УДК 004.056.5

DOI: 10.18372/2073-4751.79.19371

Селіванов В.Л., к.т.н.,
orcid.org/0000-0001-8519-6038,
e-mail: ya.kulakov@gmail.com,
Аль-Мріят Гассан Абдель Жаліль,
e-mail: grayatjo@gmail.com

МЕТОД МОДУЛЯРНОГО МНОЖЕННЯ НА ПОСТІЙНЕ ЧИСЛО ДЛЯ ШВИДКОЇ РЕАЛІЗАЦІЇ КРИПТОГРАФІЇ З ВІДКРИТИМ КЛЮЧЕМ В IoT

**Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»**

Вступ

Концепція криптографії з відкритим ключем з'явилася наприкінці 70-х років минулого століття і нині стала однією з фундаментальних основ сучасних систем інформаційної безпеки. Вона дозволяє створювати гнучкі та ефективні системи для вирішення широкого спектру задач, пов'язаних з розмежуванням прав доступу до даних. Саме тому, більшість існуючих протоколів захисту інформації в тій чи іншій формі використовують криптографію з відкритим ключем.

Разом з тим, від початку практичного використання криптографії з відкритим ключем добре відомий її основний недолік – потреба з значних обчислювальних ресурсах для реалізації покладених в її основу незворотних перетворень теорії чисел. Базовою обчислювальною операцією переважної більшості криптографії з відкритим ключем є модулярне експоненціювання $A^E \bmod M$, яке здійснюється над числами, довжина яких значно перевищує розрядність процесора. Зокрема, на сьогоднішній день для більшості практичних застосувань довжина чисел, які використовуються в криптографії відкритих ключів становить 4096 і більше. Застосування таких довгих чисел зумовлено вимогами інформаційної безпеки. Розширення використання хмарних технологій, які потенційно надають зловмисникам можливість концентрації значних обчислювальних ресурсів для порушення захисту мають наслідком подальше збільшення розрядності чисел задля забезпечення потрібного рівня захищеності. З огляду на те, що подвоєння розрядності чисел в восьмеро збільшує об'єм обчислень, актуальність проблеми швидкої реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання має перспективу для подальшого зростання. Для потужних обчислювальних платформ вказана проблема вирішується за рахунок використання спеціалізованих криптопроцесорів, які дозволяють на два порядки прискорити обчислення модулярної експоненти. Для малопотужних вбудованих мікроконтролерів систем віддаленого моніторингу стану та управління об'єктами реального світу через мережу Інтернет проблема швидкого обчислення модулярної експоненти над довгими числами задля забезпечення інформаційної безпеки залишається гострою.

Таким чином, наукова задача прискорення модулярного експоненціювання чисел великої розрядності є актуальною з позицій особливостей сучасного етапу розвитку інформаційних і комп'ютерних технологій.

Огляд сучасних технологій реалізації мультиплікативних операцій модулярної арифметики

Проблема швидкої комп'ютерної реалізації широкого спектру механізмів захисту інформації криптографії з відкритим ключем на різних обчислювальних платформах стимулює створення значної кількості підходів до її практичного вирішення. Умовно їх можна розділити на три групи:

- використання спеціалізованих апаратних засобів – криптопроцесорів та

криптоприскорювачів для швидкої реалізації базової операції зазначеної вище криптографії – модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесора [1]. Цей підхід знайшов широке застосування для комп'ютерних платформ середньої та високої потужності. Для термінальних платформ використання потужних крипто процесорів стримується їх високою вартістю та високим рівнем споживання потужності;

- застосування альтернативних алгебраїчних базисів, обчислення в яких здійснюються простіше і можуть виконуватися паралельно. Найбільш широкого використання цей підхід набув в рамках застосування алгебри кінцевих полів Галуа $GF(2^n)$ [2]. Суттєва перепона використанню альтернативних алгебр для прискорення криптографії з відкритим ключем на термінальних мікроконтролерах полягає в орієнтації їх архітектури на традиційну алгебру;
- вдосконалення процедур обчислення модулярної експоненти за рахунок зменшення об'єму обчислень за рахунок виключення дублювання, використання передобчислень, адаптації до архітектури процесорних засобів.

Останній підхід вбачається найбільш придатним при реалізації механізмів криптографічного захисту з відкритим ключем на малопотужних термінальних мікроконтролерах *IoT*.

Практичне обчислення модулярної експоненти $A^E \bmod M$ здійснюється за одним із двох різновидів класичного алгоритму [3], який складається з n ітерацій, дії в кожному з яких залежать від поточного біту коду експоненти. Відповідно, згадані вище різновиди визначаються напрямком сканування бітів коду експоненту. В разі їх сканування починаючи з молодших розрядів, алгоритм передбачує використання двох змінних: D та R, початкові значення яких дорівнюють відповідно A та одиниці. В кожній ітерації, за умови, що поточний біт експоненти дорівнює одиниці, здійснюється операція модулярного множення $R = R \cdot D \bmod M$; після чого завжди виконується $D = D^2 \bmod M$. В іншому різновиді алгоритму модулярного експоненціювання, тобто при скануванні розрядів експоненти від старших до молодших, використовується лише одна змінна R, яка на початку встановлюється в одиницю. В кожній ітерації, спочатку виконується операція модулярного піднесення до квадрату: $R = R^2 \bmod M$, після чого, за умови, що поточний біт експоненти дорівнює одиниці, здійснюється операція модулярного множення R на постійне число A: $R = R \cdot D \bmod M$.

Обидва різновиди класичного алгоритму мають строго послідовний характер. Частково може суміщатися в часі виконання обчислень в рамках однієї ітерації для першого різновиду [3]. Тому основні зусилля дослідників зосереджені на можливості прискорення двох складових класичного алгоритму: модулярних операцій піднесення до квадрату [4] та множення [5]. Обидві ці операції складаються з двох фаз: власне множення (піднесення до квадрату) та модулярної редукції, тобто обчислення залишку від ділення на модуль M. Ці дві фази можуть виконувати послідовно, або поєднуватися. Найбільш відома технологія останнього типу – метод модулярного множення Монтгомері [6]. Виконання модулярного множення $P = A \cdot B \bmod M$ за цим методом полягає в виконанні n ітерацій з аналізом розрядів множника B від молодшого до старшого. Початкове значення P дорівнює нулю. На кожній ітерації, за умови, що поточний біт B дорівнює одиниці, здійснюється додавання $P = P+A$, після чого, якщо P – непарне, до нього додається модуль: $P = P+M$; на кінець здійснюється зсув коду P ліворуч: $P = P>>1$. Після виконання останньої ітерації, якщо $P \geq M$, то від P віднімається модуль M: $P = P-M$. Результат $P = A \cdot B \cdot G \bmod M$, де G – мультиплікативна інверсія 2^n по модулю M: $G = 2^{-n} \bmod M$. Таким чином, в методі Монтгомері ділення заміняється на більш просту в реалізації операцію зсуву.

Для прискорення операції піднесення до квадрату A^2 запропоновані методи, що базуються на виключенні притаманного цій операції операційного дублювання [4]: це дозволяє для чисел великої розрядності практично вдвічі зменшити час виконання.

Широкого використання в сучасній криптографії для зменшення часу реалізації операцій множення $A{\cdot}B$ та піднесення до квадрату A^2 довгих чисел набули методи прискорення множення А. Карацуби [7] та М. Фюрера [8]. Показано [9], що для криптографічних застосувань використання схем прискореного множення дозволяє практично вдвічі зменшити об'єм обчислень для операції множення $A{\cdot}B$ і в 2.72 для піднесення до квадрату A^2.

Крім технології Монтгомері, для практичної реалізації модулярної редукції широко використовується технологія П. Барретта [11], яка полягає в заміні операції ділення двома операціями множення довгих чисел. Ця технологія ефективна за умови використання розпаралелювання мультиплікативних операцій модулярної арифметики, що виконуються над довгими числами [10].

Ефективним шляхом прискорення комп'ютерної реалізації мультиплікативних операцій модулярної арифметики для криптографічних застосувань є широке застосування передобчислень, що залежать від модуля. В реальних механізмах криптографічного захисту модуль M входить до складу відкритого ключа. Відповідно, він може вважатися практично незмінним. Це дозволяє виділити обчислення, що залежать від модуля, реалізувати їх один раз в формі передобчислень зі збереженням в пам'яті результатів, які використовуються для прискорення модулярної редукції.

З цих позицій становить практичний інтерес використання передобчислень для інших незмінних в рамках окремої операції модулярного експоненціювання компонентів, зокрема, для постійного множника A в рамках різновиду класичного алгоритму з проходом від старших до молодших розрядів коду експоненти.

Мета досліджень

Мета досліджень полягає в прискоренні базової операції криптографічних алгоритмів з відкритим ключем – модулярного експоненціювання шляхом зменшення часу реалізації її складової – модулярного множення на постійне число за рахунок використання передобчислень, що залежать від цього числа та модуля.

Метод прискореного модулярного множення на постійне число

Для досягнення поставленої мети пропонується метод прискореного модулярного множення $A{\cdot}B \bmod M$ на постійне число A. Метод орієнтовано на використання при реалізації класичного алгоритму модулярного експоненціювання зі старших розрядів коду експоненти. При цьому третина операцій модулярного експоненціювання припадає на модулярне множення на постійне число A.

В якості чинника прискорення модулярного множення в розроблено методі виступають передобчислення, що залежать від постійного числа A та модуля M, який в реальних криптографічних застосуваннях є частиною відкритого ключа і, відповідно, також може вважатися сталим. З теоретичної точки зору, ці передобчислення фактично реалізують модулярну редукцію зсунутих кодів постійного множимого A.

Модулярний добуток $P = A{\cdot}B \bmod M$ сталого n-розрядного числа – множимого A на множник $B = b_{n-1}{\cdot}2^n + b_{n-2}{\cdot}2^{n-1}+\ldots+ b_1{\cdot}2 + b_0$, $\forall i \in \{0,1,\ldots,n\text{-}1\}$: $b_i \in \{0,1\}$, може бути представлений у наступному вигляді:

$$P = \sum_{i=0}^{n-1} b_i \cdot 2^i \cdot A \bmod M = \\ = \left(\sum_{i=0}^{n-1} b_i \cdot (A \cdot 2^i \bmod M)\right) \bmod M. \quad (1)$$

В формулі (1) компоненти A, $A{\cdot}2 \bmod M$, …, $A{\cdot}2^{n-1} \bmod M$ залежать тільки від модуля M, яке в реальних криптографічних застосуваннях є частиною відкритого ключа і, відповідно, може вважатися постійним, а також від числа А, яке в рамках окремої операції модулярного експоненціювання також незмінне. Це надає змогу порахувати вказані значення перед виконанням обчислення модулярної експоненти зі збереженням результатів в

пам'яті у вигляді таблиці $Q[0]$, $Q[1]$,…, $Q[n-1]$. Для того, щоб спростити модулярну редукцію суми в формулі (1) пропонується зберігати в таблиці Q центровані значення $A \cdot 2^i \bmod M$, тобто значення, які знаходяться в діапазоні від $-M/2$ до $M/2$: $-M/2 \le Q[i] \le M/2$. За умови використання зазначених передобчислень обчислення модулярного добутку здійснюється у відповідності до наступної формули:

$$P = \left(\sum_{i=0}^{n-1} b_i \cdot Q[i]\right) \bmod M. \qquad (2)$$

Розроблений метод включає в себе дві процедури:

- процедуру формування таблиці передобчислень Q;
- процедуру модулярного множення на постійне число з використанням таблиць передобчислень.

Формування таблиці Q передобчислень здійснюється перед початком виконання операції модулярного експонентціювання. Процедура формування таблиці Q передобчислень для прискореного модулярного множення на постійне число A виконується в наступному порядку:

1. Якщо значення A більше половини модуля M, тобто за умови $A > M/2$, нульове табличне значення значення Q встановлюється рівним $A-M$: $Q[0] = A-M$; інакше $Q[0] = A$. Значення індексу i таблиці передобчислень встановлюється рівним одиниці : $i = 1$.

2. Табличне значення $Q[i]$, що індексується поточним значенням індексу i формується зсувом ліворуч попереднього значення таблиці $Q[i-1]$: $Q[i] = Q[i-1]<<1$. Якщо результат зсуву перевищує половину модуля M, тобто $Q[i] > M/2$, то виконується модулярна корекція: $Q[i]$ зменшується на значення модуля: $Q[i] = Q[i]-M$; інакше, якщо результат зсуву від'ємний і менший за $-M/2$, тобто $Q[i] < -M/2$, то також виконується модулярна корекція, яка полягає в тому, що до $Q[i]$ додається модуль M: $Q[i] = Q[i]+M$.

3. Здійснюється інкремент індексу i: $i = i+1$; якщо $i<n$, то виконується повернення на повторне виконання п.2.

Описана процедура формування таблиці передобчислень може бути ілюстрована прикладом її побудови для постійного числа $A = 1964$ за умови, що модуль $M = 4757$, тобто $n = 12$ та половина модуля $M/2 = 2378.5$. Згідно з п.1 описаної процедури оскільки $A < M/2 = 2378.5$ нульове табличне значення встановлюється рівним A: $Q[0] = A = 1964$. Поточний індекс i встановлюється рівним одиниці: $i = 1$. У відповідності з п.2 процедури здійснюється зсув ліворуч попереднього табличного значення: $Q[1] = Q[0]<<1 = 3934$. В силу того, що $Q[1] > M/2$, від нього віднімається модуль M: $Q[1] = Q[1]-M = 3934-4757 = -829$. В п.3 індекс i збільшується на одиницю: $i = 2$ та здійснюється на повторне виконання п.2. Табличне значення $Q[2]$ формується як результат зсуву ліворуч $Q[1]$ $Q[2] = Q[1]<<1 = -829<<1 = -1658$. Оскільки $Q[2]$ від'ємне, але більше за $-M/2 = -2378.5$, то корекція не виконується. В подальшому формування таблиці передобчислень здійснюється аналогічним чином. В табл. 1 наведені результати роботи процедури для всіх подальших значень індексу і до 11-ти включно.

Цілком очевидно, що запропонована процедура формування таблиці передобчислень, в середньому, потребує n операцій зсуву і $0.5 \cdot n$ операцій додавання (віднімання) n-розрядних чисел. При цьому об'єм таблиці передобчислень становить n^2 біт. Зокрема при значенні $n = 4096$, об'єм таблиці передобчислень становить $n^2 = 4096^2 = 2^{24}$ бітів, або 2 Мбайти.

Розроблена процедура обчислення модулярного добутку $P = A \cdot B \bmod M$ полягає в виконанні наступної послідовності дій:

1. Початкові значення поточної суми часткових добутків P та поточного індексу i розряду множника B встановлюються рівними нулю: $P = 0$ та $i = 0$.

2. Якщо поточний розряд b_i множника B дорівнює одиниці, тобто $b_i = 1$, то до поточного значення суми часткових добутків P додається i–те значення $Q[i]$ таблиці передобчислень: $P = P+Q[i]$.

3. Здійснюється інкремент індексу i: $i = i+1$; якщо $i<n$, виконується перехід на повторне виконання п.2 процедури.

4. Якщо поточний результат P від'ємний, тобто $P<0$, додати до нього модуль: $P = P+M$, після чого виконати п.4 повторно.

5. Якщо поточний результат P більший за модуль M або рівний з ним, тобто $P \geq M$, відняти від P значення модуля M: $P = P-M$, після чого перейти на повторне виконання п.5.

6. Кінець. Результат $P = A \cdot B \ mod \ M$.

Таблиця 1. Приклад формування таблиці Q для A = 1964, n = 12 і M = 4757

i	$Q[i]$	
	Після зсуву	Після корекції
0	1964	1964
1	3934	-829
2	-1658	-1658
3	-3316	1441
4	2882	-1875
5	-3750	1007
6	2014	2014
7	4028	-729
8	-1458	-1458
9	-2916	1841
10	3682	-1075
11	-2150	-2150

Робота запропонованої процедури модулярного множення з використанням таблиці передобчислень може бути ілюстрована наступним прикладом. Нехай виконується модулярне множення чисел A = 1964 та B = 2025 = 11111101001_2 по модулю M = 4757 для якого n = 12. Правильний результат $1964 \cdot 2024 \ mod \ 4757 = 248$.

Згідно з п.1 описаної вище процедури, стартові значення P та i встановлюються в нуль: $P = 0$, $i = 0$. Оскільки молодший розряд b_0 множника B дорівнює одиниці: $b_0 = 1$, то, у відповідності з п.2 до P додається табличне значення $T[0] = A$ = 1964. В силу того, що наступні два двійкових розряди множника B дорівнюють нулю: $b_1 = 0$ та $b_2 = 0$, при значеннях індексу $i = 1$ та $i = 2$, ніяких операцій над P не здійснюється. При $i = 3$ відповідний розряд b_3 множника B дорівнює одиниці: $b_3 = 1$; згідно п.2 процедури сума часткових добутків P збільшує на величину табличного значення $T[3] = 1441$: P = 1964+1441 = 3405. Динаміка зміни суми часткових добутків P в залежності від бітів множника b_i для всіх значень індексу i представлена в табл. 2.

Таблиця 2. Динаміка трансформацій змінних процедури при виконанні множення B = 2025 на стале число A = 1964 по модулю M = 4757.

i	b_i	P
0	1	1964
1	0	1964
2	0	1964
3	1	1964 + 1441 = 3405
4	0	3405
5	1	3405+1007 = 4412
6	1	4412 + 2014 = 6426
7	1	6426 – 729 = 5697
8	1	5697 – 1458 = 4239
9	1	4239 +1841 = 6080
10	1	6080 – 1075 = 5005
11	0	5005

Отриманий після виконання 12-ти циклів процедури результат P = 5005 більший за модуль M: $P = 5005 > M = 4757$, то у відповідності з п. 5 процедури від P віднімається модуль M: $P = P-M$ = 5005-4757 = 248.

Оцінка ефективності

В якості основного критерію ефективності запропонованого методу доцільно розглядати міру прискорення, в результаті його застосування, як окремої операції модулярного множення, так в цілому базової операції криптографії з відкритим ключем – модулярного експоненціювання.

В свою чергу, мірою прискорення модулярного множення може слугувати коефіцієнт γ прискорення виконання цієї операції, зумовлений застосуванням запропонованого методу. При цьому, чисельне значення коефіцієнту γ визначається як співвідношення числа N_0 операцій додавання чи зсуву, що здійснюються над n-розрядними числами в базовому варіанті реалізації модулярного множення методом Монтгомері [6] до числа N аналогічних

операцій в запропонованому методі. Подібним чином оцінка ефективності запропонованого методу в плані зменшення часу обчислювальної реалізації модулярного експоненціювання може бути здійснена через коефіцієнт прискорення β, який визначається співвідношенням середньої кількості F_0 операцій додавання чи зсуву *n*–розрядних чисел для виконання *n* циклів модулярного експоненціювання при реалізації множення на постійне число *A* за відомим методом Монтгомері до середньої кількості *F* таких операцій при застосуванні запропонованого методу.

В методі модулярного множення Монтгомері [6] організується виконання *n* циклів, в кожному з яких, зі ймовірністю 0.5 (в залежності від значення поточного розряду множника) здійснюється додавання множимого до суми часткових добутків, з такою ж ймовірністю 0.5 (в залежності від значення молодшого розряду суми) до неї додається модуль і завжди реалізується її логічний зсув праворуч. Таким чином, в кожному із *n* циклів, в середньому виконується 2 операції (додавання або зсув) над *n*-розрядними числами. Відповідно, загальна кількість операцій N_0, якими реалізується модулярне множення *n*-розрядних чисел становить $N_0 = 2 \cdot n$.

В запропонованому методі модулярне множення також організоване у вигляді *n* циклів, в кожному з яких, зі ймовірністю 0.5 (в залежності від значення поточного розряду множника) здійснюється додавання табличного значення до суми часткових добутків. Тобто, середня кількість *N* операцій арифметичного додавання чи зсуву над *n*–розрядними числами при реалізації модулярного множення визначається як $N = 0.5 \cdot n$.

Відповідно, застосування запропонованого методу прискореного модулярного множення на постійне число з використанням передобчислень дозволяє скоротити час в порівнянні з модулярним множенням Монтгомері в γ раз, чисельне значення γ визначається формулою:

$$\gamma = \frac{N_0}{N} = \frac{2 \cdot n}{0.5 \cdot n} = 4. \qquad (3)$$

Таким чином, запропонований спосіб використання передобчислень, що залежать від постійного множника *A* та модуля *M* дозволяє прискорити операцію модулярного множення в чотири рази. Проведені експериментальні дослідження повністю підтвердили цю отриману теоретичним шляхом оцінку.

Середня кількість F_0 операцій типу додавання чи зсуву *n*–розрядних чисел при обчисленні модулярної $A^E \bmod M$ за класичним алгоритмом зі скануванням коду експоненти, починаючи з її старших розрядів дорівнює сумі таких операцій для реалізації *n* піднесень до квадрату за модулем *M* та $0.5 \cdot n$ модулярних множень Монтгомері. При здійсненні модулярного піднесення до квадрату за скороченою схемою [9] середня кількість операцій додавання чи зсувів приблизно вдвоє менша в порівнянні з аналогічним показником для модулярного множення множення і становить *n*. Тобто для реалізації модулярного піднесення до квадрату в *n* циклах модулярного експоненціювання потрібно виконати n^2 операцій типу додавання чи зсуву *n*–розрядних чисел. Аналогічний показник для модулярного множення, яке виконується в половині з *n* циклів обчислення $A^E \bmod M$, становить $0.5 \cdot n \cdot N = n^2$. Таким чином, сумарна кількість операцій арифметичного додавання та зсуву для обчислення модулярної експоненти базовому варіанті становить $F_0 = 2 \cdot n^2$.

В запропонованому методі кількість *N* операцій арифметичного додавання чи зсуву над *n*–розрядними числами визначається сумою кількості таких операцій, що здійснюються на етапі формування таблиці передобчислень та при виконанні *n* циклів модулярного експоненціювання.

Як зазначалось вище, процедура формування таблиці передобчислень, в середньому, потребує *n* операцій зсуву і $0.5 \cdot n$ операцій додавання (віднімання) *n*-розрядних чисел, що в сумі становить $1.5 \cdot n$ операцій.

В рамках n циклів модулярного експоненціювання здійснюється, як було показано вище, n^2 операцій типу додавання чи зсуву n-розрядних чисел. Для реалізації модулярного добутку на постійне число, яке виконується в половині з n циклів обчислення $A^E \bmod M$, при використанні запропонованого методу потрібно, в середньому, $0.5 \cdot n \cdot N = 0.25 \cdot n^2$. $n^2 + 0.25 \cdot n^2 = 1.25 \cdot n^2$. Ще h операцій додавання (віднімання)
n–розрядних чисел виконується в рамках п.4 і п.5 запропонованої процедури для остаточної модулярної редукції. Оцінка чисельних значень h може бути здійснена наступним чином. При реалізації формули (2) фактично виконується підрахунок суми $n/2$ чисел, рівномірно розподілених в інтервалі від $-M/2$ до $M/2$. Середнє значення кожного такого числа дорівнює нулю, а дисперсія, при великих значеннях модуля M становить $M^2/12$. У відповідності до центральної граничної теореми теорії ймовірності, середнє значення суми $n/2$ таких чисел дорівнює нулю, а дисперсія становить – $n \cdot M^2/24$. Середньоквадратичне відхилення σ суми відповідно, визначається формулою:

$$\sigma = M \cdot \sqrt{\frac{n}{24}}. \qquad (4)$$

Кількість h операцій додавання (віднімання) модуля M для остаточно модулярної редукції суми в формулі (2) обчислюється у вигляді:

$$h = \frac{\sigma}{M} = \frac{M \cdot \sqrt{n}}{M \cdot \sqrt{24}} = \frac{\sqrt{n}}{\sqrt{24}} = 0.2 \cdot \sqrt{n}. \qquad (5)$$

Таким чином, середня кількість F операцій додавання (віднімання) n-розрядних чисел, що потрібна для реалізації модулярного експоненціювання з використанням запропонованого методу визначається виразом:

$$F = 1.5 \cdot n + 1.25 \cdot n^2 + 0.2 \cdot \sqrt{n}. \qquad (6)$$

Аналіз компонентів суми (6) показує, що формування таблиці передобчислень потребує на три порядки менше обчислень в порівнянні з виконанням циклів модулярного експоненціювання. В свою чергу, реалізація остаточної редукції суми (2) потребує на 6 порядків менше обчислень в порівнянні з виконанням циклів модулярного експоненціювання. Наприклад, при типовому в сучасних умовах значенні $n = 4096$ формування таблиць передобчислень потребує 5144 операцій типу n^2 операцій типу додавання чи зсуву n-розрядних чисел, виконання n циклів модулярного експоненціювання потребує 21000000 таких операцій, а остаточна редукція – всього 13 операцій. Виходячи з цього, на оціночних розрахунків можна вважати, що $F \approx 1.25 \cdot n$.

З урахуванням наведеного значення коефієнту β прискореннння виконання базової операції криптографії з відкритим ключем за рахунок використання запропонованого методу визначається формулою:

$$\beta = \frac{F_0}{F} = \frac{2 \cdot n^2}{1.25 \cdot n^2} = 1.6. \qquad (7)$$

Проведені експериментальні дослідження, в цілому, підтвердили обчислену теоретичним шляхом оцінку прискорення комп'ютерної реалізації криптографічних алгоритмів з відкритим ключем в 1.6 раз за рахунок використання запропонованого методу швидкого модулярного множення на постійне число.

Висновки

В результаті проведених досліджень, направлених на прискорення на комп'ютерної реалізації криптографічних алгоритмів з відкритим ключем на термінальних мікроконтролерах *IoT*, теоретично обґрунтовано та розроблено метод швидкого модулярного множення на постійне число з використанням передобчислень. Ця операція складає третину об'єму обчислень при реалізації модулярного експоненціювання над числами, довжина яких значно перевищує розрядність процесора – базової операції криптографії з відкритим ключем.

Відмінність запропонованого методу полягає в організації передобчислень, які залежать від постійних множника та модуля. Ці передобчислення здійснюються перед початком модулярного експоненціювання і дозволяють, за рахунок

використання їх результатів при кожному модулярному множенні зменшити об'єм обчислень для його реалізації.

Теоретично показано, що використання запропонованого методу дозволяє зменшити час виконання модулярного множення на постійне число в чотири рази в порівнянні з технологією Монтгомері. Теоретично доведено і експериментально підтвердьжено, що застосування розробленого методу забезпечу. прискорення реалізації базової операції криптографії з відкритим ключом – модулярного експоненціювання в 1.6 раз в порівнянні з використанням модулярного множення Монтгомері.

Розроблений метод орієнтовано для використання при реалізації протоколів інформаційної безпеки на термінальних малопотужних обчислювальних платформах систем віддаленого комп'ютерного моніторингу стану та управління об'єктами реального світу з використанням технологій *IoT*.

Література

1. Kaloulli E., Zacharioudakis E. Survey of Cryptoprocessors Advances and Technological Trends. *Lecture Notes in Networks and Systems. Vol. 1058. Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24)* / ed. by K. Daimi, A. Al Sadoon. Cham, 2024. P. 411–430. DOI: 10.1007/978-3-031-65522-7-37.

2. Daiko I., Selivanov V. Fast exponential method on Galois fields for cryptographic applications. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* : proceedings, Athens, Greece, 13–15 October 2023 / IEEE. 2023. P. 1–4. DOI: 10.1109/DESSERT61349.2023.10416519.

3. Menezes A., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. Boca Raton : CRC Press, 2001. 780 p.

4. Markovskyi O. et al. An Accelerate Approach for Public Key Cryptography Implementation on IoT Terminal Platforms. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* : proceedings, Athens, Greece, 13–15 October 2023 / IEEE. 2023. P. 1–4. DOI: 10.1109/DESSERT61349.2023.10416516.

5. Buhrow B., Gilbert B., Haider C. Parallel modular multiplication using 512-bit advanced vector instructions: RSA fault-injection countermeasure via interleaved parallel multiplication. *Journal of Cryptographic Engineering*. 2021. No. 2. P. 46–55. DOI: 10.1007/s13389-021-00256-9.

6. Montgomery P. Modular multiplication without trial division. *Mathematics of Computation*. 1985. Vol. 44, no. 170. P. 519–521.

7. Карацуба А. О., Офман Ю. П. Множення багатоцифрових чисел на автоматах. *Доповіді Академії наук СРСР*. 1962. № 2. С. 293–294.

8. Fürrer M. Faste Integer Multiplication. *SIAM Journal on Computing*. 2009. Vol. 39, no. 3.. P. 979–1005. DOI: 10.1137/070711716.

9. Марковский О. П., Аль-Мріят Гассан Абдель Жаліль. Метод прискореного модулярного множення для ефективної реалізації механізмів криптографічного захисту з відкритим ключом. *Адаптивні системи автоматичного управління*. 2024. Т. 1, № 44. С. 142–152. DOI: 10.20535/1560-8956.44.2024,302429.

10. Giorgi P., Imbert L., Izard T. Parallel modular multiplication on multi-core processors. *2013 IEEE 21st Symposium on Computer Arithmetic* : proceedings, Austin, TX, USA, 07–10 April 2013 / IEEE. 2013. P. 135–142.

11. Barrett P. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. *Lecture Notes in Computer Science. Vol. 263. Advances in Cryptology - CRYPTO '86. Proceedings* / ed. by A. M. Odlyzko. Berlin, 1987. P. 311–323.

Селіванов В.Л., Аль-Мріят Гассан Абдель Жаліль

МЕТОД МОДУЛЯРНОГО МНОЖЕННЯ НА ПОСТІЙНЕ ЧИСЛО ДЛЯ ШВИДКОЇ РЕАЛІЗАЦІЇ КРИПТОГРАФІЇ З ВІДКРИТИМ КЛЮЧЕМ В IoT

В статті запропоновано метод прискорення важливої для криптографічних застосувань операції модулярного множення на постійне число за рахунок використання передобчислень. Детально розроблено технологію формування таблиці передобчислень, що залежать від постійного множника і модуля. Наведено формалізований опис запропонованої процедури прискореного модулярного множення з застосуванням передобчислень. Виклад проілюстровано числовим прикладом. Теоретично доведено та експериментально підтверджено, що за рахунок використання передобчислень при виконанні модулярного множення на постійне число за запропонованим методом, досягається прискорення реалізації цієї операції вчетверо. При цьому час виконання базової операції криптографії з відкритим ключем – модулярного експоненціювання скорочується в 1.6 рази.

***Ключові слова**: модулярне множення; модулярна редукція; модулярне експоненціювання; криптографія з відкритии ключем; передобчислення.*

Selivanov V.L., Al-Mrayat Ghassan Abdel Jalil Halil

METHOD OF MODULAR MULTIPLICATION BY INVARIABLE NUMBER FOR OPEN KEY CRYPTOGRAPHY QUICK IMPLEMENTATION IN IoT

The article proposes a method of accelerating the operation of modular multiplication important for cryptographic applications due to use of precomputations. The technology for forming a table of precomputations, whose depend on a invariable multiplier and modulus, has been developed in detail. A formalized description of the proposed procedure for accelerated modular multiplication using precomputations is given. The statement is illustrated by a numerical example. It has been theoretically proven and experimentally confirmed that by using preccomputations according to the proposed method, the implementation of this operation is accelerated by four times. At the same time, the execution time of the basic operation of public-key cryptography – modular exponentiation – is reduced by 1.6 times.

***Key words**: modular multiplication; modular reductions; modular exponentiation; open key cryptography; precomputations.*