УДК 004.052.42 **DOI: 10.18372/2073-4751.83.20549**

Русанова О.В., к.т.н.,
orcid.org/0000-0003-0145-3012,

Марковський О.П., к.т.н.
orcid.org/0000-0003-3483-4233,

Гайдукевич О.А.,
orcid.org/0009-0008-2320-9858,

МЕТОД ПРИСКОРЕНОГО МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ НА ОСНОВІ ДИНАМІЧНИХ ТАБЛИЦЬ ПЕРЕДОБЧИСЛЕНЬ

Національний технічний університет України
“Київський політехнічний інститут ім. Ігоря Сікорського”

e-mail: olga.rusanova@gmail.com
e-mail: nyancatandme0@gmail.com
e-mail: hdksasha@gmail.com

Вступ

Динамічний прогрес технологій обміну даними, а також стрімкий розвиток в сфері мікроелектроніки обумовлюють інтенсивне розширення галузей застосування систем на базі

анню характеристик Інтернету, його низькій вартості, простоті інтеграції,

Т-технології вийшли за межі побутових застосувань і активно впроваджуються у критично важливі галузі. Мова йде про такі сфери використання, як дистанційна медицина, системи охоронної сигналізації та відеоспостереження, управління безпілотними пристроями, об’єктами інфраструктури, технологічними лініями.

Для таких систем використання мережі Інтернет як середовища передачі даних породжує низку загроз, пов’язаних із потенційною можливістю зовнішнього втручання в процеси віддаленого

Базовою математичною операцією, що лежить в основі таких алгоритмів, є операція модулярного експоненціювання A^E mod M. Для забезпечення належного рівня криптостійкості вона виконується

сорів, які використовуються у термінальних пристроях. Здійснення експоненціювання над такими числами потребує виконання мільярдів процесорних операцій, що суттєво ускладнює обчислення модулярної Інтернету Речей. В контексті таких систем йдеться про технології, що застосовують мережу Інтернет для передачі даних, а також команд управління. Завдяки можливості використання готових інфраструктурних рішень, якісному зрост а також практичній незалежності від відстані до об’єктів керування, Іо управління об’єктами та моніторингу їх стану [1]. Особливу небезпеку становлять спроби підміни або модифікації керуючих команд, які формуються пристроєм управління, а також фальсифікації даних, що надходять з термінальних платформ.

Для протидії таким загрозам ключового значення набувають криптографічні методи захисту інформації. Зокрема, для перешкоджання фальсифікації даних стану об’єктів реального світу та команд управління найбільш дієвим механізмом виступають алгоритми цифрового підпису (DSA) [2].

над числами великої розрядності. На сьогоднішній день стандартом є використання ключів довжиною 4096 бітів [3], із перспективою її зростання до 8192, що на порядки перевищує розрядність проце експоненти в системах управління в режимі реального часу. Для комп’ютерних платформ великої та середньої потужності, проблема швидкої реалізації модулярного експоненціювання вирішується за рахунок застосування вбудованих крипто-

процесорів, що здатні швидко виконувати обчислення експоненти на апаратному рівні [4]. Водночас для малопотужних термінальних платформ, що використовуються у IoT-системах, застосування криптопроцесорів вимагає додаткових ресурсів, а також потребує забезпечення особливих умов для їх функціонування.

Таким чином, наукова задача прискорення реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання на термінальних пристроях є актуальною та важливою для сучасних систем віддаленого керування об'єктами реального світу.

Оглядовий аналіз існуючих методів прискорення мультиплікативних операцій для швидкого модулярного експоненціювання

Важливість проблеми швидкого обчислення модулярної експоненти на термінальних пристроях стимулює велику кількість досліджень на цю тему [5,6].

На практиці, обчислення $A^E \bmod M$ здійснюється за одним із двох різновидів класичного алгоритму модулярного експоненціювання [7]. Для обох з них обчислення експоненти організовується у вигляді циклу з n ітерацій, де n – розрядність модуля M. Перший різновид передбачає обробку коду експоненти зі старших розрядів. Результат експоненціювання формується у змінній U, початкове значення якої ініціалізуються рівним одиниці: $U = 1$. Кожна ітерація передбачає здійснення модулярного піднесення до квадрату $U = U^2 \bmod M$ та, якщо відповідний біт експоненти дорівнює одиниці, модулярного множення $U = U \cdot A \bmod M$.

В другому різновиді обробка коду експоненти здійснюється з молодших розрядів, і обчислення $A^E \bmod M$ організовується з використанням двох змінних D і R, початкове значення яких дорівнює числу A і одиниці відповідно: $D = A$, $R = 1$. На кожній ітерації передбачається виконання двох операцій: модулярного множення $R = R \cdot D \bmod M$, за умови, що поточний біт експоненти E дорівнює одиниці, та модулярного піднесення до квадрату $D = D^2 \bmod M$. Кінцевий результат експоненціювання формується у змінній R.

Для обох різновидів класичного алгоритму експоненціювання загальна кількість мультиплікативних операцій модулярної арифметики, що виконуються над n-розрядними (довгими) числами, визначається n модулярними піднесеннями до квадрату та, в середньому, $0{,}5 \cdot n$ модулярними множеннями. Якщо для обох типів згаданих операцій використовується однаковий механізм модулярного множення, то сумарна середня їх кількість становить приблизно $1{,}5 \cdot n$.

Структура обох різновидів класичного алгоритму експоненціювання має послідовний характер, що принципово обмежує можливість їх розпаралелення. Повною мірою це стосується різновиду алгоритму зі старших розрядів, в якому кожна операція лежить на критичному шляху. Для різновиду з обробкою експоненти з молодших розрядів можлива часткова організація двох паралельних процесів, зокрема, гілка обчислення піднесення до квадрату $D^2 \bmod M$ є незалежною, тоді як обчислення множення $R \cdot D \bmod M$ залежить від поточного значення D [8].

Виходячи з цього, основні зусилля дослідників спрямовані на прискорення виконання модулярних операцій над довгими числами: модулярного множення та піднесення до квадрату.

Структурно, операція модулярного множення $A \cdot B \bmod M$ включає дві фази: власне множення $A \cdot B$ та редукцію, тобто знаходження залишку від ділення отриманого добутку $A \cdot B$ на модуль M.

Існують два основних підходи до їх реалізації. Перший полягає у послідовному виконанні множення з подальшою редукцією, другий – у здійсненні обох фаз одночасно, тобто редукція суміщається з множенням [9].

При реалізації модулярного множення в рамках першого підходу, в переважній більшості застосувань, фаза обчислення добутку $A \cdot B$ виконується з

використанням методу посекційного множення. Він передбачає розбиття обох n-розрядних множників на s секцій довжиною r, де r – розрядність процесора. Добуток $A \cdot B$ реалізується шляхом поелементного множення кожної секції числа A на кожну секцію числа B та подальшим додаванням одержаних часткових результатів. Такий метод вимагає здійснення s^2 процесорних множень та $2s \cdot (s + 1) + 1$ додавань r-розрядних чисел. При виконанні піднесення до квадрату довгих чисел за таким самим методом, кількість операцій множення зменшується майже вдвічі за рахунок виключення дублюючих добутків однакових секцій і становить $0,5 \cdot (s^2 - s) + s$. Водночас кількість додавань залишається незмінною та складає $2s \cdot (s + 1) + 1$ [10].

Для підвищення швидкодії посекційного множення довгих чисел запропоновано метод [11], що базується на схемах прискореного множення. Його застосування дозволяє реалізувати добуток двох довгих чисел за $0,5 \cdot s^2 + 1,5 \cdot s$ процесорних множень, завдяки чому обчислення прискорюється майже в два рази.

Основна перевага методів прискореного обчислення добутку, що базуються на посекційному множенні, полягає в ефективному використанні апаратних засобів процесора.

В рамках першого підходу, добуток $A \cdot B$ обчислюється в явному вигляді із використанням описаних вище методів прискореного множення. Для подальшого виконання модулярної редукції, здебільшого, застосовується метод Барретта [12], який дозволяє замінити ділення на операції множення та зсуву. Основна ідея методу полягає в обчисленні $A \cdot B \bmod M$ шляхом віднімання $A \cdot B - f \cdot M$. Значення f обчислюється як результат добутку $\lfloor \xi \cdot \lfloor A \cdot B \rfloor \cdot 2^{-2n} \rfloor$, де ξ - константа, яка залежить тільки від модуля M і обчислюється одноразово у вигляді $\xi = \lfloor 2^{2 \cdot n} \cdot M^{-1} \rfloor$. Таким чином, метод Барретта реалізує модулярну редукцію шляхом виконання двох операцій множення довгих чисел.

В якості недоліку першого підходу до реалізації модулярного множення можна виділити те, що розділення фаз множення та редукції значно уповільнює обчислення добутку $A \cdot B \bmod M$. Окрім цього, формування кінцевого результату довжиною $2n$ вимагає додаткових витрат на роботу з числами подвоєної розрядності.

При реалізації модулярного множення за другим підходом, тобто із суміщенням операцій редукції та множення, найбільш ефективним вважається метод Монтґомері [13]. Згідно з ним, множення реалізується у вигляді n ітерацій, на кожній з яких здійснюється обробка відповідного біту множника, починаючи з молодших розрядів. Якщо поточний біт множника дорівнює одиниці, виконується додавання множеного, і, в залежності від парності часткового добутку, здійснюється його корекція додаванням непарного модуля. Виконання ітерації звершується зсувом праворуч часткового добутку. Результат модулярного множення Монтґомері формується у вигляді добутку $A \cdot B \cdot 2^n \bmod M$, тому для отримання кінцевого значення $A \cdot B \bmod M$ необхідно здійснити корекцію, яка полягає у модулярному множенні одержаного числа на 2^n. На практиці, при обчисленні модулярної експоненти із використанням методу Монтґомері, описана корекція виконується одноразово – після завершення усіх ітерацій експоненціювання.

Таким чином, загальна кількість операцій, потрібних для реалізації модулярного множення за методом Монтґомері, в середньому становить приблизно $(0,5+0,5) \cdot n$ додавань та $1 \cdot n$ зсувів довгих чисел. З позиції аналізу часових характеристик, час виконання сучасними мікропроцесорами команди додавання практично ідентичний часу здійснення команди логічного зсуву. Тоді, загальний час обчислення модулярного добутку за методом Монтґомері визначається часом виконання $2 \cdot n$ додавань довгих чисел [14].

Для прискорення реалізації модулярного множення Монтґомері запропоновано метод групового множення [15]. Він передбачає одночасну обробку групи з k розрядів множника при виконанні множення із суміщеним здійсненням редукції одразу на k розрядів. Для цього виконується побудова двох таблиць передобчислень. Перша формується на основі множника A і використовується для прискорення операції множення. Друга таблиця будується на основі модуля M і застосовується для виконання корекції часткового добутку та здійснення редукції. Таким чином, обчислення $A \cdot B \bmod M$ зводиться до двох додавань значень з таблиць передобчислень та зсуву отриманого часткового добутку на k розрядів. Це дозволяє виконати модулярне множення за $\frac{3 \cdot n}{k}$ адитивних операцій над довгими числами, де k – кількість розрядів, що обробляються одночасно. Кінцевий результат, як і в класичному множенні Монтґомері, потребує корекції, яка полягає у модулярному множенні одержаного значення на 2^n.

В контексті обчислення модулярної експоненти, зазначений метод використовується лише в різновиді алгоритму експоненціювання зі старших розрядів, в якому модулярне множення на кожній ітерації здійснюється над постійним числом. При цьому, для прискорення операції модулярного піднесення до квадрату цей метод не може бути застосований, так як відповідний операнд змінюється на кожній ітерації експоненціювання. Загальна кількість операцій при обчисленні модулярної експоненти із застосуванням методу групового множення становить $n^2 \cdot (2 + \frac{1{,}5}{k})$. Таким чином, використання зазначеного методу дозволяє прискорити операцію експоненціювання приблизно в 1,5 рази в порівнянні з класичним методом Монтґомері. З огляду на сучасні вимоги до швидкості здійснення криптографії з відкритим ключем, підвищення швидкодії, яке досягається із використанням відомого методу, вбачається недостатнім для забезпечення реалізації модулярного експоненціювання в режимі реального часу.

Отже, проведений огляд показав, що існуючі методи швидкого обчислення модулярного добутку не дозволяють суттєво прискорити операцію модулярного експоненціювання. Це визначає необхідність пошуку нових шляхів для підвищення швидкодії обчислення модулярної експоненти.

Мета досліджень

Мета досліджень полягає у прискоренні комп'ютерної реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання за рахунок використання передобчислень, які здійснюються на кожній ітерації, що дозволяє виконувати модулярні операції множення та піднесення до квадрату з груповою обробкою розрядів на обох фазах: власне множення та редукції Монтґомері, завдяки чому зменшується час обчислення модулярної експоненти.

Метод прискореного медулярного експоненціювання

Для досягнення поставленої мети запропоновано метод прискореного модулярного експоненціювання на основі динамічних таблиць передобчислень для швидкої реалізації мультиплікативних операцій.

Основна ідея запропонованого методу прискорення модулярного експоненціювання полягає у зменшенні часу виконання кожної з мультиплікативних складових цієї операції шляхом використання таблиць передобчислень, які формуються, на відміну від відомих методів, на кожній ітерації експоненціювання. Мультиплікативні складові являють собою операцію модулярного множення, що здійснюється шляхом виконання двох операцій: власне множення та редукції за методом Монтґомері.

Побудова таблиць передобчислень забезпечує можливість групової обробки розрядів компонентів операцій множення

та редукції, що істотно знижує загальний об'єм обчислень. Запропонований метод базується на використанні різновиду алгоритму модулярного експоненціювання з молодших розрядів. Кожна з n ітерацій алгоритму передбачає виконання двох операцій модулярного множення, кожна з яких використовує однаковий множник, який є фіксованим на відповідній ітерації.

Ключовою особливістю розробленого методу є застосування таблиць передобчислень для однакового множника, що дозволяє виконати обробку k розрядів множника одночасно. Множник розбивається на k-розрядні фрагменти, кожен з яких слугує адресою для вибору відповідного елемента з таблиці. Таким чином, обчислення модулярного добутку зводиться до послідовного додавання значень із таблиці передобчислень відповідно до k-розрядних фрагментів двійкового коду множника, з наступною груповою редукцією Монтґомері на k розрядах. Завдяки такій організації обчислювального процесу досягається суттєве скорочення кількості необхідних арифметичних операцій, що дозволяє підвищити швидкодію всієї процедури модулярного експоненціювання.

Викладена ідея реалізована у вигляді детально розроблених процедур, які власне і складають метод. До таких процедур належать: побудова таблиці передобчислень W_Q для прискореного модулярного множення, формування таблиці C значень корекції для групової редукції Монтґомері, виконання модулярного множення з використанням зазначених таблиць, і безпосереднє обчислення модулярної експоненти.

Запропонований метод включає процедуру побудови таблиці W_Q передобчислень для заданого значення множеного Q. Розроблена процедура передбачає виконання наступної послідовності дій:

1. Початковому елементу $W_Q[0]$ таблиці присвоюється значення нуля: $W_Q[0] = 0$. Індексу p рядків присвоюється значення одиниці: $p = 1$.
2. Визначається значення наступного елементу таблиці шляхом додавання множеного Q до попереднього (p-1)-го елемента таблиці: $W_Q[p]=W_Q[p\text{-}1] + Q$.
3. Виконується інкремент індексу p рядків: $p = p + 1$.
4. Якщо $p < 2^k$, здійснюється повернення до пункту 2.

Робота запропонованої процедури може бути проілюстрована прикладом побудови таблиці W_Q для значення Q = 1974 при довжині фрагменту k = 3.

Згідно п.1 процедури значення $W_Q[0] = 0$ та $p = 1$. У відповідності з п.2 значення $W_Q[1]$ визначається як сума попереднього значення $W_Q[0] = 0$ та $Q = 1974$: $W_Q[1] = W_Q[0] + 1974 = 1974$. В рамках п.3 здійснюється інкремент індексу p рядків: $p = 1 + 1 = 2$. В силу того, що $p = 2 < 2^k = 8$ здійснюється повернення на повторне виконання п.2. В подальшому виконання процедури здійснюється по аналогії з описаним. Побудована в результаті виконання таблиця W_Q для Q = 1974 наведена в табл.1.

Таблиця 1. Таблиця W_Q передобчислень для $Q = 1974$

p	W_Q
0	0
1	1974
2	3948
3	5922
4	7896
5	9870
6	11844
7	13818

Запропонований метод передбачає реалізацію модулярного множення з використанням групової редукції Монтґомері. Цей підхід полягає у виконанні модулярної редукції часткового добутку відразу на k розрядів. Щоб не втратити значущі розряди часткового добутку під час зсуву на k розрядів, передбачається виконання корекції, яка полягає у додаванні до нього числа кратного модулю. Унаслідок такої корекції молодші k бітів часткового добут-

ку приймають значення нуля. Для швидкого виконання корекції доцільним видається використовувати таблицю C передобчислень, що дозволяє по значеннях молодших k розрядів часткового добутку одразу визначити код корекції.

Процедура побудови таблиці C значень корекції зводиться до виконання наступної послідовності дій:

- Значення елементу $C[0]$ таблиці C встановлюється рівним нулю: $C[0] = 0$. Змінній H присвоюється значення одиниці: $H = 1$.
- Значення індексу i номеру розряду встановлюється в одиницю: $i = 1$. Значення коригуючого коефіцієнту l встановлюється рівним нулю $l = 0$. Змінній $Y = y_k \cdot 2^{k-1} + \ldots + y_2 \cdot 2^1 + y_1$, $\forall\, x \in \{1,2,\ldots k\}$: $y_x \in \{0,1\}$ присвоюється значення H: $Y = H$.
- Якщо значення розряду y_i дорівнює одиниці: $y_i = 1$, то до коригуючого коефіцієнту l додається 2^{i-1} : $l = l + 2^{i-1}$ та значення Y обчислюється як: $Y = Y + M \cdot 2^{i-1} \bmod 2^k$.
- Здійснюється інкремент індексу i: $i = i + 1$. Якщо $i < k$, виконується перехід на повторне виконання п.3.
- Значення елементу $C[H]$ таблиці C обчислюється як добуток коригуючого коефіцієнту l та модуля M: $C[H] = l \cdot M$.
- Виконується інкремент H: $H = H + 1$. Якщо $H < 2^k$, здійснюється перехід на п.2.

Робота описаної процедури може бути ілюстрована прикладом побудови таблиці C для модуля $M = 3763$ при довжині фрагменту $k = 3$.

Відповідно до п.1 процедури, значення H встановлюється рівним одиниці: $H = 1$. За п.2 індекс номеру розряду $i = 1$, коригуючий коефіцієнт $l = 0$ та змінна $Y = H = 1$. В силу того, що $y_i = 1$, за п.3 коригуючий коефіцієнт $l = 0+2^0 = 1$ та значення $Y = 1 + 3763 \cdot 2^0 \bmod 2^3 = 4$. Згідно з п.4 здійснюється інкремент $i = 1+1 = 2$. З огляду на те, що $i = 2 < k = 3$, відбувається повернення на п.3. Оскільки $y_i = 0$, здійснюється перехід до п.4, в рамках якого індекс $i = 2 + 1 = 3$. Внаслідок того, що $i = k$, виконується п.5. Згідно п.5 елемент $C[0] = 0 \cdot 3763 = 0$. Відповідно до п.6, $H = 0 + 1 = 1$. В силу того, що $H = 1 < 2^k = 8$, реалізація процедури повертається до п.2. Наступні дії виконуються по аналогії з вищеописаним. Результатом виконання процедури побудови таблиці C корекції при модулі $M = 3763$ є наведена нижче табл.2.

Таблиця 2. Приклад заповнення таблиці C значень корекції для групової редукції при M = 3763 та довжині фрагменту k = 3

Значення H	Значення корекції
000	0
001	$5 \cdot M = 18\,815$
010	$2 \cdot M = 7526$
011	$7 \cdot M = 26\,341$
100	$4 \cdot M = 15\,052$
101	$M = 3763$
110	$6 \cdot M = 22\,578$
111	$3 \cdot M = 11\,289$

В силу того, що побудова таблиці C залежить виключно від значення модуля, який є частиною відкритого ключа, її формування здійснюється одноразово з подальшим збереженням в постійній пам'яті.

З використанням побудованих таблиць W_Q та C реалізується модулярне множення $U = B \cdot Q \bmod M$, де $B = b_n \cdot 2^{n-1} + \ldots + b_3 \cdot 2^2 + b_2 \cdot 2 + b_1$, $\forall\, z \in \{1,2,\ldots n\}$: $b_z \in \{0,1\}$. Обчислення модулярного добутку U полягає у виконанні наступної послідовності дій:

- Частковому добутку $U = u_n \cdot 2^{n-1} + \ldots + u_3 \cdot 2^2 + u_2 \cdot 2 + u_1$, $\forall\, z \in \{1,2,\ldots n\}$: $u_z \in \{0,1\}$ та індексу $g \in \{0;\ n/k\text{-}1\}$ присвоюється значення нуля: $U = 0$ та $g = 0$.
- Змінній B_g присвоюється значення k-розрядного коду g-ого фрагмента множника $b_{g\cdot k+k} \cdot 2^{k-1} + \ldots + b_{g\cdot k+2} \cdot 2^1 + b_{g\cdot k+1}$: $B_g = b_{g\cdot k+k} \cdot 2^{k-1} + \ldots + b_{g\cdot k+2} \cdot 2^1 + b_{g\cdot k+1}$.

- Здійснюється додавання до часткового добутку U значення з таблиці W_Q, яке адресується k-розрядним кодом g-ого фрагмента множника B_g: $U = U + W_Q[B_g]$. Значення U' складає k молодших розрядів коду U: $U' = u_k \cdot 2^{k-1} + \ldots + u_1$.
- Виконується корекція проміжного результату шляхом додавання значення корекції з таблиці C, яке адресується k молодшими розрядами коду U: $U = U + C[U']$.
- Реалізується зсув праворуч часткового добутку U на k розрядів: $U = U >> k$.
- Здійснюється інкремент індексу g: $g = g + 1$. Якщо $g < n/k$, реалізується перехід для повторного виконання до пункту 2.

Подальші операції виконуються з одержаним значенням U. Результат модулярного множення, як і результат звичайного множення Монтґомері, потребує корекції, яка здійснюється шляхом добутку $U \cdot 2^n \bmod M$.

Роботу процедури обчислення модулярного добутку із використанням таблиці W_Q передобчислень та таблиці C значень корекції можна проілюструвати прикладом обчислення $U = B \cdot Q \bmod M = = 2025 \cdot 1974 \bmod 3763 = 1044$. В рамках прикладу обчислюється модулярний добуток з наступними значеннями параметрів: $B = = 2025_{10} = 0111\ 1110\ 1001_2$;
$Q = 1974_{10} = 0111\ 1011\ 0110_2$; $M = 3763_{10} = = 1110\ 1011\ 0011_2$.

Кількість n двійкових розрядів модуля M дорівнює 12. В рамках прикладу обирається двійкова розрядність фрагментів для одночасного множення $k = 3$. Для обраного значення $Q = 1974$ таблиця W_Q передобчислень наведена у табл.1. Для модуля $M = 3763$ таблиця C значень корекції наведена у табл.2. У відповідності до п.1 процедури обчислення модулярного добутку значення $U = 0$ та $g = 0$. Згідно з п.2 процедури, значення B_g дорівнює двійковим розрядам $b_{g\cdot k+k} \cdot 2^{k-1} + b_{g\cdot k+2} \cdot 2^1 + + b_{g\cdot k+1}$ g-ого фрагмента множника B: $B_g = 001_2$. За п.3, відповідно до коду B_g здійснюється додавання $U = U + W_Q[1] = 0 + 1974 = 1974$. Значення U' складає $u_k \cdot 2^{k-1} + \ldots + u_1$: $U' = 110_2$. За п.4 реалізується корекція результату виходячи зі значення U': $U = U + C[6] = 1974 + + 22578 = 24552$. Відповідно до п.5 виконується зсув часткового добутку U на k: $U = 24552 >> 3 = 3069$. За п.6 індекс $g = 0+1=1$. В силу того, що $g = 1 < n/k = 4$, відбувається перехід для повторного виконання до п.2. Аналогічним чином виконується подальше обчислення для наступних фрагментів коду множника B довжиною k для $g \in \{1; 3\}$. Динаміка покрокових змін параметрів процедури наведена у табл.3. В результаті виконання п.4 при $g = 3$, частковий добуток U становить 2444. За п.6 здійснюється інкремент індексу $g = 3 + 1 = 4$. З огляду на те, що $g = n/k = 4$, виконання процедури завершується. Для отримання правильного результату обчислене значення U=2444 помножається на 2^{12}: $2444 \cdot 4096 \bmod 3763 = 1044$.

Таблиця 3. Динаміка покрокових змін параметрів процедури при обчисленні модулярного добутку при значеннях B = 2025, Q = 1974 та M = 3763

g	k-розрядний фрагмент коду B	$W_Q[B_g]$	Частковий добуток U	Молодші k розрядів U	$C[U']$	Частковий добуток U після корекції та зсуву на k розрядів
0	001	1974	1974	110	22578	3069
1	101	9870	12939	011	26341	4910
2	111	13818	18728	000	0	2341
3	011	5922	8263	111	11289	2444

Обчислення модулярної експоненти за запропонованим методом передбачає попереднє формування таблиці передобчислень C, що виконується відповідно до процедури побудови таблиці значень корекції на основі модуля для групової редукції Монтґомері. У рамках розробленого методу прискорена реалізація модулярного експоненціювання $A^E \bmod M$ здійснюється шляхом виконання наступної послідовності дій:

1. Змінній D присвоюється значення $A \cdot 2^n \bmod M$: $D = A \cdot 2^n \bmod M$, змінній результату R та індексу j двійкових розрядів коду експоненти присвоюється значення одиниці: $R = 1, j = 1$.
2. Виконується побудова таблиці W_Q передобчислень за описаною вище процедурою побудови таблиці W_Q для значення множеного Q: $Q = D$.
3. Якщо j-тий розряд коду експоненти E дорівнює одиниці: $e_j = 1$, то здійснюється прискорене модулярне множення $R = R \cdot Q \bmod M$ з використанням таблиці W_Q передобчислень та таблиці C для групової редукції за наведеною процедурою обчислення модулярного добутку.
4. Здійснюється прискорене модулярне множення $D = D \cdot Q \bmod M$ з використанням таблиць передобчислень W_Q та C відповідно до процедури обчислення модулярного добутку.
5. Реалізується інкремент індексу j: $j = j + 1$. Якщо $j <= n$, здійснюється повернення до п.2.

Обчислення модулярної експоненти з використанням запропонованої процедури ілюструється наступним прикладом. Нехай для наведеного прикладу обираються наступні значення параметрів: $A = 2025_{10} = 0111\ 1110\ 1001_2$; $E = 2731_{10} = 1010\ 1010\ 1011_2$; $M = 3763_{10} = 1110\ 1011\ 0011_2$; $A^E \bmod M = 2025^{2731} \bmod 3763 = 2025$.

Попередньо сформована таблиця C значень корекції для обраного модуля $M = 3763$ представлена у табл.2. Відповідно до п.1 процедури, значення $D = 2025*2^{12} \bmod 3763 = 748$, $R = 1$, $j = 1$. За п.2 виконується побудова таблиці W_{Q1} передобчислень для значення $Q = 748$, що наведена у табл.4 для $j = 1$.

Таблиця 4. Таблиця W_Q передобчислень для Q

j	1	2	3	4	5	6	7	8	9	10	11	12
Q	748	1974	3057	1316	2613	1282	890	3181	1424	1671	554	2063
p	W_{Q1}	W_{Q2}	W_{Q3}	W_{Q4}	W_{Q5}	W_{Q6}	W_{Q7}	W_{Q8}	W_{Q9}	W_{Q10}	W_{Q11}	W_{Q12}
0	0	0	0	0	0	0	0	0	0	0	0	0
1	748	1974	3057	1316	2613	1282	890	3181	1424	1671	554	2063
2	1496	3948	6114	2632	5226	2564	1780	6362	2848	3342	1108	4126
3	2244	5922	9171	3948	7839	3846	2670	9543	4272	5013	1662	6189
4	2992	7896	12228	5264	10452	5128	3560	12724	5696	6684	2216	8252
5	3740	9870	15285	6580	13065	6410	4450	15905	7120	8355	2770	10315
6	4488	11844	18342	7896	15678	7692	5340	19086	8544	10026	3324	12378
7	5236	13818	21399	9212	18291	8974	6230	22267	9968	11697	3878	14441

Виходячи з того, що $e_1 = 1$, за п.3 здійснюється прискорене модулярне множення $R = 1 \cdot 748 \bmod 3763 = 2025$ з використанням таблиці передобчислень W_Q

(табл.4) та таблиці C передобчислень (табл.2). Згідно з п.4 виконується модулярне множення D=748·748 mod 3763 = 1974 з використанням таблиці W_Q та таблиці C. Відповідно до п.5, реалізується інкремент індексу j = 1+1= 2. В силу того, що $j = 2 < n = 12$, здійснюється перехід до повторного виконання на п.2. За п.2 формується таблиця W_{Q2} передобчислень для значення $Q = D$ = 1974, наведена у табл.4 для j = 2. Згідно з п.3 здійснюється модулярне множення $R = 2025 \cdot 1974 \bmod 3763 = 2444$ з використанням таблиць W_Q та C передобчислень. Детальний опис обчислення модулярного добутку $R = 2025 \cdot 1974 \bmod 3763$ наведений у табл.3. Згідно з п.4 виконується модулярне множення $D = 1974 \cdot 1974 \bmod 3763 = 3057$ з використанням таблиці W_Q та таблиці C. Відповідно до п.5, реалізується інкремент індексу j =2+1= 3. В силу того, що $j = 3 < n = 12$, здійснюється перехід до повторного виконання на п.2. Аналогічним чином виконуються подальші обчислення. Таблиці передобчислень W_Q, сформовані на кожній ітерації алгоритму для спільного множника для мультиплікативних операцій наведено у таблиці 4. Проміжні результати, отримані в ході кожної ітерації, представлені в таблиці 5.

Таблиця 5. Динаміка покрокових змін при обчисленні $2025^{2731} \bmod 3763$

j	e_j	Q	R	D
-	-	-	1	748
1	1	748	2025	1974
2	1	1974	2444	3057
3	0	3057	2444	1316
4	1	1316	3240	2613
5	0	2613	3240	1282
6	1	1282	676	890
7	0	890	676	3181
8	1	3181	1734	1424
9	0	1424	1734	1671
10	1	1671	3311	554
11	0	554	3311	2063
12	1	2063	2025	1955

Остаточний результат модулярного експоненціювання, одержаний шляхом модулярного множення $3311 \cdot 2063 \bmod M$ становить 2025.

Оцінка ефективності

Виходячи з поставленої мети, ефективність розробленого методу визначається прискоренням виконання операції модулярного експоненціювання з його використанням. Для кількісної оцінки такого прискорення може бути використаний коефіцієнт прискорення β, що визначається співвідношенням часу T'_E реалізації експоненціювання класичним способом до часу T_E виконання цієї операції із застосуванням запропонованого методу:

$$\beta = \frac{T'_E}{T_E} . \qquad (1)$$

За класичним алгоритмом, модулярне експоненціювання здійснюється за n ітерацій, на кожній з яких виконується операція піднесення до квадрату та, в залежності від поточного розряду коду експоненти, операція модулярного множення. Тобто, у середньому, обчислення модулярної експоненти передбачає здійснення $1{,}5 \cdot n$ мультиплікативних операцій. На практиці, для їх реалізації найбільш ефективним вважається використання методу Монтґомері[]. Згідно з ним, час T'_M реалізації одного модулярного множення становить $T'_M = 2 \cdot n \cdot t_{ADD}$.

Таким чином, час T'_E здійснення всієї операції модулярного експоненціювання класичним способом складає:

$$T'_E = 1{,}5 \cdot n \cdot 2 \cdot n \cdot t_{ADD} = 3 \cdot n^2 \cdot t_{ADD} . \qquad (2)$$

Розроблений метод модулярного експоненціювання також передбачає виконання n ітерацій, на кожній з яких виконується, в середньому, 1,5 операції множення, для яких в якості одного з операндів використовується однаковий множник.

В рамках запропонованого методу, модулярне множення виконується згідно з описаною вище процедурою, яка використовує таблиці W_Q та C передобчислень.

Таблиця W_Q передобчислень залежить від значення поточного спільного операнда мультиплікативних операцій, що здійснюються на одній ітерації. Відповід-

но, побудова такої таблиці також виконується на кожній ітерації алгоритму експоненціювання, що впливає на загальний час обчислення модулярної експоненти. Водночас, таблиця C значень корекції для здійснення групової редукції відразу на k розрядів залежить виключно від модуля M, який є частиною відкритого ключа. Тому формування таблиці C реалізується практично одноразово на етапі генерації криптосистеми і не враховується при оцінці загального часу експоненціювання. Таким чином, час T_E обчислення модулярної експоненти із застосуванням запропонованого методу становить:

$$T_E = n \cdot (T_{TW} + 1{,}5 \cdot T_M), \qquad (3)$$

де T_{TW} – час побудови таблиці W_Q, і T_M – час реалізації модулярного множення із використанням розробленої процедури.

Час T_{TW} формування таблиці W_Q передобчислень становить

$$T_{TW} = 2^k \cdot t_{ADD}, \qquad (4)$$

де k – розрядність фрагментів множника, що оброблюються одночасно.

Запропонована процедура обчислення модулярного добутку передбачає здійснення n/k ітерацій. На кожній з них виконується дві операції додавання: числа з таблиці W_Q, яке адресується k-розрядним фрагментом множеного, та значення елементу таблиці C для виконання корекції проміжного результату. Кінцевою операцією в рамках ітерації є зсув часткового добутку на k розрядів праворуч. З цього випливає, що час здійснення модулярного множення із використанням таблиць передобчислень складає.

$$T_M = \frac{(1+1+1)\cdot n}{k} \cdot t_{ADD} = \frac{3\cdot n}{k} \cdot t_{ADD}. \qquad (5)$$

Відповідно, підстановка виразів (4) та (5) у (3), дозволяє представити формулу часу T_E обчислення модулярної експоненти із застосуванням запропонованого методу у наступному вигляду:

$$T_E = n \cdot (2^k \cdot t_{ADD} + 1{,}5 \cdot \frac{3\cdot n}{k} \cdot t_{ADD}). \qquad (6)$$

Підставивши значення T'_E та T_E у формулу (1), одержаний коефіцієнт прискорення β набуває вигляду:

$$\beta = \frac{3\cdot n}{2^k + \frac{4{,}5\cdot n}{k}}. \qquad (7)$$

З одержаного виразу випливає, що коефіцієнт β залежить від довжини k фрагментів та набуває найбільшого значення при мінімумі функції:

$$\varphi(k) = 2^k + \frac{4{,}5\cdot n}{k}. \qquad (8)$$

Теоретично, для визначення найбільш вигідного значення параметра k, можна розв'язати рівняння $2^k \cdot \ln 2 - \frac{4{,}5\cdot n}{k^2} = 0$. Очевидно, що воно не може бути розв'язане у явному вигляді. Тому значення k, за якого досягається найбільше прискорення, може бути знайдене лише числовими методами.

Результат обчислень коефіцієнта прискорення β для розрядностей n = 4096 та n = 8192 наведений у таблиці 6. Аналіз отриманих значень показав, що найбільшого прискорення β досягає при $k = 9$. Дані таблиці свідчать про те, що значення коефіцієнту β збільшується зі зростанням розрядності n.

Таблиця 6. Залежність коефіцієнту прискорення β від значення k

Параметр k	Коефіцієнт прискорення β	
	n = 4096	n = 8192
2	1.33275	1.33304
4	2.65744	2.66205
6	3.91837	3.95876
8	4.72125	5.05263
9	4.8	5.33333
10	4.28571	5.21739
12	2.18182	3.42857

Одержане підвищення швидкодії досягається за рахунок використання додаткових ресурсів оперативної пам'яті, необхідної для збереження таблиць передобчислень. Зокрема, для обробки 4096-бітових чисел при виборі розрядності фрагментів k = 8, обсяг необхідної пам'яті становить

$2^{12} \cdot 2^8 = 2^{20}$ біт, що еквівалентно 128 КБ. Такий об'єм ресурсних витрат цілком відповідає можливостям переважної більшості сучасних мікроконтролерів.

Проведені експериментальні дослідження показали близькі до наведених вище теоретично одержаних результатів оцінки ефективності.

Таким чином, теоретично доведено та експериментально підтверджено, що розроблений метод дозволяє підвищити швидкодію обчислення модулярної експоненти приблизно в 5 разів в порівнянні з класичним алгоритмом експоненціювання.

Висновки

В ході проведених досліджень, направлених на прискорення комп'ютерної реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання, були отримані наступні результати.

Теоретично обґрунтовано, розроблено та досліджено метод прискореного обчислення модулярної експоненти, відмінність якого полягає в тому, що в кожній ітерації здійснюються передобчислення, які дозволяють виконувати модулярні операції множення та піднесення до квадрату з груповою обробкою розрядів на обох фазах: власне множенні та редукції Монтґомері, завдяки чому досягається скорочення часу реалізації експоненціювання.

Теоретичні дослідження ефективності розробленого методу довели, що його використання дозволяє прискорити обчислення приблизно в 5 разів у порівнянні з класичним алгоритмом. Проведені моделювання, а також практичні експерименти показали результати, в цілому, близькі до оцінок ефективності, одержаних теоретичним шляхом.

Запропонований метод модулярного експоненціювання орієнтований на використання у системах віддаленого управління об'єктами у режимі реального часу для забезпечення цілісності даних та автентичності команд у технологіях Інтернету Речей.

Література

1. Jurcut A.D., Xu R.R. Introduction to IoT Security. *IoT Security. Advances in Authentication.* 2020. P. 1-64. DOI: 10.1002.9781119527978.ch2.

2. Alfred Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. *CRC Press.* 2001. 780 p.

3. Гуцуляк Н.А., Селіванов В.Л., Володін В.В. Модулярне множення на постійне число з суміщенням групової обробки розрядів множника та редукції Монтгомері. *Проблеми управління та інформатизації.* 2025. № 1 (81). P. 95-104. DOI: 10.18372/2073-4751.81.20135

4. Kaloulli E., Zacharioudakis E. Survey of Cryptoprocessors Advances and Technological Trends. *Third International Conference on Innovation in Computing Research ICR 2024. Lecture Notes in Networks and Systems. Springer.* 2024. Vol. 1058. P. 441-430. DOI: 10.1007/978-3-031-65522-7-37

5. Haidukevych O. et al. A Secure Cloud Computing Method for Rapid Implementation of Cryptographic Data Protection in IoT. *13-th International Conference on Dependable system, Service and Technologies DESSERT-2023.* 2023. P. 674-677. DOI: 10.1109/DESSERT61349.2023.10416477.

6. Giorgi P., Imbert L., Izard T. Parallel modular multiplication on multicore processors. *IEEE Symposium on Computer Arithmetic, Apr 2013, Austin, TX, United States.* P.135-142

7. Bernstein D. J. Algorithmic Number Theory. *MSRI Publications.* 2008. Vol. 44. Ch. Fast multiplication and its applications, P. 325–384.

8. Стіренко С.Г. et al. Спосіб прискореного обчислення модулярної експоненти. *Вісник Національного технічного університету України "КПІ" Інформатика, управління та обчислювальна техніка.* 2017. №65. P. 110-115.

9. Zuras D. More on squaring and multiplying larges integers. *IEEE Transactions*

on Computers. 1994. Vol. 43, №8. P. 899-908.

10. Марковський О.П., Аль-Мраят Гассан Абдель Жаліль. Метод прискорення модулярного піднесення до квадрату довгих чисел для криптографічних застосувань. *Проблеми управління та інформатизації.* 2024. № 1 (77). P. 68-79. DOI: 10.18372/2073-4751.77.18659

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

12. Barrett P. Implementing the Rivest Shamir and Adleman Public Key Encryption Algorithm on a Standard Digital Signal Processor. *Proceedings CRYPTO'86.* 1986. P. 311-323.

13. Montgomery P. Modular multiplication without trial division. *Mathematics of Computation.* 1985. 44 (170). P. 519-521.

14. Bos J.W. et al: Montgomery multiplication using vector instructions. *Selected Areas in Cryptography — SAC.* 2013. P. 471–489. DOI: 10.1007/978-3-662-43414-7_24

15. Марковський О.П., Аль-Мраят Гассан Абдель Жаліль. Метод прискорення модулярного множення для механізмів криптографічного захисту з відкритим ключем. *Проблеми управління та інформатизації.* 2023. № 4 (76). P. 48-58. DOI: 10.18372/2073-4751.76.18240 .

Русанова О.В., Марковський О.П., Гайдукевич О.А.

МЕТОД ПРИСКОРЕНОГО МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ НА ОСНОВІ ДИНАМІЧНИХ ТАБЛИЦЬ ПЕРЕДОБЧИСЛЕНЬ

Теоретично обґрунтовано, розроблено та досліджено метод прискореного обчислення модулярної експоненти, відмінність якого полягає в тому, що в кожній ітерації здійснюються передобчислення, які дозволяють виконувати модулярні операції множення та піднесення до квадрату з груповою обробкою розрядів на обох фазах: власне множенні та редукції Монтґомері, завдяки чому досягається скорочення часу реалізації експоненціювання.

Прискорення досягається за рахунок формування таблиць передобчислень на кожній ітерації алгоритму експоненціювання. В роботі теоретично обґрунтована така можливість шляхом використання вбудованої оперативної пам'яті термінального пристрою, наведено детальний опис методу, робота якого ілюстрована числовим прикладом, представлена розгорнута оцінка ефективності.

Теоретично та експериментально показано, що запропонований метод дозволяє в 5 разів прискорити модулярне експоненціювання в порівнянні з відомими методами її реалізації на термінальних пристроях в технологіях IoT.

Ключові слова: *модулярне експоненціювання, криптографія з відкритим ключем, захищеність систем IoT, цифровий підпис.*

Rusanova O.V., Markovskyi O.P., O. Haidukevych

METHOD OF ACCELERATED MODULAR EXPONENTATION BASED ON DYNAMIC PRE-CALCULATION TABLES

A method for accelerated calculation of the modular exponent has been theoretically substantiated, developed and investigated, the difference of which is that in each iteration, recalculations are performed, which allow performing modular operations of multiplication and squaring with group processing of bits in both phases: multiplication itself and Montgomery reduction, due to which the time for implementing exponentiation is reduced.

Acceleration is achieved by forming recalculation tables at each iteration of the exponentiation algorithm. The paper theoretically substantiates this possibility by using the built-in RAM of the terminal device, provides a detailed description of the method, the operation of which is illustrated by a numerical example, and presents a detailed assessment of its effectiveness.

It is theoretically and experimentally shown that the proposed method allows for 5 times faster modular exponentiation compared to known methods for its implementation on terminal devices in IoT technologies.

Keywords: *modular exponentiation, open key cryptography, security of IoT, digital signature.*

УДК 629.735.064 5:621.39 (075.8) **DOI: 10.18372/2073-4751.83.20550**

Толстікова О.В., к.т.н.,
orcid.org/0000-0002-7616-2757
Водоп'янов С.В., к.т.н.,
orcid.org/0009-0006-0424-6173
Андреєв О.В., к.т.н.,
orcid.org/0000-0001-9032-1139
Толстіков О.Д.
orcid.org/0009-0006-1620-5221

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ОПТИМІЗАЦІЇ ЕКСПЕРТНИХ СИСТЕМ ТА БАЗ ДАНИХ РЕАЛЬНОГО ЧАСУ

Державний університет «Київський авіаційний інститут»

e-mail: olena.tolstikova@npp.kai.edu.ua,
e-mail: serhii.vodopianov@npp.kai.edu.ua,
e-mail: oleksandr.andreiev@npp.kai.edu.ua,
e-mail: tolstikov.o@kitu.nau.edu.ua

Вступ

Розглядається завдання застосування експертної системи з базою даних (БД) реального часу, які використовуються для сумісної (інтегральної) оптимізації маршрутів інформаційно-комунікаційної мережі. Існують алгоритми маршрутизації з різними технологіями доставляння даних по критеріям мінімальної затримки (latency), прийнятної наскрізної якості сервісу (Quality of Service, QoS) та надійності доставляння у сенсі мінімальної величини перекручених бітів відносно загальної кількості доставлених бітів (Bit Error Ratio, BER). Найпоширенішими є алгоритми адаптивної (або динамічної) маршрутизації з дуальним навчанням [13]. Ці алгоритми забезпечують автоматичну апперцепцію таблиць маршрутизації (ТМ) після зміни конфігурації мережі. Протоколи, побудовані на основі адаптивних алгоритмів, забезпечують всім маршрутизаторам збирання інформації про топологію зв'язків у мережі, оперативне опрацювання всіх змін конфігурації зв'язків. У ТМ при адаптивній маршрутизації зазвичай є інформація про інтервал часу, протягом якого даний маршрут залишатиметься дійсним (Time-to-Live, TTL)

Адаптивні алгоритми маршрутизації мають розподілений характер і повинні відповідати декільком ключовим вимогам [5]. Перше, вони повинні забезпечувати якщо не оптимальність, то хоча б раціональність маршруту. Друге, алгоритми мають бути достатньо простими, щоб при їх реалізації не витрачалося дуже багато мережних ресурсів, зокрема, вони не повинні вимагати надмірно великого об'єму обчислень або