УДК 681.3.06

ИССЛЕДОВАНИЕ ЭФФЕКТИВНОСТИ ВАРИАНТОВ ПРЕДСТАВЛЕНИЙ БОЛЬШИХ ЧИСЕЛ ПО МНОЖЕСТВЕННЫМ ОСНОВАНИЯМ В НЕСИММЕТРИЧНОЙ КРИПТОГРАФИИ

О.А. МЕЛЬНИКОВА, А.С. БУТЕНКО

В статье приведены результаты исследования эффективности методов выполнения скалярного умножения с использованием представлений больших чисел по множественным основам. В работе предлагаются результаты сравнительного анализа реализаций методов между собой и с реализацией метода, что использует знаково-цифровые представления чисел. На основе приведенных результатов сделаны выводы относительно эффективности методов выполнения скалярного умножения с использованием представлений больших чисел по множественным основам и рассмотрены перспективы последующих исследований.

Ключевые слова: несимметричная криптография, скалярное умножение.

ВВЕДЕНИЕ

Криптосистемы на основе эллиптических кривых обеспечивают требуемый уровень безопасности при меньших размерах ключа и, вследствие этого, имеют явные преимущества над другими асимметричными методами. При практическом внедрении криптосистем на основе эллиптических кривых особую актуальность приобретают вопросы эффективной реализации основных операций. Большинство криптографических протоколов на эллиптических кривых требует вычисление скалярного произведения. Таким образом, требуется разработать быстрые алгоритмы вычисления скалярного произведения $[k]P$ для любого целого числа k и для любой точки P эллиптической кривой.

В статье представлены результаты исследования эффективности скалярного умножения на основе методов представления больших чисел по множественным основаниям: представление чисел по двойным основаниям с нетривиальными коэффициентами (Extended DBNS [1]), представление чисел по двойным основаниям с построением бинарного дерева (Tree-based DBNS [2]) и представление чисел по тройным основаниям с нетривиальными коэффициентами (SMBR [3]).

В данной статье рассматриваются эллиптические кривые над расширенным двоичным полем $E(GF(2^m))$. Как известно, наиболее вычислительно сложной операцией является инверсия элемента поля [3]. Для того, чтобы исключить эту операцию, берём за основу проективные координаты. На сегодняшний день известно несколько их типов. Наиболее эффективными проективными координатами для выполнения групповых операций для $E(GF(2^m))$ являются координаты Лопеса-Дахаба [4].

В этой статье представлены результаты, полученные в ходе экспериментального сравнения реализаций указанных методов, а также сравнения с функцией скалярного умножения ecurve2_mult из библиотеки MIRACL [5], в которой используются знаково-цифровые представления чисел. Необходимо отметить, что ранее уже проводилось сравнение реализации скалярного умножения на основе метода представления больших чисел по множественным основаниям, использующего “золотое сечение”, с функцией скалярного умножения ecurve2_mult. Метод с использованием “золотого сечения” дал уменьшение вычислительной сложности скалярного умножения по сравнению с функцией скалярного умножения ecurve2_mult для аффинных координат.

1. КЛАССИФИКАЦИЯ МЕТОДОВ

Представлением числа k по множественным основаниям называется представление в виде суммы степеней элементов набора “маленьких” целых чисел $B=\{b_1,...,b_j\}$:

$$k=\sum_{i=1}^{m} s_i b_1^{e_{ij}} ... b_j^{e_{ij}}, \qquad (1)$$

где $|s_i|\in S$, $|b_j|\in B$.

Система представлений по двойным основаниям (DBNS) является частным случаем представления по множественным основаниям с количеством оснований $\#B=2$. В данной работе рассматривается вариант с набором оснований $B=\{2,3\}$. В системе представления по двойным основаниям любое целое число k может быть представлено в виде:

$$k=\sum_{i=1}^{m} s_i 2^{a_i} 3^{b_i}, \qquad (2)$$

где $|s_i|\in S$.

Метод Extended DBNS использует ограничения (3) на значения a_i, b_i и наборы коэффициентов $S=\{1,5,7,11,13,17,19,23,25...\}$, состоящие из чисел, взаимно простых с 2 и 3. Необходимо отметить, что авторами данной работы были проведены эксперименты с использованием других наборов коэффициентов. Однако при использовании указанного набора коэффициентов была получена самая высокая эффективность поиска представлений чисел:

$$a_1 \ge a_2 \ge ... \ge a_m \qquad (3)$$
$$b_1 \ge b_2 \ge ... \ge b_m .$$

Метод Tree-based DBNS основан на построении бинарных деревьев. Данный подход не ограничивается нахождением одного разложения числа (2). В Tree-based DBNS выполняется заданное количество разложений, равное границе T, и выбирается лучшее среди них.

Система представлений по тройным основаниям является частным случаем представления по множественным основаниям с количеством оснований $\#B = 3$. В данной работе рассматривается вариант с набором оснований $B = \{2,3,5\}$. В системе представления по тройным основаниям любое положительное число k может быть представлено в виде:

$$k = \sum_{i=1}^{m} s_i 2^{a_i} 3^{b_i} 5^{c_i}, \quad (4)$$

где $|s_i| \in S$.

Метод SMBR использует ограничения (5) на значения a_i, b_i, c_i и наборы коэффициентов $S = \{1,7,11,13,17,19,23,29,31...\}$, состоящие из чисел, взаимно простых с 2, 3 и 5.

$$\begin{aligned} a_1 &\geq a_2 \geq ... \geq a_m \\ b_1 &\geq b_2 \geq ... \geq b_m \\ c_1 &\geq c_2 \geq ... \geq c_m \end{aligned} \quad (5)$$

2. АНАЛИЗ ПРЕДСТАВЛЕНИЙ ПО МНОЖЕСТВЕННЫМ ОСНОВАНИЯМ

При исследовании скалярного умножения на основе представлений по множественным основаниям эксперименты проводились на выборках по 1000 скалярных множителей для каждой из 13 тестовых эллиптических кривых стандартов [6, 7].

Анализируемые методы требуют использования предвычислений. При этом размер таблицы предвычислений определяется значениями границ P (максимальная степень основания 3) и Q (максимальная степень основания 5, только для SMBR), а также количеством коэффициентов $\#S$. Для метода Tree-based DBNS изменяется размер бинарного дерева (граница T).

В табл. 1 приведены параметры из [1-3], использованные при исследовании указанных методов.

Таблица 1

Значения параметров

Метод	P	Q	T	$\#S$
Extended DBNS	5 – 200	—	—	1 – 13
Tree-based DBNS	5 – 200	—	1 – 16	1
SMBR	85 – 200	40 – 70	—	5 – 13

Был проведен анализ и поиск оптимальных значений параметров реализаций указанных методов, которые приведены в табл. 2.

Таблица 2

Оптимальные значения параметров

Метод	P	Q	T	$\#S$
Extended DBNS	5	–	–	9
Tree-based DBNS	5	–	4 – 8	1
SMBR	85 – 100	40 – 70	–	9

На рис. 1 представлены оценки эффективности поиска разложений больших чисел по рассмотренным методам. Количество термов метода SMBR ниже на 40-55% и 50-65% по сравнению с методами Extended DBNS и Tree-based DBNS соответственно.

На рис. 2 приведены сравнительные оценки вычислительной сложности (времени выполнения) реализаций скалярного умножения рассмотренных методов (без учёта этапа разложения), а также функции скалярного умножения ecurve2_mult. Вычислительная сложность скалярного умножения по методу Extended DBNS ниже на 20-25% и 25-40% по сравнению с методами SMBR и Tree-based DBNS соответственно. Из реализаций рассмотренных методов только Extended DBNS дал уменьшение вычислительной сложности скалярного умножения до 12% по сравнению с функцией скалярного умножения ecurve2_mult.

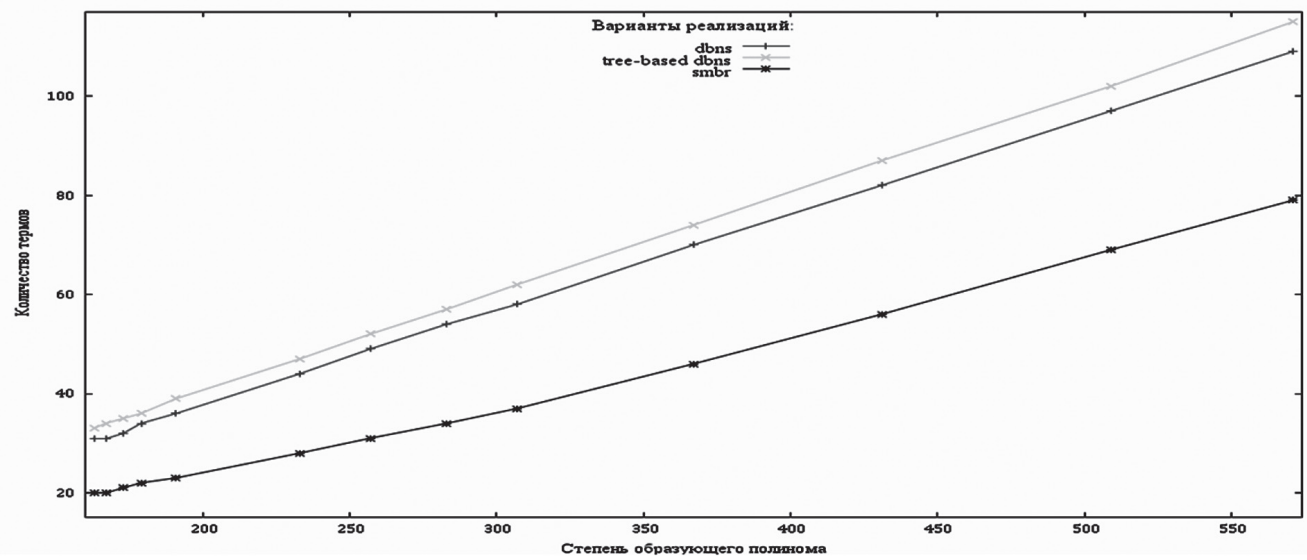

Рис. 1. Сравнение длин разложений

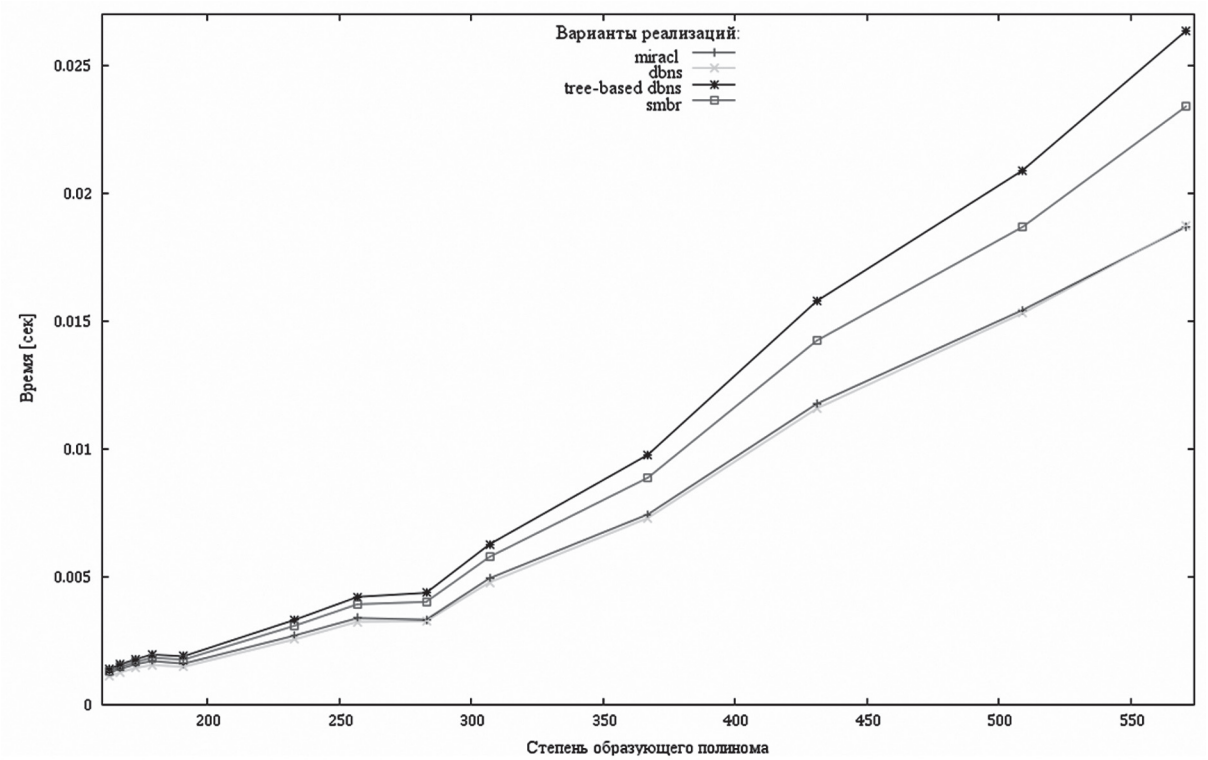

Рис. 2. Сравнение времени скалярного умножения

ЗАКЛЮЧЕНИЕ

Анализ полученных результатов показал, что для уменьшения вычислительной сложности реализаций скалярного умножения рассмотренных методов по сравнению с функцией скалярного умножения ecurve2_mult необходимо существенно уменьшить вычислительную сложность как этапа поиска разложений чисел, так и скалярного умножения чисел.

Для снижения вычислительной сложности этапа поиска разложений чисел необходимо уменьшить время поиска разложений чисел. Авторами данной работы была уменьшена вычислительная сложность преобразования больших чисел в бинарные строки, которые необходимы для нахождения разложений, что привело к уменьшению вычислительной сложности поиска представлений чисел на 100-105%. Однако вычислительная сложность преобразования больших чисел в бинарные строки составляет более 60% вычислительной сложности этапа поиска разложений чисел. В дальнейшем необходимо рассмотреть альтернативные алгоритмы поиска разложений больших чисел по множественным основаниям без использования преобразования чисел в бинарные строки.

Однако при уменьшении времени поиска необходимо не снизить эффективность поиска (длины разложений), которая влияет на вычислительную сложность этапа скалярного умножения. Также для снижения вычислительной сложности этапа скалярного умножения чисел необходимо оптимизировать операции утроения (1.2, 1.4) и упятерения (1.4) для проективных координат Лопеса-Дахаба либо другого более эффективного типа координат. Как известно из литературы [8], существуют оптимизированные формулы утроения в проективных координатах Лопеса-Дахаба, которые на момент написания статьи отсутствуют в открытом доступе.

Литература

[1] *C. Doche and L. Imbert,* “Extended double-base number system with applications to elliptic curve cryptography” // Progress in Cryptology, INDOCRYPT’06, ser. Lecture Notes in Computer Science, vol. 4329. Springer, 2006, pp. 335–348.

[2] *Doche, C., Habsieger, L.:* “A Tree-Base Approach for Computing Double-Base Chains” // ACISP 2008, ser. Lecture Notes in Computer Science, vol. 5107, pp. 433-446.Springer, Heidelberg (2008).

[3] *Dimitrov, V., Mishra, P.K.:* “Efficient Quintuple Formulas for Elliptic Curves and Efficient Scalar Multiplication using Multibase Number Representation” // ISC 2007, ser. Lecture Notes in Computer Science, vol. 4779, pp. 390-406. Springer, Heidelberg (2007).

[4] *T. Lange:* “A notes on Lopez-Dahab coordinates” // Cryptology ePrint Archive, report 2002/323, 2002.

[5] Shamus Software Ltd: “M.I.R.A.C.L Users Manual”// 4 Foster Place North, Ballybough, Dublin 3, Ireland, 2010.

[6] ДСТУ 4145 – 2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння. – Перше видання; Введ. 1.07.2003. — К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003 р. — 36 с.

[7] Federal Information Processing Standards Publication 186 – 2 (FIPS PUB 186 - 2). Digital Signature Standard // U.S. Department of Commerce. Technology Administration, National Institute of Standards and Technology (NIST). – 2001. – 74 pp.

[8] *Haihua Gu, Dawu Gu, Ya Liu:* "Efficient Scalar Multiplication for Elliptic Curve over Binary Field"// ChinaCrypt'2008, Wuhan, Oct.2008.

Поступила в редколлегию 7.06.2010.

Мельникова Оксана Анатольевна, кандидат технических наук, доцент кафедры БИТ ХНУРЕ. Область научных интересов: защита информации, криптография.

Бутенко Александр Сергеевич, магистр кафедры БИТ ХНУРЭ. Область научных интересов: оптимизация и криптоанализ.

УДК 681.3.06

Дослідження ефективності варіантів подань великих чисел по множинним основам у несиметричній криптографії / О.А. Мельникова, О.С. Бутенко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2010. Том 9. № 3. – С. 374-377.

У статті приведені результати дослідження ефективності методів виконання скалярного множення з використанням подань великих чисел по множинним основам. У роботі пропонуються результати порівняльного аналізу реалізацій методів між собою та з реалізацією метода, що використовує знаково-цифрові подання чисел. На основі приведених результатів зроблені висновки стосовно ефективності методів виконання скалярного множення з використанням подань великих чисел по множинним основам та розглянуті перспективи подальших досліджень.

Ключові слова: несиметрична криптографія, скалярне множення.

Іл. 2. Табл. 2. Бібліогр.: 8 найм.

UDK 681.3.06

Researching effectiveness of multibase big number representation methods for using in public key cryptography / O.A. Melnikova, O.S. Butenko // Applied Radio Electronics: Sci. Mag. – 2010. Vol. 9. № 3. – P. 374-377.

This paper presents efficiency estimations of scalar multiplication methods which use multiple base big number representations. Comparative analysis results of methods implementations are proposed. Comparison is made not only between the methods under consideration, but also with the signed-digit representation method implementation. Conclusions about efficiency of different scalar multiplication methods are made. Possibilities of further improvements are analyzed.

Key words: public key cryptography, scalar multiplication.

Fig. 2. Tab. 2. Ref.: 8 items.