УДК 004.056.5

МАРКОВСЬКИЙ О.П.,
ВИНОГРАДОВ Ю.М.,
КОСЕЙКІНА Г.С.

СПОСІБ ПРИСКОРЕНОГО ОБЧИСЛЕННЯ КОРЕНІВ НА ПОЛЯХ ГАЛУА GF (2^m) З ВИКОРИСТАННЯМ ПЕРЕДОБЧИСЛЕНЬ

В статті запропоновано спосіб прискореного обчислення кореня на полях Галуа GF (2^m). Основною особливістю запропонованого способу є багаторазове використання результатів передобчислень, які обчислюються лише один раз. Детально викладена запропонована технологія виконання передобчислень, наведено приклади. Досліджено, як ця технологія прискорює обчислення кореня на полях Галуа GF (2^m). Доведено, що обчислювальна складність O*(m)* наведеного способу істотно менша за складність відомих способів, яка становить O*(m^2)*.

In article the method of accelerated calculation of square root on Galois fields GF (2^m) has been proposed. The main feature of proposed method is using results of precalculations many times, which are calculated only once. The technology of executing of precalculations is given in details, examples are given. It is researched how proposed technology accelerates calculation of square root on Galois fields GF (2^m). It is proved, that calculation complexity O*(m)* of proposed method is much smaller then complexity of known methods, which equals O*(m^2)*.

Вступ

В обчислювальній алгебрі та в теорії чисел дуже важливими є розв'язання рівнянь на кінцевих полях, тобто на полях Галуа [1]. На сучасному етапі розвитку інформаційних технологій, крім теоретичного інтересу, ця задача є значимою в практичному сенсі, оскільки вона грає важливу роль в інформаційних технологіях для корекції помилок, кодування та стиснення даних. Поштовхом до розвитку технологій розв'язання рівнянь на полях Галуа стало практичне використання криптографічних систем захисту інформації, основаних на еліптичних кривих та інших різновидах Абелевих груп [2].

В багатьох технологіях розв'язання алгебраїчних рівнянь на кінцевих полях необхідне обчислення квадратного кореня. Наприклад, квадратний корінь потрібен для стиснення та відновлення точки на еліптичній кривій [3]. Точка з координатами (x,y) на кривій стискається до вигляду (x,β), де $\beta \in \{0,1\}$. Щоб відновити y по (x,β), необхідно розв'язати квадратне рівняння $y^2 = P(x)$, тобто обчислити квадратний корінь $\sqrt{P(x)}$. Такі обчислення потрібні при хешуванні на еліптичних кривих, що широко використовується в багатьох криптосистемах [4].

Обчислення квадратних коренів на полях Галуа використовуються і для більш складних задач, наприклад, при оцінці рівня взаємної кореляції багатовимірних сигналів. Значна частина застосувань обчислення коренів виконується в реальному часі, тому швидкість обчислень є принципово важливим фактором.

Обчислення квадратного кореня на полях Галуа GF(2^m) є однією з найбільш складних для обчислення операцій і від швидкості її реалізації значною мірою залежить продуктивність засобів корекції помилок, кодування та стиснення даних, а також систем криптографічного захисту інформації. В існуючих методах обчислення квадратного кореня на полях Галуа GF(2^m) час виконання пропорційний m^2. Таким чином, час обчислення суттєво залежить від розрядності поля.

На сучасному етапі розвитку інформаційних технологій широкого розповсюдження набувають розподілені та хмарні обчислення, які дозволяють сконцентрувати значні обчислювальні потужності для розв'язання певних задач. Серед цих задач можуть бути і задачі, пов'язані з порушенням криптографічного захисту. Таким чином, зворотною стороною розповсюдження розподілених та хмарних обчислень є збільшення потенційних можливостей зловмисників для злому існуючих систем захисту інформації. Єдиним адекватним способом протидії цій новій загрозі, тобто підвищення кріптостійкості є збільшення розрядності поля Галуа, що має наслідком експоненційне зростання об'єму обчислювальних ресурсів для злому криптосистеми. З іншого боку, при існуючих технологіях обчислення кореня, збільшення розрядності чисел на полях Галуа призводить до квадратичного росту об'ємів обчислень, потрібних для

віднаходження квадратного кореня, що суттєвим чином уповільнює роботу систем захисту інформації.

Виходячи з цього, виникає необхідність в створенні методів криптографічних перетворень, в тому числі обчислення квадратного кореня на полях Галуа, обчислювальна складність яких лінійно залежить від розрядності поля Галуа.

Таким чином, задача прискорення обчислення квадратного кореня на полях Галуа є актуальною та важливою для сучасного етапу розвитку інформаційних технологій.

Аналіз відомих методів обчислення коренів на кінцевих полях

Важливість задачі обчислення квадратного кореня на кінцевих полях у практичному сенсі, особливо в системах криптографічного захисту інформації на основі еліптичних кривих, стимулює інтенсивні дослідження в області методів вирішення цієї задачі. Більше сторіччя тому були запропоновані базові методи для обчислення квадратного кореня на полях Галуа GF (2^m): Tonelli [1] та Cipolla [4].

Пізніше ці методи були модифіковані для випадку поля GF (q^m), де q – просте число і отримали відповідні назви: Tonelli-Shanks [3] та Cipolla-Lehmer [1]. В 1977 році метод Tonelli-Shanks було модифіковано для обчислення кореня довільного ступеню [4]. Існує також метод обчислення кубічного кореня, що має підвищену швидкодію [2].

Базовими операціями на полях Галуа GF (2^m) є додавання та множення їх елементів. Перша з цих операцій відповідає додаванню в поліноміальній математиці, тобто по суті є операцією додавання за модулем 2 (xor) і нижче позначається символом ‘+’. Операція множення на полях Галуа GF (2^m) відбувається двома етапами. Спершу виконується поліноміальне множенням (тобто множення без переносів), що нижче позначається як ‘⊗’. Потім виконується редукція результату, тобто знаходження залишку від поліноміального ділення добутку на утворюючий поліном поля. Операція редукції нижче позначається як ‘rem’, на відміну від арифметичної редукції ‘mod’.

Для кожного елементу поля Галуа GF (2^m), що утворюється нерозкладним поліномом $P(x)$ ступеню m, якому відповідає число p, існує мультиплікативна циклічна група, порядок n якої не перевищує 2^m-1. Порядок циклічної групи дорівнює 2^m-1, якщо її генератор не має спільних дільників з 2^m-1.

В кожній циклічній групі поля GF (2^m) може бути виділена циклічна підгрупа, кожен елемент якої є квадратом попередньої. При цьому порядок кожної з квадратичних підгруп не перевищує $\log_2 n$, тобто не перевищує m.

Суть методу Tonelli-Shanks знаходження квадратного кореня на полях Галуа полягає в тому, що послідовно аналізуються елементи циклічної підгрупи до знаходження її елемента, який передує підкореневому числу. В процедурному значенні прохід по квадратичній циклічній підгрупі еквівалентний до операції експоненціювання [2]:

$$B = A^{2^{m-1}} rem(p). \qquad (1)$$

Таким чином, ідея обчислення квадратного кореня на полях Галуа, що лежить в основі методу Tonelli-Shanks, теоретично є дуже простою, але практична її реалізація пов’язана з значними витратами обчислювальних ресурсів, оскільки реалізація (1) потребує виконання m-1 операцій піднесення до квадрату та редукції. Піднесення до квадрату виконується за правилами поліноміального множення, тобто переноси не враховуються. Операція піднесення до квадрату може бути ефективно реалізована з використанням важливої властивості: в двійковій формі представлення квадрата числа A розряди, що знаходяться на парних позиціях, дорівнюють нулю, а непарні розряди дорівнюють відповідним розрядам числа A, тобто, якщо $A=a_0+a_1\cdot 2+a_2\cdot 2^2+...+a_{m-1}\cdot 2^{m-1}$, то:

$$A \otimes A = A^2 = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + ... + a_{m-1} \cdot 2^{2m-2}. \qquad (2)$$

З наведеної властивості випливає, що обчислення поліноміального квадрату не потребує обчислювальних операцій, а зводиться лише до перестановки розрядів числа A.

Для оцінки обчислювальної складності операції знаходження квадратного кореня за методом Tonelli-Shanks слід врахувати, що розрядність елементів поля істотно перевищує розрядність процесора, тобто при виконанні операції елементи поля розбиваються на s секцій, де s – результат ділення кількості розрядів елементу на кількість розрядів процесору.

Редукція виконується шляхом обчислення залишку від поліноміального ділення ($2\cdot m$-1)-розрядного коду p та його логічне додавання до коду поточного залишку в випадку, коли старший розряд останнього дорівнює одиниці. Для

зсуву (m+1)- розрядного коду p на один розряд потрібно виконати (s+1) процесорних операцій зсуву. Оскільки ця операція виконується в кожному з (m-1) циклів редукції, то сумарна кількість процесорних операцій зсуву становить (s+1)·(m-1). Враховуючи що в процесі редукції додавання виконується, в середньому, в половині циклів, а також те, що для реалізації додавання 2·m-розрядного коду потрібно (s+1) операцій логічного додавання, загальна кількість операцій редукції становить (s+1)·(m-1)/2. З цього випливає, що середній час редукції результату піднесення до квадрату становить 1.5·(s+1)·(m-1)· τ, де τ – час виконання на процесорі логічної операції. Тобто, для реалізації (m-1) операції піднесення до квадрату для обчислення квадратного кореня на полі Галуа, в середньому потрібна наступна кількість логічних операцій:

$$N_T = 1.5 \cdot (s+1) \cdot (m-1)^2. \qquad (3)$$

Таким чином, з формули (3) випливає, що обчислювальна складність розглянутого методу Tonelli-Shanks становить O(m^2). Аналогічну оцінку складності має і метод Cipolla-Lehmer [1]. Квадратична залежність складності обчислення кореня відомими методами від розрядності чисел в умовах її зростання має наслідком різке сповільнення реалізації систем захисту інформації на основі еліптичних кривих. Для прискорення обчислень потрібно розробити нові методи віднаходження квадратного кореня.

Відомі методи обчислення квадратного кореня на полях Галуа GF (2^m) вирішують цю задачу без врахування особливостей її практичного використання. Врахування таких особливостей є важливим резервом підвищення швидкості реалізації обчислення кореня.

Ціллю досліджень є прискорення обчислення однієї з базових операцій криптографічних систем на основі еліптичних кривих – віднаходження квадратного кореня на полях Галуа.

Спосіб прискореного обчислення квадратного кореня з використанням передобчислень

В реальних системах захисту інформації з відкритим ключем, що використовують поля Галуа, їх утворюючий поліном залежить тільки від ключа і змінюється доволі рідко, тобто його можна вважати постійним. Відповідно, ефективним підходом для прискорення обчислення квадратного кореня на полях Галуа є використання попередніх обчислень, що залежать від утворюючого поліному та виконуються один раз. Результати цих обчислень зберігаються у таблицях та використовуються при кожному обчисленні квадратного кореня на полях Галуа.

На основі вказаного підходу пропонується спосіб прискореного обчислення квадратного кореня на полях Галуа. Число A можна представити у вигляді логічної суми: $A=a_0+a_1\cdot 2+a_2\cdot 2^2+...+a_{m-1}\cdot 2^{m-1}$, де $a_0,\ldots,a_{m-1}\in\{0,1\}$. Оскільки при парному n логічна сума має властивість: $(a+b)^n = a^n + b^n$,то формула (1) для обчислення квадратного кореня $B=\sqrt{A}$ може бути представлена у вигляді:

$$\begin{aligned} B &= A\Big|^{2^{m-1}} \operatorname{rem} p = = \\ & a_0 + a_1 \cdot 2\Big|^{2^{m-1}} + ... + a_{m-1}\cdot 2^{m-1}\Big|^{2^{m-1}} \operatorname{rem} p = \\ &= a_0 + a_1 \cdot 2\Big|^{2^{m-1}} \operatorname{rem} p + \ldots + a_{m-1}\cdot 2^{m-1}\Big|^{2^{m-1}} \operatorname{rem} \\ & p = = a_0 + a_1 \cdot 2^{2\cdot 2^{m-1}} \operatorname{rem} p + \ldots + a_{m-1}\cdot 2^{(m-1)\cdot 2^{m-1}} \\ & \operatorname{rem} p. \end{aligned} \qquad (4)$$

Якщо попередньо обчислити добутки чисел, які представляють собою ступені двійки та їх редукції, і позначити результати як W_i, то формула (4) може бути представлена таким чином:

$$B = a_0 \cdot W_0 + a_1 \cdot W_1 + a_2 \cdot W_2 + ... + a_{m-1} \cdot W_{m-1}. \qquad (5)$$

Отримана формула може бути безпосередньо використана для швидкого обчислення квадратного кореня. Запропонований спосіб може бути проілюстровано наступним прикладом. Нехай поле Галуа утворено поліномом $P(x)=x^3+x^2+1$. p=16, m=3. W_0=1, $W_1=2^5$rem16=2, $W_2=2^{11}$rem16=10. Обчислимо на цьому полі корінь з числа A=7. В двійковому вигляді це число дорівнює 111. Відповідно корінь з нього обчислюється як логічна сума:

$$B = W_0 + W_1 + W_2 = 1 + 2 + 10 = 3. \qquad (6)$$

Нескладно побачити, що кількість логічних операцій, що використовуються в наведеному способі, залежить від числа одиничних бітів коду A. Якщо взяти кількість цих розрядів як половину від загального числа розрядів, то кількість логічних операцій можна обчислити за формулою:

$$N_T = 0.5 \cdot s \cdot m. \qquad (7)$$

Порівняння виразів (7) і (3) показує, що запропонований спосіб дозволяє зменшити кількість операцій в 3·m разів.

Для експериментальної оцінки ефективності розробленого методу було проведено експериментальне дослідження програмної реалізації

обчислення квадратного кореня за запропонованим методом та методом Tonelli-Shanks. Програму було виконано з різними розрядностями поля Галуа, m=512, m=1024, m=2048. Реалізація методів була протестована на системі HP Blade System C3000.

Дані порівняльного аналізу швидкодії запропонованого способу обчислення квадратного кореня на полях Галуа і метода Tonelli-Shanks за результатами експериментальних досліджень наведено у вигляді графіку на рис.1. Досліджувалась залежність відношення T_{SH}/T_0 часу виконання обчислення квадратного кореня методом Tonelli-Shanks (T_{SH}) та запропонованого способу (T_0) для найбільш поширених на практиці значень m=512, 1024, 2048.

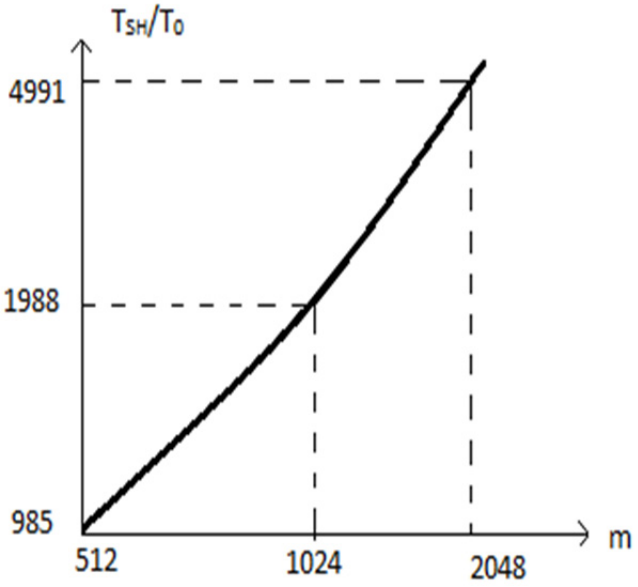

Рис.1 Графік залежності T_{SH}/T_0 від m

Аналіз наведеного графіку показує, що експериментальні оцінки ефективності запропонованого способу в цілому співпадають з теоретичними значеннями і доводять практичну доцільність використання запропонованого способу обчислення кореня на полях Галуа в системах криптографічного захисту з відкритим ключем на основі еліптичних кривих.

Висновки

Запропоновано спосіб прискореного обчислення квадратного кореня на полях Галуа. Спосіб орієнтовано на використання в системах криптографічного захисту інформації з відкритим ключем. Виходячи з того, що ключі в таких системах є практично незмінними, обчислювальна складність операції віднаходження кореню може бути зменшена за рахунок передобчислень, що залежать тільки від ключа. Це дозволило суттєво зменшити обчислювальну складність віднаходження квадратного кореня на полях Галуа в порівнянні з відомими методами. Теоретично доведено, що запропонований спосіб має обчислювальну складність O(m), значно меншу за складність O(m^2) існуючих способів, які не враховують конкретики застосування операції знаходження квадратного кореня в системах криптографічного захисту. Вважаючи на те, що в реальних системах значення m вимірюється тисячами бітів, запропонований метод дозволяє на порядки прискорити операції віднаходження кореня на полях Галуа. Проведені експериментальні дослідження в цілому підтвердили високу практичну ефективність розробленого методу.

Запропонований спосіб може бути ефективно використаний для реалізації систем криптографічного захисту інформації з відкритим ключем для застосувань з підвищеними вимогами щодо швидкодії, в тому числі з такими, що працюють в реальному часі.

Список літератури

1. Агуров П.В. Интерфейс USB. Практика использования и программирования / П.В. Агуров – СПб.:БХВ-Петербург, 2005.- 576 с.
2. Klove T. Error Detecting Codes: General Theory and Their Application in Feedback Communication Systems / T. Klove, V. Korzhik.- Norwell, MA: Kluwer, 1995. – 433 p.
3. Zumbragel J. On the Pseudocodeword Redundacy of Binary Linear Codes / J. Zumbragel, V. Skachek, M.F. Flanagan // IEEE Trans. of Information Theory.-2012.-Vol.58.- № 7.-P.4848-4861.
4. Марковский А.П. Использование взвешенных контрольных сумм для обнаружения ошибок в линиях передачи с асинхронным кодированием данных/ А.П. Марковский , Пуя Солеймани Нежадиан, Мулки Ахмед Яссин Ал Бадайнех. //Современные информационные и электронные технологи: 9-тая междунар. науч.-техн. конф., 19-22 мая. 2008 р.: тезисы докл. – Одесса., 2008.- С.201.