УДК 004.056

Ст. викладач Мальчиков В.В., магістрант Новосад І.В.

Національний технічний університет України
«Київський політехнічний інститут»

МЕТОДИКА ШВИДКОГО ОБЧИСЛЕННЯ ТА ВАЛІДАЦІЇ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Abstract

Malchikov V.V., senior lecturer; Ivan Novosad, student
Methodology of fast evaluation and validation of digital signature

Current article is dedicated to computation digital signature of electronic message using Ukrainian cryptographic algorithm DSTU 4145-2002. Analysis of methods of modular reduction and speed testing of each method make possible to give a well-founded recommendations about development of EDS-systems, based on concerned algorithm.

Вступ

Необхідність забезпечення надійного функціонування комп'ютеризованих систем обробки інформації ставить високі вимоги щодо цілісності та автентичності даних, які надходять, зберігаються та обробляються в цих системах. Автентифікація повідомлення - перевірка того, що повідомлення було передано без порушення цілісності з очікуваного джерела. Автентифікація здійснюється виходячи з аналізу структури відповідних даних за узгодженими алгоритмами. Одним з найефективніших та найнадійніших підходів, які застосовуються для розв'язування задач, пов'язаних з автентифікацією даних та джерел повідомлень, є процедури цифрового підпису, побудовані на основі асиметричних криптографічних алгоритмів.

Одним з найслабкіших і найпроблемніших місць у сучасній криптографії є швидкодія алгоритмів. Зменшення часу, необхідного на виконання шифрування даних чи обчислення їх цифрового підпису, залишається актуальною проблемою при розробці криптографічних систем.

Постановка задачі

Мета роботи – методика якнайшвидшого виконання обчислень при реалізації алгоритму електронного цифрового підпису на ЕОМ у відповідності до стандарту ДСТУ 4145-2002.

Об’єкт досліджень – національний стандарт України ДСТУ 4145-2002, що описує алгоритми формування та перевірки електронного цифрового підпису.

Предмет досліджень – методи оптимізації виконання арифметичних операцій та методи швидкого обчислення.

Основні терміни та поняття

Електронний цифровий підпис (ЕЦП) – це блок даних невеликого розміру, одержаний в результаті криптографічного перетворення повідомлення довільної довжини з використанням особистого (таємного) ключа відправника [1]. Процедура обчислення цифрового підпису побудована таким чином, що кожний цифровий підпис має унікальну структуру, пов’язану з повідомленням та ідентифікаційними даними власника особистого ключа. Перевірка цифрового підпису полягає в установленні істинності деяких алгебричних співвідношень між цифровим підписом та величинами, обчисленими за повідомленням, виходячи із зв’язку між відкритим та особистим ключами. Цей зв’язок не дає змоги відновити особистий ключ з відкритого. Таким чином, відкритий ключ є унікальним параметром, що дає змогу здійснити перевірку цифрового підпису конкретної особи.

Застосування ЕЦП дозволяє вирішити такі завдання:

- здійснити аутентифікацію джерела повідомлення;
- встановити цілісність повідомлення;
- забезпечити неможливість відмови від факту підпису конкретного повідомлення.

Еліптична криптографія - розділ криптографії, який вивчає асиметричні криптосистеми, що ґрунтуються на еліптичних кривих над скінченними полями [2]. Забезпечення неможливості обчислювально знайти особистий ключ цифрового підпису в таких системах спирається на задачу дискретного логарифмування в групах точок еліптичних кривих. На сьогодні невідомі субекспоненціальні алгоритми для вирішення даної задачі [3]. Тому при реалізації таких криптосистем на ЕОМ забезпечується еквівалентний рівень захисту при значно меншій кількості розрядів, внаслідок чого зменшується завантаження процесора. Саме у цьому полягає перевага застосування криптографічних алгоритмів, що базуються на еліптичних кривих.

Алгоритм ЕЦП за ДСТУ 4145-2002

Стандарт ДСТУ 4145-2001 установлює механізм цифрового підписування, що ґрунтується на властивостях груп точок еліптичних кривих над скінченними полями $GF(2^m)$, та правила застосування цього механізму до повідомлень, які пересилаються каналами зв'язку та/або обробляються у комп'ютеризованих системах загального призначення [4].

Елементи скінченного поля $GF(2^m)$

Елементи скінченного поля $GF(2^m)$ в поліноміальному базисі зображуються многочленами степеня не більше $m-1$ або, що еквівалентно, двійковими рядками довжини, що складаються з коефіцієнтів таких многочленів. Многочлен $f(t)$ степеня m над полем $GF(2)$ є многочлен виду

$$f(t) = t^m + f_{m-1}t^{m-1} + \cdots + f_0,$$

де коефіцієнти многочлена $f_i \in GF(2),\ i = 0, \ldots m-1$.

Операції над такими многочленами виконуються як операції над звичайними многочленами, тільки операції над коефіцієнтами виконуються в полі $GF(2)$. Зокрема, многочлен $g(t)$ ділиться з остачею $r(t)$ на многочлен $f(t)$, $f(t) \neq 0$, якщо $g(t)=h(t)f(t)+r(t)$, де степінь многочлена $r(t)$ менший за степінь многочлена $f(t)$. Многочлен $h(t)$ називається неповною часткою. Операція обчислення остачі від ділення многочлена $g(t)$ на многочлен $f(t)$ називається зведенням многочлена $g(t)$ за модулем $f(t)$ і позначається $g(t) \bmod f(t)$.

При виконанні обчислень у скінченному полі часто доводиться зводити результат за модулем примітивного многочлена. Ця операція займає багато процесорного часу при реалізації на ЕОМ, особливо при застосуванні методу простого ділення із остачею. Проаналізувавши існуючі методи швидкого зведення за модулем та перевіривши швидкість роботи цих методів в контексті даної задачі, можна сформувати обґрунтовані рекомендації щодо виконання математичних обчислень при реалізації даного алгоритму ЕЦП на ЕОМ.

Методи зведення за модулем многочленів

Многочлени над скінченним полем можуть бути представлені двійковими рядками довжини, що складаються з коефіцієнтів таких многочленів. Тому операція зведення за модулем над многочленами виконується аналогічно цій операції над цілими числами. Будемо розглядати обчислення остачі від ділення l -розрядного числа x (ділене) на k–розрядне число m (дільник). Введемо наступні позначення: b – основа

позиційної системи числення, у якій представлені числа (будь-яке ціле число >=2), k – кількість розрядів представлення числа m у b-системі.

Класичним методом є просте ділення у стовпчик. На кожному кроці алгоритму виконується ділення $(k+1)$-розрядного числа x на k-розрядний дільник m. Як наслідок отримують частку q та k-розрядну остачу r. На кожному кроці остача r буде меншим за m, тому вона об'єднується з наступною цифрою діленого у $(k+1)$-розрядне число $x = (r*b + наступна\ цифра\ діленого)$.

Метод обчислення ($x\ mod\ m$), запропонований Монтгомері у 1985 році полягає у наступному [5]. Частку знаходять шляхом багаторазового додавання m. Замість обчислення t одразу, обчислюється один розряд t_i, множиться на mb_i та додається з x.

Інший метод був запропонований Барретом у 1986 році [6]. Він базується на спостереженні, що вираз $q = x\ mod\ b$ еквівалентний виразу $q = x - m*[x/m]$. Для виконання обчислень за Барретом необхідне попереднє обчислення $\mu = b^{2k} div\ m$.

Було виконано зведення за модулем чисел за трьома наведеними алгоритмами. В табл.1 наведено середні швидкості обчислень на ЕОМ (AMD Athlon 64 Processor 3200+ 2.00 GHz, 3 Gb RAM). Розбиття по стовбцях відповідає бітовій довжині числа (128 біт, 256 біт і т.д.). Значення у ланках – кількість мілісекунд, затрачених на обчислення. Отримані результати дозволяють зробити висновок, що для обчислення остачі від ділення при реалізації на ЕОМ для невеликих чисел доцільніше використовувати метод Барретта, а для великих (понад 1024 біт) швидше працює алгоритм Монтгомері.

Таблиця 1.

Тестування швидкості зведення за модулем на ЕОМ

	128	**256**	**384**	**512**	**768**	**1024**	**2048**
Класичний метод	0,875	4,545	4,62	6,345	7,78	9,945	16,94
Метод Барретта	0,15	0,6	1,155	1,705	3,105	5,05	17,52
Метод Монтгомері	7,795	7,8	7,82	7,585	7,515	7,625	8,07

Висновок

В роботі розглянуто алгоритми зведення многочлена за модулем та експериментально встановлено швидкість роботи цих алгоритмів при реалізації на ЕОМ. Проведено тести при різних порядках многочленів. В

результаті аналізу отриманих результатів можна зробити висновок, що при реалізації на ЕОМ алгоритму ЕЦП за ДСТУ 4145-2002 операцію зведення многочленів за модулем слід реалізовувати двома методами – Монтгомері та Баррета. Вибір одного з цих методів повинен залежати від порядку многочлена, над яким виконується операція.

Подальші дослідження будуть пов'язані з дослідженням операцій, що використовуються при формуванні та валідації ЕЦП згідно з стандартом, які потенційно можна оптимізувати при реалізації на ЕОМ.

Література

1. *Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.* Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
2. *Болотов А.А., Гашков С. Б.* Алгоритмические основы эллиптической криптографии. – М.: МЭИ, 2000. –100 с.
3. *Жданов О.Н., Чалкин Т.А.* Применение эллиптических кривых в криптографии, СГАУ им. Решетнева. –22 с.
4. *О. Шаталов, А. Кочубінський*. ДСТУ 4145-2002. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка, м. Київ, 2003. –14-24 с.
5. *Montgomery P.* Modular Multiplication without Trial Division.// Mathematics of Computation. – 44, – 1985. –p.519-521.
6. *Barrett P.* Implementing the Rivest, Shamir and Addleman Public Key Encryption Algorithm on a Standard Digital Signal Processor.// Advances in Cryptology – Crypto'86 (LNCS 263), – 1986. –p.311-323.