, а также может быть использована для программной реализации арифметических операций в конечных полях в компьютерной алгебре.

Апробация результатов

Результаты диссертации докладывались на научной конференции «Ломоносовские чтения» в Московском государственном университете имени М. В. Ломоносова (механико-математический факультет, кафедра дискретной математики) в апреле 2007 г., на научной конференции «Ломоносовские чтения» в Московском государственном университете имени М. В. Ломоносова (механико-математический факультет, кафедра дискретной математики) в апреле 2006 г., на VI молодёжной научной школе-семинаре «Дискретная математика и её приложения» (Москва, Институт прикладной математики им. М.В.Келдыша РАН) в апреле 2007 г., на IX Международном научном семинаре «Дискретная математика и её приложения» (Московский государственный университет имени М. В. Ломоносова, механико-математический факультет) в июне 2007 г., на Нижегородском городском научном семинаре «Дискретная математика и её приложения» (Нижегородский государственный университет имени Н. И. Лобачевского, факультет ВМК, кафедра математической логики и высшей алгебры) в октябре 2007 г.

Публикации

Основное содержание диссертации опубликовано в 5 работах [1-5], список которых приведен в конце автореферата. Работы [1-2] написаны в соавторстве. Автору диссертации принадлежат доказательства всех основных результатов. В работах [3-5] соавторов нет. Работы [1-3] опубликованы в журналах, рекомендованных ВАК для публикаций диссертационных материалов.

Структура и объем работы

Диссертация состоит из введения, четырёх глав и списка литературы. Полный объём диссертации составляет 128 страниц. Список литературы содержит 58 наименований.

Краткое содержание диссертации

Во **введении** излагается история вопроса, формулируются постановка задачи и основные цели работы, кратко описывается её содержание, а также вводятся основные обозначения.

Первая глава служит предисловием к основной тематике и посвящена оптимизации метода Карацубы[5] и некоторых случаев метода Тоома[6,7] для умножения n-битовых целых чисел с целью получения эффективных числовых оценок схемной сложности умножения для реально используемых на практике диапазонов изменения n. Методы синтеза схем для умножения целых чисел с некоторыми изменениями могут быть перенесены на умножение многочленов над конечными полями, что в свою очередь может быть использовано для эффективного схемного умножения элементов конечных полей.

Показано, что метод Карацубы умножения n-битовых чисел можно схемно реализовать с рекуррентной оценкой сложности

$$T(2n) \leq 3T(n) + 52n - 9.$$

Этот метод эффективнее школьного метода для всех $n \geq 16$. На каждом шаге рекурсии в нем n-битовые сомножители эффективно разбивать на блоки длины $\lceil \frac{n}{2} \rceil$ и $\lfloor \frac{n}{2} \rfloor$ бит. Сложность оптимизированного варианта метода Карацубы для $n = 2^s$, $s \geq 4$, оценивается сверху как

$$\frac{731{,}5}{27} \cdot n^{\log_2 3} - 52n + 4{,}5.$$

Приблизительно это вдвое лучше неоптимизированного варианта.

Показано, что метод Тоома умножения n-битовых чисел для $n = 4^s$, $s \geq 4$, можно схемно реализовать с рекуррентной оценкой сложности

$$T(4n) \leq 7T(n) + 662n + 1085.$$

[5] Карацуба А. А., Офман Ю. П. Умножение многозначных чисел на автоматах. // ДАН СССР. — 1962. — Т. 145(2). — С. 293–294.

[6] Тоом А.Л. О сложности схемы из функциональных элементов, реализующей умножение целых чисел // ДАН СССР. — 1963. — Т. 150. — С. 496–498.

[7] Кнут Д. Искусство программирования, т.2, 2-е изд., 2000.

Сложность оптимизированного варианта метода Тоома для $n = 4^s,\ s \geq 4$, оценивается сверху как

$$402{,}5n^{\log_4 7} - \frac{662}{3}n - \frac{1085}{6}.$$

Приблизительно это в 4,5 раза лучше неоптимизированного варианта. В частности, $T(1024) \leq 1\ 279\ 651$, а стандартный (школьный) метод умножения имеет оценку сложности выше шести миллионов.

Метод Тоома для $n = 8^s,\ s \geq 5$, можно схемно реализовать с рекуррентной оценкой сложности $T(8n) \leq 15T(n) + 5762n + 63589$. Сложность оптимизированного варианта метода Тоома для $n = 8^s$, $s \geq 5$, оценивается сверху как $257{,}05n^{\log_8 15} - 823n - 4542$. Это приблизительно в 21 раз лучше неоптимизированного варианта.

Во **второй главе** изучается сложность и глубина схем для арифметики в некоторых башнях конечных полей характеристики два. Методы умножения в конечных полях зависят от типа базисов, используемых для представления элементов поля. Чаще всего используются стандартные полиномиальные базисы, в которых элементы поля размерности n представляются в виде многочленов степени $n-1$, операции над которыми выполняются по модулю данного неприводимого многочлена. Очевидные оценки сложности и глубины таких схем равны $O(n^2)$, $O(\log n)$. Методом Карацубы можно для тех же базисов построить схемы сложности $O(n^{\log_2 3})$. Вопросы практического использования метода Карацубы для умножения в поле $GF(2^n)$ рассмотрены, в частности, в диссертации К.Паара[8]. Известно[9,10], что при использовании стандартных базисов в полях $GF(2^n)$ сложность схемы для умножения равна $O(n \log n \log\log n)$. Для инвертирования в компьютерных вычислениях можно использовать быстрый алгоритм Евклида[9] с оценкой сложности $O(n \log^2 n \log\log n)$. Однако мультипликативная константа в этой оценке велика (несколько сотен), и при актуальных для приложений значениях n стандартный алгоритм Евклида лучше. Кроме того, этот алгоритм затруднительно применить при построении схемы для инвертирования.

Во второй главе диссертации построены схемы для умножения и инвертирования в башнях конечных полей вида $GF(2^n)$, $n = m^s$. Далее приводятся формулировки результатов при помощи следующих обозначений: $L(M(n))$, $M(n)$ – сложность схемы для умножения, $L(I(n))$,

[8] C. Paar, *Effective VLSI architectures for bit paralel computation in Galois fields*, Ph. D. Thesis, Universität GH Essen, Germany, 1994.

[9] von zur Gathen J., Gerhard J. Modern computer algebra. Cambridge University Press, 1999.

[10] Schonhage A. Schnelle Multiplication von Polynomen ueber Koerpern der Charakteristik 2. Acta Informatica (1977), vol.7, 395-398.

$I(n)$ – сложность схемы для инвертирования, $L(S(n))$ – сложность схемы для возведения в квадрат, $D(M(n))$ – глубина схемы для умножения, $D(I(n))$ – глубина схемы для инвертирования, $D(S(n))$ – глубина схемы для возведения в квадрат в конечном поле $GF(2^n)$.

Теорема 2.1.1. *Для любого $\varepsilon > 0$ при любом m для $n = m^s$ и $s \geq s_\varepsilon$ можно указать в поле $GF(2^n)$ базис, для которого можно построить схему умножения сложности $M(m^s) < n^{1+\varepsilon/2}$, и схему инвертирования сложности $I(m^s) < n^{1+\varepsilon}$.*

Результаты этой теоремы в специальном случае $n = 2 \cdot 3^k$ усиливает следующая

Теорема 2.1.2. *При $n = 2 \cdot 3^k$ в поле $GF(2^n)$ можно указать некоторый базис, для которого можно построить схемы для умножения сложности $M(n) = n(\log_3 n)^{(\log_2 \log_3 n)/2+O(1)}$ и схемы для инвертирования сложности $I(n) = O(M(n))$.*

В работе[11] были указаны рекуррентные верхние оценки сложности и глубины схем для умножения и деления в некоторых базисах полей $GF(2^{4n})$, $GF(2^{6n})$ при нечетном n и n, взаимно простом с 6, соответственно. Во второй главе диссертации получены подобные оценки для схем в некоторых нормальных базисах тех же полей, а также для схем в некоторых базисах полей $GF(2^{8n})$ при нечетном n и некоторых других композитных полей. Далее приводятся формулировки полученных результатов (**теоремы 2.2.1 – 2.2.4**).

Для расширения $GF((2^n)^4)$ поля $GF(2^n)$ при нечетном n и выборе в поле $GF(2^4)$ нормального базиса

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8\}, \quad 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = 0,$$

и произвольного нормального базиса в поле $GF(2^n)$, можно построить схемы для умножения и инвертирования со следующими рекуррентными оценками сложности и глубины

$$L(M(4n)) \leq 10L(M(n)) + 21n, \quad D(M(4n)) \leq D(M(n)) + 3,$$

$$L(I(4n)) \leq L(I(n)) + 19L(M(n)) + 13n,$$
$$D(I(4n)) \leq 3D(M(n)) + 2 + \max\{D(I(n)), 2\}.$$

Можно также построить схемы для инвертирования с оценками

$$L(I(4n)) \leq L(I(n)) + 18L(M(n)) + 15n,$$

[11] Гашков С. Б., Хохлов Р. А. О глубине логических схем для операций в полях $GF(2^n)$. Чебышевский сборник, т. 4, вып. 4(8), 2003. С. 59-71.

$$D(I(4n)) \le 3D(M(n)) + 2 + \max\{D(I(n)), 3\}.$$

Для расширения $GF((2^n)^6)$ *поля* $GF(2^n)$*, где* n *взаимно просто с* 6*, при выборе в подполе* $GF(2^6)$ *нормального базиса*

$$\{\alpha, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}\}, \quad 1 + \alpha + \alpha^4 + \alpha^5 + \alpha^6 = 0,$$

и произвольного нормального базиса в поле $GF(2^n)$*, можно построить для умножения и инвертирования схемы со следующими рекуррентными оценками сложности и глубины*

$$L(M(6n)) \le 21L(M(n)) + 60n, \quad D(M(6n)) \le D(M(n)) + 4,$$

$$L(I(6n)) \le L(I(n)) + 42L(M(n)) + 65n,$$
$$D(I(6n)) = 4D(M(n)) + 4 + \max\{D(I(n)), 4\}.$$

В башне расширений $GF((((2^n)^2)^2))^2$ *поля* $GF(2^n)$ *при нечетном* n *можно выбрать базис так, что справедливы следующие рекуррентные оценки сложности и глубины умножения и возведения в квадрат:*

$$L(M(8n)) \le 27L(M(n)) + 80n, \quad D(M(8n)) \le D(M(n)) + 7,$$

$$L(S(8n)) \le 10n + 4L(S(n)), \quad D(S(8n)) \le 5 + D(S(4n)).$$

Если в поле $GF(2^n)$ *выбрать нормальный базис, то для инвертирования справедливы следующие рекуррентные оценки сложности и глубины:*

$$L(I(8n)) \le L(I(n)) + 45L(M(n)) + 101n,$$

$$D(I(8n)) \le 4D(M(n)) + 8 + \max\{D(I(n)), 6\}.$$

В башне расширений $GF(((2^n)^4)^2)$ *поля* $GF(2^n)$ *при нечетном* n *можно выбрать базис так, что справедливы следующие рекуррентные оценки сложности и глубины умножения и инвертирования:*

$$L(M(8n)) \le 30L(M(n)) + 82n, \quad D(M(8n)) \le D(M(n)) + 5,$$

$$L(I(8n)) \le L(I(n)) + 52L(M(n)) + 88n,$$
$$D(I(8n)) \le 4D(M(n)) + 6 + \max\{D(I(n)), 2\}.$$

В **третьей главе** изучаются схемы для умножения многочленов в некоторых конечных полях малой нечётной характеристики и схемы для умножения в этих полях. Особое внимание уделяется полям $GF(7^{14n})$, НОД$(n, 14) = 1$, имеющим приложения в криптографии на эллиптических кривых. В ней обычно применяются кривые или над простыми полями, или над полями характеристики два. Последние наиболее удобны для реализации в виде электронных схем[12,13,14]. В связи с открытием возможности использования в криптографии так называемых билинейных спариваний (введенных в работах Вейля, Тейта и Лихтенбаума), для конструирования новых криптоалгоритмов начали применяться эллиптические и гиперэллиптические кривые над полями характеристики три[15,16]. Как следствие, появился интерес к реализации арифметики в этих и других полях нечетной характеристики[17,18,19]. В частности, поля $GF(p^{2pn})$, где НОД$(n, 2p) = 1$, $p \equiv 3 \pmod 4$, появляются в алгоритме Дуурсма-Ли[20], а поля $GF(7^{14n})$ – в работе[21], но вопросы эффективной реализации арифметики в этих полях там не затрагиваются.

Далее приводятся формулировки некоторых результатов главы, используются следующие обозначения: $GF(q)$ – конечное поле порядка q, n – произвольное натуральное число, p – простое, $M(G)$ – схемная сложность умножения, $D(M(G))$ – глубина схемы умножения в поле G, $A(p)$ – сложность сложения, $D(A(p))$ – глубина схемы сложения , $D(M(p))$ – глубина схемы умножения в поле в поле $GF(p)$, $M(n)$ – сложность умножения многочленов степени меньшей n над $GF(7^2)$.

---

[12] I. Blake, G. Seroussi, N. Smart *Elliptic curves in cryptography.* Cambridge University Press, 1999.

[13] Blake I.,Seroussi G., Smart N. Advances in elliptic curve cryptograhy, Cambridge University Press, 2005.

[14] Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы и протоколы криптографии на эллиптических кривых. М.: КомКнига, 2006.

[15] Barreto P.S.L.M., Kim H.Y., Lynn B., Scott M. Efficient algorithms for pairing-based cryptosystems. Crypto-2002, LNCS 2442(2002), 354-368.

[16] Barreto P.S.M.L., Galbraith S., OhEigeartaigh C. and Scott M. Efficient pairing computation on supersingular abelian varieties Cryptology ePrint Archive, Report 2004/375. http://eprint.iacr.org/2004/375

[17] Kerins T., Marname W.P., Popovici E.M., and Barreto P.S.L.M. Efficient hardware for Tate pairing calculation in characteristic three. CHES-2005.

[18] Page D., Smart N.P. Hardware implementation of finite fields of characteristic three, CHES-2002, LNCS, 2002.

[19] Granger R., Page D., Stam M. Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three. IEEE Trans. on Comp. v.54, No 7 (2005), 852-860.

[20] Duursma I. and Lee H.-S. Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$. Asiacrypt-2003, LNCS 2894(2003), 111-123.

[21] Eunjeong Lee, Huang-Sook Lee and Yoonjin Lee. Fast computation of Tate pairing on general divisors for hyperelliptic curves of genus 3. Cryptology ePrint Archive, Report 2006/125. http://eprint.iacr.org/2006/125.

Теорема 3.2.1. *Умножение элементов поля* $GF(7^{14n})$ *может быть выполнено схемой сложности* $M(GF(7^{14n})) \leq 13M(GF(7^{2n}))+258nA(7)$ *и глубины* $D(M(GF(7^{14n}))) \leq 11D(A(7)) + D(M(GF(7^{2n})))$. *В частности, при* $n = 31$, $M(GF(7^{14\cdot 31})) \leq 698\ 554$.

Следующая теорема может использоваться для оптимизации сложности алгоритма Дуурсма-Ли эффективнее, чем предыдущая теорема, так как указанная в ней оценка учитывает особенности этого криптоалгоритма.

Теорема 3.2.2. *Умножение в поле* $GF(7^{14n})$ *элемента* f, *представимого многочленом степени* 6 *над полем* $GF(7^{2n})$, *на элемент* g, *представимый многочленом степени* 4 *с единичным старшим коэффициентом над полем* $GF(7^{2n})$, *имеет сложность не выше* $10M(GF(7^{2n})) + 176nA(7)$. *Глубина схемы не превосходит* $13D(A(7)) + D(M(GF(7^{2n})))$. *В частности, при* $n = 31$, *сложность умножения не превосходит* 557 392, *а глубина схемы не превосходит* $31D(A(7)) + D(M(7)) = 253$. *Ухудшив оценку сложности, можно получить оценку для глубины* 129.

Выбор приведенных выше конкретных примеров мотивируется тем, что порядок поля $GF(7^{14\cdot 31})$ приблизительно равен 2^{1000} и является минимально возможным, при котором обеспечивается необходимый уровень криптографической надёжности согласно современным стандартам. В следующей теореме указывается асимптотическая оценка сложности умножения многочленов произвольной степени над $GF(7^2)$.

Теорема 3.3.1. *Многочлены степени* $n-1$ *над* $GF(7^2)$ *могут быть умножены со сложностью* $M(n) \lesssim \frac{609\ 707}{8}\ n^{\log_5 7}$.

В **четвёртой главе** изучаются схемы для арифметики в полях большой характеристики. Интерес к эффективной реализации арифметики в таких полях также возник в связи с возможными применениями в криптографии на эллиптических кривых. С этой целью было предложено в работе[22] использовать поля с характеристикой, относительно мало отличающейся от степени двойки (такие простые числа названы ней псевдомерсенновскими), в которых существуют полиномиальные базисы, соответствующие неприводимым двучленам (такие представления этих полей названы в указанной работе оптимальными расширениями простых полей). В работе[23] среди таких расширений выделены расширения размерности 2^n, 3^n и представлены в виде башен полей, построенных из

[22]Bailey D.V., Paar C. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. J. of Cryptology 14:3(2001), 156- 173.

[23]S.Baktir, B.Sunar. Optimal tower fields. IEEE Trans. Comp. v. 53 N 10 (2004), 1231-1243.

квадратичных и кубических расширений. С использованием этих башен (названных оптимальными башнями полей) в этой работе была указана для оптимальных расширений эффективная реализация операций умножения и инвертирования.

Далее для формулирования результатов используются следующие обозначения: $M(q)$ – сложность умножения в $GF(q)$, $A(q)$ – сложность сложения в $GF(q)$, $M(C,q)$ – сложность умножения на константу C в $GF(q)$. В цитированной работе получен результат, который можно сформулировать следующим образом.

Умножение в башне полей $GF(q^{2^k})$ имеет рекуррентную верхнюю оценку сложности

$$M(q^{2^k}) \le 3^k M(q) + 5(3^k - 2^k)A(q) + \frac{1}{2}(3^k - 1)M(\alpha_0, q),$$

где многочлен $x^2 - \alpha_0$ неприводим над $GF(q)$, $\alpha_0 \in GF(q)$. Умножение в башне полей $GF(q^{3^k})$ имеет рекуррентную верхнюю оценку сложности

$$M(q^{3^k}) \le 6^k M(q) + 5(6^k - 3^k)A(q) + \frac{2}{5}(6^k - 1)M(\alpha_0, q),$$

где многочлен $x^3 - \alpha_0$ неприводим над $GF(q)$, $\alpha_0 \in GF(q)$.

Для случаев, когда характеристика поля является числом Мерсенна или Ферма, в четвёртой главе диссертации предлагается несколько лучшая реализация арифметики в башнях полей некоторых типов. В отличие от цитированной работы в диссертации рассматривалась не программная, а схемная реализация. Но приведённые результаты (за исключением касающихся глубины) можно интерпретировать и в терминах программной реализации. Сравнения с результатом цитированной работы указаны в тексте четвёртой главы в виде замечаний.

Далее приводятся формулировки полученных результатов (**теоремы 4.2.1 – 4.5.4**) с использованием следующих обозначений: w_k – примитивный корень k-ой степени из единицы в $GF(q)$, $\varepsilon = w_3$; n, k_i – неотрицательные целые, p – простое.

Умножение в башне полей $GF(q^3)$, $q = p^n$, имеет оценку сложности

$$M(q^3) \le 5M(q) + 21A(q) + 6M(2,q) +$$
$$+2(M(4,q) + M(1/2,q) + M(1/6,q)) + 2M(\alpha_0, p)$$

в предположении, что $q-1$ кратно 3, двучлены $x^n - \alpha_0$ и $x^{3n} - \alpha_0$ неприводимы над $GF(p)$.

Умножение в башне полей $GF(q^4)$, $q = p^n$, *имеет оценку сложности*

$$M(q^4) \le 7M(q) + 6M(\omega_3, q) + 54A(q) + 6M(1/6, q) + 3M(\alpha_0, p)$$

в предположении, что $q-1$ *кратно* 12 *и многочлены* $x^n - \alpha_0$ *и* $x^{4n} - \alpha_0$ *неприводимы над* $GF(p)$.

Умножение в башне полей $GF(q^6)$, $q = p^n$, *имеет оценку сложности*

$$M(q^6) \le 12M(q) + 121A(q) + 6M(\alpha_0, p) + M(1/12, q)+$$
$$+2(M(-3/2, q) + M(\frac{\varepsilon - \varepsilon^2}{2}, q) + M(-1/8, q) + M(\frac{\varepsilon - \varepsilon^2}{24}, q))+$$
$$+2(M(\omega_4, q) + M(-3\omega_4/2, q) + M(\omega_4\frac{\varepsilon - \varepsilon^2}{2}, q))+$$
$$+M(\frac{\omega_4}{12}, q) + M(-\omega_4/8, q) + M(\omega_4\frac{\varepsilon - \varepsilon^2}{24}, q)$$

в предположении, что $q-1$ *кратно* 12, *многочлены* $x^n - \alpha_0$ *и* $x^{6n} - \alpha_0$ *неприводимы над* $GF(p)$.

Для $q = p^n$, $p = 2^{13} - 1$, $n = 2^{k_0} \cdot 3^{k_1} \cdot 5^{k_2} \cdot 7^{k_3} \cdot 13^{k_4}$, $k_0 = 0, 1$, *умножение в поле* $GF(q^5)$ *имеет оценку сложности* $M(q^5) \le 77A(q) + 11M(q)$, *умножение в поле* $GF(q^7)$ *имеет оценку сложности* $M(q^7) \le 13M(q) + 344A(q) + 6A(p)$, *умножение в поле* $GF(q^{13})$ *имеет оценку сложности* $M(q^{13}) \le 26M(q) + 1026A(q) + 12A(p)$, *умножение в поле* $GF(q^{14})$ *имеет оценку сложности* $M(q^{14}) \le 26M(q) + 1032A(q) + 13A(p)$.

Для $q = p^n$, $p = 2^{17} - 1$, $n = 2^{k_0} \cdot 3^{k_1} \cdot 5^{k_2} \cdot 17^{k_3}$, $k_0 = 0, 1$, *умножение в поле* $GF(q^9)$ *имеет оценку сложности* $M(q^9) \le 17M(q) + 578A(q) + 6A(p)$, *умножение в поле* $GF(q^{18})$ *имеет оценку сложности* $M(q^{18}) \le 35M(q) + 1825A(q) + 17A(p)$.

Умножение в поле $GF(q^{2^k})$, $k \le 4$, $q = p^n$, $n = 2^m$, $p = 2^{16} + 1$, *имеет оценки сложности*

$$M(q^4) \le 7M(q) + 59A(q) + 3M(3, p),$$

$$M(q^8) \le 15M(q) + 193A(q) + 7M(3, p),$$
$$M(q^{16}) \le 31M(q) + 558A(q) + 15M(3, p).$$

Далее используются также следующие обозначения: $I(q)$ – сложность инвертирования, $S(q)$ – сложность возведения в квадрат, $D(I(q))$ – глубина схемы инвертирования, $D(S(q))$ – глубина схемы возведения в квадрат, $D(M(C,q))$ – глубина схемы умножения на константу C в поле $GF(q)$, $M(2^s,q) = \max\{M(C,q) : C = 2^s, s = 1,2,3,\dots\}$, $D(M(2^s,q)) = \max\{D(M(C,q)) : C = 2^s, s = 1,2,3,\dots\}$.

В поле $GF(p^{2^m}), p = 2^{16}+1$, *существует схема для инвертирования, у которой сложность рекуррентно оценивается как*

$$I_{2^m} = I_{2^{m-1}} + 6S_{2^{m-1}} + 12M_{2^{m-1}} + 15A_{2^{m-1}} + 5M(3,p) + M(6,p) +$$

$$+(2^{m-1}-1)M(2,p),$$

где I_k *есть сокращение для* $I(p^k)$, *и аналогично определяются* M_k, S_k, A_k. *Глубина этой схемы рекуррентно оценивается как*

$$D(I_{2^m}) = D(I_{2^{m-1}}) + 2D(M_{2^{m-1}}) + D(S_{2^{m-1}}) + 2(D(A(p)) + D(M(3,p)).$$

Для инвертирования в поле $GF(q^{16})$, $q = p^n$, $n = 2^m$, $p = 2^{16}+1$, *может быть построена схема сложности*

$$I(q)+410M(q)+24S(q)+2173A(q)+735M(2^s,q)+119M(3,p)+M(6,p).$$

Если $D(M(q)) + 2(D(A(p)) + D(M(3,p))) \le D(I(q))$, *то глубина этой схемы не больше*

$$D(I(q))+4D(M(q))+D(S(q))+19D(A(p))+10D(M(2^s,p))+3D(M(3,p)).$$

В противном случае она не превосходит

$$5D(M(q)) + D(S(q)) + 21D(A(p)) + 10D(M(2^s,p)) + 5D(M(3,p)).$$

Инвертирование в поле $GF(p^{10n})$, $p = 1 \pmod{10n}$, *может быть выполнено схемами, имеющими оценки сложности*

$$I(p^{10n}) \le I(p^{2n}) + 28M(p^{2n}) + 143nA(p) + (16n+2)M(\alpha_0,p) +$$

$$+6n(M(\omega_5,p) + M(\omega_5^2,p) + M(\omega_5^3,p) + M(\omega_5^4,p)),$$

$$I(p^{10n}) \le I(p^n) + 445nA(p) + 76M(p^n) + 34M(\alpha_0,p) +$$

$$+6n(M(\omega_5,p) + M(\omega_5^2,p) + M(\omega_5^3,p) + M(\omega_5^4,p)),\ \alpha_0 \in GF(p).$$

Умножение в поле $GF(q^n)$ *для* $q = p^2$, $p = 2^{13} - 1$, $n = 5^m$, $m = 1, 2$, *имеет оценку сложности*

$$M(q^5) \leq 27M(p) + 121A(p), \quad M(q^{25}) \leq 1462A(p) + 243M(p).$$

Умножение в поле $GF(p^{2n})$ *для* $p = 2^k - 1$ *при* $n \leq 2^{k-1}$, *имеющем только простые нечетные делители, делящие* $p-1$, *может быть выполнено с помощью схемы, имеющей оценку сложности*

$$M(p^{2n}) \leq (15 \cdot 2^{m-2} + 9(2^{m-1}(m-2)+1))M(p)+$$

$$+((12m+7)2^{m-1} + 9(2^{m-1}(m-2)+1))A(p),$$

где $2^{m-1} \leq 2n - 2 < 2^m, m \leq k$. *Если* $2n - 2 = 2^m, m \leq k$, *тогда к указанной оценке сложности прибавляется* $M(p^2) + A(p^2)$.

Публикации автора по теме диссертации

1. *Бурцев А. А., Гашков И. Б., Гашков С. Б.* О сложности булевых схем для арифметики в некоторых башнях конечных полей // Вестн. Моск. ун-та. Сер. 1, Математика. Механика. 2006. №5. С. 10-16.

2. *Бурцев А. А., Гашков С. Б.* О схемах для арифметики в композитных полях большой характеристики // Чебышевский сборник. Том 7. Выпуск 2 (2006). С. 186 - 204.

3. *Бурцев А. А.* О схемах для умножения и инвертирования в композитных полях // Чебышевский сборник. Том 7. Выпуск 2 (2006). С. 172 - 185.

4. *Бурцев А. А.* О булевых схемах умножения многочленов в конечных полях нечётной характеристики. // Материалы VI молодёжной научной школы по дискретной математике и её приложениям (Москва, 16-21 апреля 2007 г.) Часть I. С. 13 – 16.

5. *Бурцев А. А.* О булевых схемах для арифметики в псевдомерсенновских полях. // Материалы IX Международного научного семинара «Дискретная математика и её приложения». (Москва, 18-23 июня 2007 г.) С. 66 - 68.