

ПРИСКОРЕННЯ ЕКСПОНЕНЦІЮВАННЯ НА ПОЛЯХ ГАЛУА В СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ

В статті запропоновано новий спосіб прискорення експоненціювання на полях Галуа. В основу способу покладено використання результатів передобчислень при реалізації однієї з двох базових операцій експоненціювання – множення на основу. Детально описано процедури запропонованого способу: формування значень таблиці передобчислень та виконання операцій з ними. Теоретично доведено та практично підтверджено, що розроблений підхід забезпечує прискорення виконання операції експоненціювання на полях Галуа на 30%.

In article the new method of shortcut exponentiation on Galois fields is proposed. The method is based on utilization of precomputations on executing of multiplication by radix – one of two basis exponentiation operations. Procedures of the offered method, such as forming prediction table values and executing operations with them were described in details. It was proved in theory and confirmed by the experimental way that the offered method provides acceleration executing exponentiation operation on Galois fields by thirty per cents.

Вступ

Арифметичні операції, які виконуються на полях Галуа, відіграють важливу роль в сучасних інформаційних технологіях. Зокрема, вони покладені в основу більшості методів виявлення та корекції помилок при передачі й зберіганні даних, широко використовуються при кодовому ущільненні передачі інформації, в системах вимірювання та реєстрації даних.

Особливо важливу роль відіграють обчислення на полях Галуа в сучасних криптографічних механізмах захисту інформації: вони застосовуються в алгоритмі симетричного шифрування Rijndael, який став переможцем всесвітнього конкурсу AES, а також в механізмах асиметричного шифрування і цифрового підпису на основі еліптичних кривих [1]. У криптографії на основі еліптичних кривих базовою операцією є експоненціювання на полях Галуа, яка виконується над числами великої розрядності (512-1024 біт), що значно перевищує довжину слова сучасних процесорів.

Суттєвою складністю реалізації арифметики на полях Галуа є непристосованість до неї архітектури звичайних процесорних засобів, які орієнтовані на двійкову арифметику. Тому існує необхідність в розробці складних програмних засобів, що уповільнює виконання арифметичних операцій на полях Галуа [2].

Аналіз динаміки розвитку прикладних задач, в яких активно використовується арифметика на полях Галуа, показує, що більша їх частина виконується в реальному часі і потребує швидкої реалізації відповідних обчислень. Іншою

суттєвою особливістю використання арифметики на полях Галуа на сучасному етапі розвитку інформаційних технологій є збільшення розрядності чисел.

Все це вимагає розробки нових методів організації обчислень на скінченних полях. В першу чергу, це стосується найбільш трудомістких обчислювальних операцій, таких як експоненціювання.

Таким чином, наукова задача прискорення процедури експоненціювання на скінченних полях, що виконується над числами великої розрядності, є актуальною і важливою для сучасного етапу розвитку інформаційних технологій.

Аналіз способів експоненціювання на полях Галуа

Поле Галуа задається утворюючим нерозкладним поліномом $Q(x)$ степені $n+1$, якому співвідноситься $(n+1)$ -розрядне двійкове число M . Операція експоненціювання $A|E \bmod M$ на такому полі передбачає, що числа A та E являють собою n -розрядні двійкові коди: $A = \{a_0, a_1, \dots, a_{n-1}\}$ і $E = \{e_0, e_1, \dots, e_{n-1}\}$, $\forall j \in \{0, 1, \dots, n-1\}$, $a_j \in \{0, 1\}$, $e_j \in \{0, 1\}$, яким відповідають поліноми: $P(A) = a_0 + a_1 \cdot x + a_2 \cdot x^2 + \dots + a_{n-1} \cdot x^{n-1}$ та $P(E) = e_0 + e_1 \cdot x + e_2 \cdot x^2 + \dots + e_{n-1} \cdot x^{n-1}$.

До теперішнього часу запропоновано ряд способів виконання операції експоненціювання на полях Галуа [2-5]. Їх аналіз показує, що в якості підвищення швидкодії їх автори розглядають можливість розпаралелювання виконан-

ня при апаратній реалізації базової операції експоненціювання – множення на полях Галуа.

Сама процедура модулярного експоненціювання $A|E \text{ rem } M$ на полях Галуа, як і звичайне модулярне експоненціювання, зводиться до послідовного виконання n циклів, у кожному з яких здійснюється операція піднесення до квадрату отриманого на попередньому циклі результату (R^2) і, додатково, в залежності від поточного біту експоненти E , – операція множення ($R \otimes A$) без переносів. Досліджується модулярне експоненціювання зліва направо, тобто аналіз розрядів експоненти E виконується починаючи зі старших розрядів. Структурно цей спосіб обчислення експоненти $A|E \text{ rem } M$ на полях Галуа показано на рис. 1.

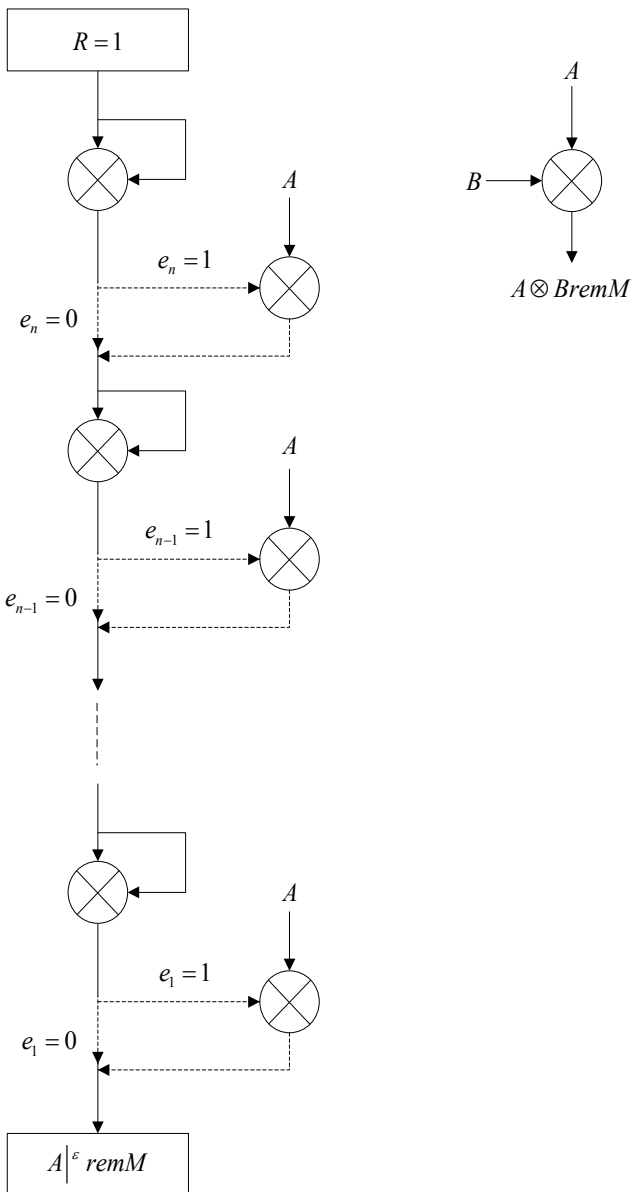


Рис.1. Структура операції експоненціювання

Наприклад, при обчисленні $14|^{10} \text{ rem } 19=6$, $n=4$, $A=14_{10}=1110_2$; $E=10_{10}=1010_2$; $M=19_{10}=10011_2$ динаміка перетворення змінних у відповідності з наведеним на рис.1 алгоритмом представлена в таблиці 1.

Для оцінки швидкодії доцільно провести аналіз виконання процесором базових операцій експоненціювання.

Позначимо за n розрядність числа, а за w – розрядність процесору. На практиці розрядність чисел n значно перевищує розрядність процесору w ($n \gg w$), тому обробка виконується w -розрядними фрагментами, кількість яких дорівнює $s = n / w$.

Табл. 1. Цифрова діаграма змінних при виконанні експоненціювання $14|^{10} \text{ rem } 19=6$.

i	e_i	$R \otimes R \text{ rem } 19$	$R \otimes A \text{ rem } 19$	R
3	1	1	1110 ₂	1110 ₂
2	0	1011 ₂	-	1011 ₂
1	1	1001 ₂	0111 ₂	0111 ₂
0	0	0110 ₂	-	0110 ₂

Операція множення виконується за n циклів, кожен з яких складається з операції зсуву n -розрядного множеного та, за умови, що поточний розряд множника дорівнює одиниці, – операції логічного додавання.

Для зсуву n -розрядного числа на один розряд необхідно виконати $(s+1)$ процесорних операцій зсуву, причому ця операція виконується в кожному циклі множення, відповідно сумарна кількість процесорних операцій зсуву становить $(s+1) \cdot n$.

Вважаючи, що значення розрядів множника з рівною ймовірністю можуть приймати значення як 0, так і 1, то, в середньому, операція додавання виконується в $n/2$ циклах. Для логічного додавання n -розрядних чисел слід виконати $(s+1)$ процесорну операцію, так що сумарна кількість операцій при додаванні становить: $(s+1) \cdot (n/2)$.

Отже, загальний час виконання множення без переносів n -розрядних чисел T_{mc} дорівнює:

$$T_{mc} = (s+1) \cdot n \cdot \tau + (s+1) \cdot (n/2) \cdot \tau = 1.5 \cdot n \cdot (s+1) \cdot \tau,$$

де τ – час виконання однієї логічної операції.

Операція множення на полях Галуа передбачає після виконання множення без переносів реалізацію редукції отриманого результату,

тобто приведення його в рамки поля. Редукція виконується шляхом віднаходження залишку від поліноміального ділення $(2 \cdot n - 1)$ -розрядного результату множення без переносів на $(n + 1)$ -розрядний код утворюючого поліному M поля. Реалізація редукції передбачає виконання $(n - 1)$ циклів, в кожному з яких відбувається зсув на один розряд $(n + 1)$ -розрядного коду M та додавання його до поточного залишку в разі, коли його старший розряд дорівнює одиниці. Для зсуву $(n + 1)$ -розрядного коду M на один розряд потрібно виконати $(s + 1)$ процесорних операцій зсуву. Так як ця операція виконується в кожному з $(n - 1)$ циклів редукції, то сумарна кількість процесорних операцій зсуву складає $(s + 1) \cdot (n - 1)$. Виходячи з того, що в процесі редукції операція додавання, в середньому, виконується в половині циклів, то середня кількість таких операцій становить $(n - 1) / 2$. Приймаючи до уваги, що для реалізації цієї операції на w -розрядному процесорі потрібно виконати $(s + 1)$ процесорних операцій додавання, середня кількість процесорних операцій для редукції результату множення становить $(s + 1) \cdot (n - 1) / 2$. Відповідно, середній час T_R виконання редукції результату множення складає

$$T_R = 1.5 \cdot (s + 1) \cdot (n - 1) \cdot \tau.$$

Таким чином, загальний час T_{mGF} виконання операції множення на полі Галуа дорівнює:

$$T_{mGF} = T_{mc} + T_R - 3 \cdot (n - 1) \cdot (s + 1) \cdot \tau \approx 3 \cdot n \cdot s \cdot \tau \quad (1)$$

Враховуючи, що значення розрядів експоненти з рівною ймовірністю приймають значення нуля та одиниці, то операція множення на основу виконується, в середньому, в $n/2$ циклах. Відповідно, при звичайному експоненціюванні загальний час T_e експоненціювання становить:

$$T_e = 1.5 \cdot n \cdot T_{mGF} \approx 4.5 \cdot n^2 \cdot s \cdot \tau \quad (2)$$

Експоненціювання з використанням передобчислень

Проведений аналіз операції експоненціювання показав, що операція множення на постійне число повторюється, в середньому, $n/2$ о раз. Тому доцільно виконати передобчислення, результати яких будуть використовуватися на всіх етапах обчислення і, тим самим, прискорити процес експоненціювання.

Зокрема, пропонується використання результатів передобчислень при виконанні множення проміжного результату на код основи A . Результати передобчислень зберігаються в таблиці, формування якої виконується перед обчисленням $A|^E \bmod M$ шляхом здійснення редукції зсунутих значень A : $T[0]=A$, $T[1]=A \cdot 2 \bmod M$, $T[3]=A \cdot 2^2 \bmod M$, ..., $T[n-1]=A \cdot 2^{n-1} \bmod M$.

Відповідно, для множення n -розрядного проміжного результату $R = \{r_0, r_1, \dots, r_{n-1}\}$, $\forall j \in \{0, 1, \dots, n-1\}$ $r_j \in \{0, 1\}$, на код A в процесі експоненціювання на полях Галуа пропонується наступний алгоритм:

1. $s=0$; $i=0$.
2. Якщо $r_i = 1$, то $s = s \oplus T[i]$.
3. $i = i + 1$
4. Якщо $i < n$, повернення на пп.2.

Запропонований спосіб ілюструється в рамках наведеного вище прикладу експоненціювання $14|^{10} \bmod 19$, ($n=4$, $A=14_{10}=1110_2$; $M=19_{10}=10011_2$).

У відповідності із запропонованим способом перед процедурою експоненціювання виконується заповнення таблиці результатів передобчислень. $T[0]=A=1110_2$; $T[1]=A \cdot 2 \bmod M = 11100_2 \oplus 10011_2 = 1111_2$; $T[2] = A \cdot 2^2 \bmod M = T[1] \cdot 2 \bmod M = 11110_2 \oplus 10011_2 = 1101_2$; $T[3]=A \cdot 2^3 \bmod M = T[2] \cdot 2 \bmod M = 11010_2 \oplus 10011_2 = 1001_2$.

На третьому кроці експоненціювання для $R = \{1, 0, 0, 1\}$ виконується множення $R \otimes A \bmod 19 = 1001_2 \otimes 1110_2 \bmod 19 = 126 \bmod 19 = 7 = 0111_2$ (третій рядок таблиці 1). При виконанні цієї операції з використанням передобчислень у відповідності з запропонованим алгоритмом множення на число A реалізується у вигляді: $R = T[0] \oplus T[3] = 1110_2 \oplus 1001_2 = 0111_2$.

Для формування $n-1$ значень таблиці передобчислень для n -розрядного числа A необхідно виконати $n-1$ циклів. На кожному з циклів треба робити зсув попередньо отриманого результату і, при необхідності, приведення його в рамки поля, тобто редукцію. Операція зсуву n -розрядного числа на w -розрядному процесорі займає $s+1$ процесорних операцій. Редукція $(n+1)$ -розрядного результату зсуву полягає в додаванні до цього $(n+1)$ -розрядного коду утворюючого поліному P за умови, що старший розряд результату зсуву дорівнює одиниці. Оскільки цей розряд з рівною ймовірністю приймає

одиничне і нульове значення, редукція проводиться, в середньому, на половині циклі заповнення таблиці. Приймаючи до уваги, що додавання $(n+1)$ -розрядних чисел потребує $s+1$ процесорних операцій логічного додавання, то середній час T_T формування таблиці передобчислень становить:

$$T_T = 1.5 \cdot (s+1) \cdot (n-1) \cdot \tau \approx 1.5 \cdot s \cdot n \cdot \tau \quad (3)$$

При експоненціюванні на полях Галуа з використанням таблиць передобчислень вся процедура експоненціювання залишається такою ж, а змінюється лише множення на основу. Тому доцільно провести аналіз виконання даної операції процесором. Для початку, слід виконувати множення основи на проміжний результат, адже за такої умови множене залишається незмінним і значення таблиць вибираються відповідно до значень розрядів проміжного результату.

При множенні n -розрядної основи на проміжний результат з використанням результатів передобчислень виконується n циклів. В кожному з них виконується операція логічного додавання n -розрядного коду з таблиці. Так як коди таблиці n -розрядні, то їх додавання складається з s процесорних операцій. В результаті логічного додавання розрядність результату не змінюється, а відповідно, редукцію результату проводити не потрібно.

Таким чином, виконання процесором операції множення основи на проміжний результат з використанням таблиць передобчислень займає час T_{TGF} , рівний:

$$T_{TGF} = n \cdot s \cdot \tau. \quad (4)$$

Порівнюючи (4) та (1) можна зробити висновки, що використання передобчислень дозволяє скоротити час виконання операції множення на полях Галуа не менше, ніж в 3 рази.

Оцінка часу експоненціювання

При експоненціюванні n -розрядного числа A на полях Галуа виконується n кроків, відповідно до розрядів експоненти, на кожному з яких здійснюється піднесення до квадрату, та, за умови, що поточний розряд n -розрядної експо-

ненти E дорівнює одиниці, – множення його на основу A .

Якщо виконувати експоненціювання запропонованим способом, тобто з використанням таблиць передобчислень, то необхідно сформувати таблиці, а потім в n циклах виконується піднесення проміжного результату до квадрату і в $n/2$ циклах – множення на основу. Відповідно, час, який витрачається на ці операції:

$$T_{eT} = n \cdot T_{mGF} + 0.5 \cdot n \cdot T_{TGF} + T_T = 3 \cdot n^2 \cdot s \cdot \tau + 0.5 \cdot n^2 \cdot s \cdot \tau + 1.5 \cdot s \cdot n \cdot \tau \quad (5)$$

Час, який витрачається на піднесення проміжного результату до квадрату та множення на основу, пропорційний n^2 , а час формування таблиць згідно (3) пропорційний до n . Тому, враховуючи, що розрядність чисел $n > 1000$, часом формування таблиць можна знехтувати.

Таким чином, загальний час експоненціювання на полях Галуа з використанням передобчислень становить:

$$T_{eT} = n \cdot T_{mGF} + 0.5 \cdot n \cdot T_{TGF} \approx 3.5 \cdot n^2 \cdot s \cdot \tau \quad (6)$$

Співвідношення часу класичної процедури експоненціювання, що визначається (2) та часу експоненціювання за запропонованим способом, що визначається (6) становить:

$$T_e / T_{eT} = 4.5 / 3.5 \approx 1.3$$

Отже, використання при експоненціюванні на полях Галуа результатів передобчислень дозволяє скоротити час виконання цієї операції в рази, тобто приблизно на 30%.

Висновки

В результаті проведених досліджень розроблено новий спосіб прискорення операції експоненціювання на полях Галуа з використанням таблиць передобчислень при виконанні однієї з двох базових операцій – множення на основу.

За рахунок того, що виконання множення на основу прискорюється втричі у порівнянні зі класичною процедурою множення на полях Галуа, розроблений підхід дозволяє скоротити час експоненціювання на 30% порівняно зі звичайною реалізацією експоненціювання.

Список літератури

1. Menezes A.J., Blake I.F., Gao S., Mullin R.C., Vanstone S.A., Yacobi T. Application of Finite Fields.//N.Y. Kluwer Academic Published.-1993.-387p.
2. Стефанская В.А., Мухаммад Мефлех Алиса Абабне, Левчун Д.Ю. К проблеме повышения эффективности аппаратной реализации мультипликативных операций на полях Галуа // Вісник Національного технічного університету України «КПІ». Інформатика, управління та обчислювальна техніка. К., «ВЕК++», -2005.-№43.-с.104-112.
3. Popovici E.M., Fitzpatrick P. Algorithm and Architecture for a Galois Field Multiplicative Arithmetic Processor.// IEEE Transaction on Information theory. Vol. 49.– № 12,-2003.-pp.3303-3307.
4. Wu H., Hasan M.A., Blake I.F., Gao S. Finite field multiplier using redundant representation.// IEEE Trans. Computers, Vol. 51.– № 51, – 2002. – pp.1306-1316.
5. Марковский А.П., Шаршаков А.С. Способ ускоренной реализации экспоненцирования на полях Галуа в системах защиты информации // Збірник наукових праць НАУ. Проблеми інформатизації та управління – 2011, №1(32) – 188с.