УДК 004.421

О. А. Мельникова, канд. техн. наук,
А. О. Маслєннікова, студентка

Харківський національний університет радіоелектроніки, м. Харків

ПІДСТАНОВКИ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРОГРАМНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМІВ, ЯКІ ВИКОРИСТОВУЮТЬ ЗНАКОВО-ЦИФРОВІ ПРЕДСТАВЛЕННЯ

Запропоновано прийом використання підстановок адрес функцій разом із підстановками даних, який дозволяє виключити умовні переходи в коді програми та може покращити час виконання багатьох алгоритмів, наприклад, в галузі арифметики еліптичних кривих. В цій роботі представлений прийом продемонстровано на найпростіших прикладах декількох алгоритмів скалярного множення точок еліптичних кривих, які використовують знаково-цифрові форми подання. Але він може дати кращі результати при модифікації складніших алгоритмів зі значною кількістю умовних розгалужень.

Ключові слова: *знаково-цифрові представлення багаторозрядних цілих чисел, скалярне множення точок еліптичних кривих, еліптична криптографія, несиметрична криптографія, обчислювальна складність алгоритмів.*

Вступ. Як відомо, операція множення точки P еліптичної кривої (ЕК) на багаторозрядне ціле число $k \in [2, n-1]$ (де n — порядок базової точки ЕК) є основною та найбільш обчислювально складною базовою операцією в алгоритмах еліптичної криптографії. Тому приділяється значна увага постійному розвитку різних класів методів покращення ефективності її реалізації. Одним з них є використання «нестандартних» форм представлення багаторозрядних цілих чисел. На цей час запропоновано багато таких форм представлення та продовжують з'являтися нові результати досліджень і все більш складні системи кодування багаторозрядних цілих чисел.

Наприклад, відомі такі типи «нестандартних» форм представлення:

- знаково-бінарні (SBR) такі, як NAF, MOF і т. ін.;
- знаково-цифрові (SDR) такі, як wNAF, wMOF і т. ін.;
- знаково-цифрові за подвійними основами (DBNR), потрійними або множинними основами (MBNR);
- об'єднані знаково-бінарні представлення (JSBR) такі, як JSF і т. ін.;
- об'єднані знаково-цифрові (JSDR);
- об'єднані представлення за подвійними (JDBNR), потрійними або множинними основами (JMBNR).

Основною метою «нестандартних» форм представлення є мінімізація кількості значущих (ненульових) елементів у представленні багаторозрядного цілого числа k або пари чисел (r, s) і, як наслідок, зменшення кількості операцій додавання точок ЕК під час реалізації операції скалярного множення точки ЕК $k \cdot P$ або одночасного двократного (багатократного) скалярного множення $r \cdot P + s \cdot Q$. Остання операція, як відомо, є основною (найбільш обчислювально складною) для багатьох сучасних алгоритмів перевірки електронного цифрового підпису (ЕЦП).

Деякі з вищенаведених форм представлення вже знаходили практичне застосування при розробці ефективних бібліотек виконання операцій над багаторозрядними числами, у тому числі варіантів операцій скалярного множення точки ЕК (наприклад, JSF для одночасного подвійного множення точок ЕК в окремих версіях бібліотеки [3]). Інші знаходяться здебільшого на етапі теоретичних досліджень і потребують значного покращення обчислювальних характеристик. Але, в цілому, цей клас методів для покращення ефективності реалізації алгоритмів еліптичної криптографії є досить перспективним і розвивається в сучасних розробках багатьох авторів.

Одним із невирішених питань є те, що алгоритми як формування «нестандартних» форм представлення, так і їх використання мають досить складну структуру із великою кількістю умовних розгалужень, тощо. Така структура може суттєво погіршувати обчислювальні характеристики реалізацій алгоритмів за умов конвеєрної обробки на сучасній обчислювальній техніці.

У цій роботі розглянуто один із можливих варіантів підвищення ефективності програмної реалізації алгоритмів, що використовують SBR та SDR, за рахунок комбінування взаємопов'язаних підстановок адрес функцій і підстановок даних (таблиць передобчислень різного типу та обсягу). Цей підхід дозволяє зменшувати кількість умовних розгалужень в алгоритмах, які використовують SDR.

Для спрощення викладення почнемо з окремих (вироджених) випадків несуміжних знаково-цифрових представлень (SDR) із параметром несуміжності $w = 2$, які також називають знаково-бінарними представленнями (SBR).

Знаково-бінарне представлення (SBR) цілого числа $k > 0$ має вигляд

$$k = \sum_{j=0}^{t-1} 2^j \cdot k_j \ ,$$

де $k_j \in S$ для $j = 1, 2, \ldots, (t - 1)$; $S = \{0, \pm 1\}$ — знаково-цифровий набір (множина цифр, які використовуються у певному варіанті реалізації SBR, при цьому особливості представлення елементів множини можуть варіюватися).

Традиційно алгоритм скалярного множення, який використовує знаково-бінарне представлення (SBR) багаторозрядних цілих чисел, має наступний вигляд [1, p. 13] (нотацію дещо спрощено та частково наближено до синтаксису мови програмування С).

Алгоритм 1. Бінарний, від старших біт, NAF-метод множення точки P еліптичної кривої E.

Вхідні дані: $NAF(k) = \sum_{j=0}^{t-1} k_j \cdot 2^j$ (для $k > 0$, $k_j \in \{0,1,-1\}$), $P \in E\left(F_{2^m}\right)$.

Вихідні дані: $R = k \cdot P$.

1. $R = I$;
2. for ($j = t - 1; j \geq 0; j--$).
   2.1. $R = 2 \cdot R$;
   2.2. if ($k_j == 1$) $R = R + P$;
   2.3. if ($k_j == -1$) $R = R - P$;
3. return (R).

Зазначимо, що у цьому алгоритмі NAF використано лише як приклад знаково-бінарного представлення (SBR), яке може бути замінено будь-яким SBR із негіршими характеристиками. А також, у цьому та всіх наступних алгоритмах лише для визначеності відмічено, що використовується ЕК над F_{2^m}, проте може бути задіяний інший тип ЕК.

Модифікований варіант алгоритму із використанням таблиць підстановки точок $T[]$ та підстановки адрес функцій $pF[]$ (за умови альтернативного кодування знаково-цифрового набору SBR $S = \{1, 2, 0\}$ замість $S = \{0,1,-1\}$) має наступний вигляд.

Алгоритм 2. Бінарний, від старших біт, SBR-метод множення точки P еліптичної кривої E.

Вхідні дані: $SBR(k) = \sum_{j=0}^{t-1} s_j \cdot 2^j$ (для $k > 0$, $s_j \in \{1,2,0\}$), $T[3] = \{-P, I, P\}$ (де $P \in E\left(F_{2^m}\right)$).

Вихідні дані: $R = k \cdot P$.

0. $pF[3](R, T[3]) = \{SubP, AddI, AddP\}$; // таблиця підстановки адрес функцій із двома параметрами
1. $R = T[2]$; // $R = P$, за рахунок пропуску старшої цифри s_{t-1}
2. for ($j = t - 2; j \geq 0; j--$)
   $pF[s_j](R, T[])$; // $s_j == 0: SubP()$, $s_j == 1: AddI()$, $s_j == 2: AddP()$
3. return (R).

Наведемо короткий опис переліку допоміжних функцій із двома параметрами (де R — точка для збереження поточного результату,

$T[]$ — таблиця підстановки передобчислених точок разом із представленням точки I на нескінченності).

SubP(R, $T[]$) // $s_j == 0$ (при традиційному кодуванні $k_j == -1$)
1. $R = 2 \cdot R$;
2. $R = R + T[0]$; // фактично, $R = R - P$

AddI(R, $T[]$) // $s_j == 1$ (при традиційному кодуванні $k_j == 0$)
$R = 2 \cdot R$;

AddP(R, $T[]$) // $s_j == 2$ (при традиційному кодуванні $k_j == 1$)
1. $R = 2 \cdot R$;
2. $R = R + T[2]$; // фактично, $R = R + P$

Більш загальною формою представлення є знаково-цифрове представлення (SDR) цілого числа $k > 0$:

$$k = \sum_{j=0}^{t-1} 2^j \cdot k_j ,$$

де $k_j \in S$ для $j = 1, 2, \ldots, (t-1)$; $S = \{0, \pm1, \pm3, \pm5, \ldots, \pm(2^{w-1} - 1)\}$ — знаково-цифровий набір (множина цифр, які використовуються у певному варіанті реалізації); w — параметр несуміжності ($w \geq 2$, значною мірою визначає ефективність застосування SDR).

У традиційній формі представлення S є множиною непарних чисел таких, що $|k_j| < 2^{w-1}$. Але, як і вище для SBR, можливі модифікації з метою покращення характеристик безпосередньо програмних реалізацій. Особливості представлення елементів множини S можуть значно варіюватися та впливати на обчислювальні характеристики як алгоритмів формування SDR, так і алгоритмів їх використання.

Традиційно алгоритм скалярного множення, який використовує знаково-цифрове представлення (SDR) багаторозрядних цілих чисел, має наступний вигляд [1, p. 13] (нотація дещо змінено та частково наближено до синтаксису мови програмування C).

Алгоритм 3. Блоковий, від старших біт, wNAF-метод множення точки P еліптичної кривої E.

Вхідні дані: $NAF_w(k) = \sum_{j=0}^{t-1} k_j \cdot 2^j$ (для $w \geq 2$, $k > 0$, непарних $k_j \in \{0, \pm1, \pm3, \ldots, \pm(2^{w-1} - 1)\}$), $P \in E\left(F_{2^m}\right)$.

Вихідні дані: $R = k \cdot P$.

1. $T[k_j] = j \cdot P$, для $j \in \{1, 3, 5, \ldots, (2^{w-1} - 1)\}$;
2. $R = I$;
3. for ($j = t - 1; j \geq 0; j--$)
   3.1. $R = 2 \cdot R$;

3.2. if ($k_j \neq 0$)
if ($k_j > 0$) $R = R + T[k_j]$;
else $R = R - T[k_j]$; // $k_j < 0$
4. return (R).

Зазначимо, що в традиційному поданні алгоритму не враховуються особливості розподілу пам'яті при формуванні таблиці T. Більш доцільним може бути використання повної таблиці, включаючи від'ємні значення індексів k_j, наприклад, при такому розподілі елементів для $w = 4$: $T[8] = \{-P, P, -3P, 3P, -5P, 5P, -7P, 7P\}$. У цьому випадку пункт 3.2 алгоритму 3 набуває наступного вигляду:

if ($k_j > 0$) $R = R + T[k_j]$;
else if ($k_j < 0$) $R = R + T[-k_j - 1]$;

У цьому алгоритмі wNAF використано лише в якості прикладу знаково-цифрового представлення (SDR), тобто його може бути замінено будь-яким SDR із відповідними характеристиками, наприклад, wMOF [2, p. 131–132] і т. ін.

Далі наведено модифікований варіант алгоритму із використанням таблиць підстановки $T[]$ передобчислених точок ЕК та підстановки адрес функцій $pF[]$. Деякі частини алгоритму спрощено для окремого прикладу параметра несуміжності $w = 4$. Наприклад, альтернативне кодування множини $S = \{8, 0, 7, 1, 6, 2, 5, 3, 4\}$ при $w = 4$ замість традиційного $S = \{0, 1, -1, 3, -3, 5, -5, 7, -7\}$. У загальному випадку, для довільного значення w, формальний опис альтернативного кодування множини S може бути створений, наприклад, із використанням особливостей зберігання від'ємних чисел у додатковому коді. Розмір таблиць $T[]$ та $pF[]$ також залежить від значення параметру несуміжності, а саме, $2^{w-1}+1$.

Алгоритм 4. Блоковий, від старших біт, SDR-метод множення точки P еліптичної кривої E.

Вхідні дані: $SDR_w(k) = \sum_{j=0}^{t-1} s_j \cdot 2^j$ (для $w \geq 2$, $k > 0$, для $w = 4$ $s_j \in \{8, 0, 7, 1, 6, 2, 5, 3, 4\}$), для $w = 4$, $T[9] = \{P, 3P, 5P, 7P, -7P, -5P, -3P, -P, I\}$ (де $P \in E\left(F_{2^m}\right)$).

Вихідні дані: $R = k \cdot P$.

0. $pF[9](R, T[9]) = \{wAddSjP, wAddSjP, \ldots wAddSjP, wAddI\}$; // таблиця підстановки адрес функцій із двома параметрами для $w = 4$ ($2^{w-1}+1 = 9$)
1. $R = T[s_{t-1}]$; // за рахунок пропуску старшої цифри s_{t-1}
2. for ($j = t - 2; j \geq 0; j--$)
$pF[s_j](R, T[s_j])$; // $s_j == 8$: $wAddI()$, $s_j \in \{0,1,\ldots,7\}$: $wAddSjP()$
3. return (R).

Наведемо короткий формальний опис допоміжних функцій із двома параметрами (де R — точка для збереження поточного результату, $T[]$ — таблиця підстановки передобчислених точок разом із представленням точки I на нескінченності).

wAddSjP(R, $T[s_j]$) // s_j==0 (у попередній нотації k_j==–1)
1. $R = 2^w \cdot R$; // w подвоєнь точки R
2. $R = R + T[s_j]$;
wAddI(R, $T[s_j]$) // s_j==8 (при традиційному кодуванні k_j==0)
$R = 2 \cdot R$;

При проведенні експериментальних досліджень запропоновані модифіковані версії алгоритмів були реалізовані із використанням мови C та спеціалізованої бібліотеки MIRACL [3] для виконання базових операцій над багаторозрядними цілими числами та над точками «стандартних» (у формі Вейєрштраса) еліптичних кривих над GF(2^m). При цьому використовувалися проективні координати Лопеса-Дахаба та порядки базового поля від m = 163 до 571, а також параметр несуміжності від w = 2 до 8. Експериментальні чисельні оцінки обчислювальної складності (в тактах) програмних реалізацій запропонованих модифікацій алгоритмів були отримані на Intel Core i3-2120 (3.30 ГГц). В середньому, отримано зменшення часу виконання алгоритмів на приблизно два відсотки, але ці результати можуть будуть покращені в подальших експериментах. Звичайно, при використанні іншої обчислювальної техніки та варіантів бібліотек багаторозрядної арифметики можуть спостерігатися суттєві відмінності (плануються подальші експериментальні дослідження).

Висновки. В цілому, запропонований прийом використання таблиць підстановок адрес функцій у комбінації із таблицями підстановки даних (таблицями передобчислень) задля усунення операцій умовних переходів дозволяє зменшити час виконання алгоритмів, подібних до розглянутих модифікований варіантів. При подальших дослідженнях для алгоритмів із значно більшою кількістю розгалужень, наприклад, для алгоритму формування wMOF [2, p. 131–132], заміна умовних операторів таблицями підстановки може дати набагато кращі результати. Хоча безпосередньо розробка таких таблиць заміни є складним завданням. Також цікавими напрямками подальших досліджень можуть бути подібні експерименти з варіантами об’єднаних знаково-цифрових представлень пар багаторозрядних чисел [4, p. 1–23] та з ще більш складними представленнями за подвійними (DBNS) [4, p. 31–52] та множинними основами (MBNS) [4, p. 109–134].

Список використаних джерел:

1. Hankerson D., Hernandez J. L., Menezes A. Software Implementation of Elliptic Curve Cryptography Over Binary Fields. Cryptographic Hardware and Embedded Systems, CHES'2000, P. 1–24, 2000.

2. Okeya K., Schmidt-Samoa K., Spahn C., Takagi T. Signed Binary Representations Revisited, in *«Advances in Cryptology. CRYPTO 2004»*, Lecture Notes in Computer Science 3152 (2004), P. 123–139.
3. Multiprecision Integer and Rational Arithmetic Cryptographic Library (MIRACL): [Електронний ресурс]. Режим доступу: https://github.com/miracl/MIRACL
4. Solinas J. A. Low-Weight Binary Representations for Pairs of Integers, Technical Report CORR 2001-41, University of Waterloo, 2001. 23 p. Режим доступу: http://cacr.uwaterloo.ca/techreports/2001/corr2001-41.ps
5. Dimitrov V., Jullien G., Muscedere R. Multiple-Base Number System: Theory and Applications. CRC Press, 2012. 294 p.

This paper presents functions addresses substitutions «trick» combining with data substitutions. This computational technique allows to eliminate conditional branches and thus to improve timing results for many algorithms, such as elliptic curve arithmetic algorithms. In this paper proposed technique is shown on simplest examples of several elliptic curve point multiplication algorithms with multiprecision integers signed digit representations. But it can give better results combined with more complicated highly branched algorithms.

Key words: *signed digit representations, elliptic curve arithmetic, elliptic curve point multiplication, elliptic curve cryptography, algorithm complexity.*

Одержано 20.02.2017

УДК 519.642

Л. В. Мосенцова, канд. техн. наук

Физико-технологический институт металлов и сплавов
НАН Украины, г. Киев

ЧИСЛЕННО-АНАЛИТИЧЕСКИЙ АЛГОРИТМ ИНТЕРПРЕТАЦИИ В ЗАДАЧЕ ВОССТАНОВЛЕНИЯ СИГНАЛА

Представлен численно-аналитический алгоритм интерпретации в задаче восстановления сигнала. Алгоритм состоит в преобразовании нелинейных интегральных уравнений типа Вольтерра I рода к уравнениям типа Вольтерра II рода и их численного решения путем применения алгоритма «естественной интерполяции».

Ключевые слова: *нелинейные интегральные уравнения типа Вольтерра I рода, задача восстановления сигнала, интерпретация результатов.*

Введение. Моделями динамической интерпретации результатов в задачах восстановления сигналов являются уравнения типа Вольтерра I рода, в частности нелинейные [1]. Отличительная особенность данного