УДК 004.052.42

DOI: 10.18372/2073-4751.78.18966

Русанова О.В., к.т.н.,
orcid.org/0000-0003-0145-3012,
e-mail: olha.rusanova@npp.nau.edu.ua,
Гайдукевич М.А.,
orcid.org/0000-0003-2334-2401,
e-mail: mgrnchnk@gmail.com

МЕТОД РОЗПОДІЛЕНОГО МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ НА ТЕРМІНАЛЬНИХ МІКРОКОНТРОЛЕРАХ IoT ІЗ ЗАХИЩЕНИМ ЗАЛУЧЕННЯМ ХМАРНИХ ОБЧИСЛЕНЬ

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

Вступ

В епоху динамічного прогресу мережевих технологій, широкого розповсюдження набувають системи віддаленого моніторингу стану об'єктів реального світу та керування ними з використанням Інтернету в якості середовища обміну даними. Вказані системи отримали назву Інтернет Речей (*Internet of Things*). Останніми роками технології *IoT* стали активно поширюватись на такі сфери комп'ютерного управління, як віддалене керування інфраструктурними об'єктами, транспортними засобами, технологічними процесами [1]. Для всіх цих застосувань критично важливим є забезпечення високого рівня захисту даних. Останнє зумовлене тим, що використання Інтернету, як потенційно вразливого середовища для обміну даними, спричиняє небезпеку зовнішнього втручання в роботу систем керування критичними об'єктами.

З практичної точки зору важливо забезпечити достовірність та автентичність повідомлень, якими обмінюються термінальні мікроконтролери таких систем керування. Для забезпечення цього традиційно використовуються механізми цифрового підпису типу *DSS* чи *ISO* 979. В основі вказаних механізмів цифрового підпису лежить операція модулярного експоненціювання $A^E \bmod M$. Зазначена операція проводиться над числами великої розрядності, яка визначає рівень захищеності цифрового підпису від фальсифікації. На сьогоднішній день розрядність чисел складає 4096, причому існує перспектива її збільшення до 8192 протягом найближчих років [2]. Водночас збільшення зазначеної розрядності з метою підвищення рівня захищеності спричиняє значне зростання обчислювальної складності модулярного експоненціювання. Показано [3], що збільшення розрядності вдвічі має наслідком зростання обчислювальної складності у 8 разів. В силу того, що всі системи Інтернету Речей працюють в режимі реального часу, існують жорсткі вимоги щодо швидкості реалізації модулярного експоненціювання. На практиці у більшості випадків належна швидкість обчислень не може бути забезпечена за рахунок можливостей малопотужних портативних термінальних мікроконтролерів.

Одне із ефективних рішень цієї проблеми полягає в залученні до обчислень модулярної експоненти віддалених потужних комп'ютерних систем. Недоліком такого рішення виступає потреба у використанні додаткових засобів для захисту від незаконної реконструкції секретних компонент модулярного експоненціювання за даними, що передаються на віддалену систему.

Таким чином, наукова задача підвищення ефективності віддаленої розподіленої реалізації операції модулярного експоненціювання шляхом прискорення обчислень із забезпеченням належного рівня захищеності, є актуальною зважаючи на сучасний стан та перспективи подальшого розвитку інформаційних технологій.

Оглядовий аналіз існуючих методів розподіленого захищеного модулярного експоненціювання

Реалізація операції модулярного експоненціювання $A^E \bmod M$ проводиться за одним із двох існуючих алгоритмів [4]. Для обох з них передбачається виконання циклу побітової обробки n-розрядного коду експоненти, причому на кожній ітерації в залежності від значення поточного біту здійснюються різні операції. Суттєва різниця вказаних алгоритмів полягає у порядку обробки коду E. На відміну від першого із них, який передбачає виконання обчислень починаючи зі старших розрядів, у другому алгоритмі обробка експоненти проводиться з молодших бітів коду E.

Для вирішення проблеми віддаленої швидкої реалізації модулярного експоненціювання $A^E \bmod M$ в системах *IoT* на сьогоднішній день розроблено низку методів розподілу обчислень між термінальною та хмарною платформами, із забезпеченням практичного унеможливлення реконструкції секретних компонентів A і E. Критеріями оцінки ефективності існуючих рішень виступають два показники: прискорення виконання операції модулярного експоненціювання за рахунок залучення до її обчислень віддалених комп'ютерних потужностей, а також рівень захищеності від незаконних спроб відновлення значень секретних компонентів у вказаній операції.

Усі запропоновані на сьогоднішній день методи захищеного модулярного експоненціювання можна розділити на два класи. До першого належать методи, які виходять із того, що відомі параметри генерації криптосистеми з відкритим ключем [3]. Другий клас, відповідно, складається з методів, які припускають, що такі параметри невідомі. Для другого класу методів, шифрування компоненти закритого ключа E здійснюється шляхом адитивного або адитивно-мультиплікативного розкладання коду E. Зокрема найпростіший спосіб адитивно-мультиплікативного представлення n-розрядного коду E передбачає його розкладення у вигляді $E = (L + Q) \cdot \gamma$. Використання такого розкладання дозволяє реалізувати шифрування інформаційної компоненти A як: $B = A^\gamma \bmod M$ [5]. Тоді на термінальній платформі *IoT* виконується обчислення $V = B^L \bmod M$, в той час як у хмарі реалізується обрахунок $W = B^Q \bmod M$. Отримане в ході віддалених розрахунків значення W відправляється на мікроконтролер, де обчислюється кінцевий результат R шляхом виконання на мікроконтролері модулярного множення $R = (B^L \bmod M \cdot B^Q \bmod M) \bmod M$. Якщо позначити через r_L та r_γ розрядності кодів L та γ відповідно, то об'єм обчислень, що виконуються на термінальній платформі визначається тривалістю здійснення $1.5 \cdot (r_L + r_\gamma)$ модулярних множень. У відомих рішеннях [5,6] $r_L + r_\gamma << n$, а часова ефективність визначається співвідношенням $n/(r_L + r_\gamma)$. При цьому рівень захисту від незаконного відновлення кодів A та E на віддаленій комп'ютерній системі визначається об'ємом перебору можливих значень L та γ, який дорівнює $2^{r_L + r_\gamma}$. Це означає, що у існуючих методах швидкодія виконання операції модулярного експоненціювання з використанням можливостей віддалених систем жорстко обмежена рівнем захищеності.

Серед запропонованих рішень проблеми прискореного захищеного віддаленого модулярного експоненціювання, одним із найбільш перспективних вбачається [7]. Цей метод передбачає представлення коду експоненти у вигляді $E = (L + F) \cdot 2$, зі збереженням при цьому значення $E \bmod 2$ в змінну β: $\beta = E \bmod 2$. Обчислення модулярної експоненти $A^E \bmod M$ проводиться за алгоритмом з молодших розрядів. Ідея методу полягає у тому, що на віддаленій комп'ютерній системі обчислюється $B^F \bmod M$, в той час як на термінальному мікроконтролері реалізується обрахунок $B^L \bmod M$, де B – зашифроване представлення компоненти A після її піднесення до модулярного квадрату: $B = A^2 \bmod M$. В рамках реалізації методу [7], існує суттєва відмінність в організації обчислень на хмарній та термінальній платформах. Якщо на першій з них алгоритм модулярного експоненціювання з молодших

розрядів виконується в повному обсязі, то в ході обчислень на термінальній платформі використовуються результати здійснених у хмарі обрахунків. Для цього код $G = L + F$ поділяється на k інтервалів, в кінці обробки кожного з яких частковий результат обчислень передається із хмари на термінальний мікроконтролер. Тоді на останньому відбувається обробка компоненти F, яка представляється у вигляді $F = f_0 + f_1 \cdot 2^h + \ldots + f_{k-1} \cdot 2^{(k-1)h}$, тобто суми кодів $f_0, f_1, \ldots, f_{k-1}$, де $\forall i \in \{0,1,\ldots,k\text{-}1\}$: $f_i \in \{0,1,\ldots,2^h\text{-}1\}$.

Об'єм обчислень, які виконуються на термінальній платформі, у рішенні [7] визначається кількістю модулярних множень $C = 1.5 \cdot \delta + 1 + \beta + k$, де δ – це сумарна кількість розрядів кодів $f_0, f_1, \ldots, f_{k-1}$. При цьому передбачається, що зловмиснику відоме число C, а також значення B, F, h, k та модуль M, де h – це довжина кожного з k сегментів експоненти G. Окрім цього сторона, що здійснює злам, має доступ до результату обчислення $B^L \bmod M$ у хмарі та до кінцевого результату модулярного експоненціювання $A^E \bmod M$. Об'єм перебору всіх можливих значень δ-розрядного коду $f_0, f_1, \ldots, f_{k-1}$ складає 2^δ. Водночас з огляду на те, що зловмиснику невідомі розрядності кожного з кодів $f_0, f_1, \ldots, f_{k-1}$, кількість всіх можливих варіантів їх значень складає:

$$\theta = \frac{(\delta+k-1)!}{\delta! \cdot (k-1)!}. \qquad (1)$$

Таким чином об'єм перебору можливих значень кодів $f_0, f_1, \ldots, f_{k-1}$ з врахуванням всіх варіантів їх розрядностей визначається як $2^\delta \cdot \theta$.

Числа k та δ у розглянутому рішенні визначаються вимогами до захищеності при конкретному практичному застосуванні методу. Цілком очевидно, що зростання рівня захищеності зумовлює збільшення цих значень, а отже і числа C об'єму обчислень на термінальній платформі.

Детальний аналіз розглянутого відомого рішення [7] свідчить про те, що існують теоретичні можливості підвищення його ефективності за рахунок зменшення обчислювального навантаження на малопотужну термінальну платформу шляхом перенесення для реалізації в хмарі частини операцій, не пов'язаних з секретним кодом експоненти. Іншими словами існують можливості підвищення часової ефективності розподіленого обчисления модулярної експоненти без втрати рівня захищеності.

Мета досліджень

Мета досліджень полягає в підвищенні ефективності розподіленого обчислення модулярної експоненти з залученням віддалених потужностей за рахунок зменшення обчислювального навантаження на малопотужну термінальну платформу.

Метод розподіленого багатоваріантного експоненціювання

Для досягнення поставленої мети запропоновано метод розподіленого обчислення модулярної експоненти на термінальному мікроконтролері та хмарних системах з захистом від відновлення секретного коду експоненти за даними, які передаються на такі системи.

Основним чинником підвищення ефективності в запропонованому методі виступає зменшення навантаження на менш потужну складову апаратних засобів, залучених до обчислення модулярної експоненти.

Для забезпечення захисту інформаційної складової A, В рамках віддаленої реалізації модулярного експоненціювання $A^E \bmod M$, запропонований метод передбачає її шифрування. Таке шифрування здійснюється шляхом виконання на термінальному мікроконтролері модулярного піднесення до квадрату значення A: $B = A \cdot A \bmod M$. При цьому n-розрядний код E ділиться на число 2, тобто виконується зсув E на один розряд $P = E >> 1$. Подальше обчислення модулярної експоненти $B^P \bmod M$ здійснюється вже з використанням $(n\text{-}1)$-розрядного коду P. Перед початком обчислень на термінальному мікроконтролері змінній R присвоюється значення A або 1, залежно від парності коду експоненти E: $R = A^{E \bmod 2}$.

Запропонований метод передбачає поділ коду $P = p_1 \cdot 2^0 + p_2 \cdot 2^1 + \ldots + p_{n-1} \cdot 2^{n-2}$, де $\forall\, j \in \{1,2,\ldots, n\text{-}1\}$: $p_j \in \{0,1\}$, на h сегментів, в рамках кожного з яких a розрядів залишаються секретними, в той час як b розрядів надсилаються на віддалений процес. Тобто розрядність кожного з h сегментів дорівнює $b+a$. Таким чином у хмару надсилаються число B, модуль M, та код $F = f_1 \cdot 2^0 + f_2 \cdot 2^1 + \ldots + f_{n-1} \cdot 2^{n-2}$, отриманий в ході наступної модифікації коду P:

$$\forall j \in \{1,2,\ldots,n-1\}: \begin{cases} j\ mod(a+b) \le b: f_j = p_j; \\ j\ mod(a+b) > b: f_j = 0. \end{cases} \quad (2)$$

На віддаленій комп'ютерній системі змінній D_0 присвоюється значення B: $D_0 = B$. Після цього відбувається послідовна обробка кожного з h сегментів коду експоненти F описаним нижче способом.

Для i-того сегменту, $i \in \{1, h\}$, організовується рекурентне обчислення значень $D_{(i\text{-}1)(a+b)+1} = D_{(i\text{-}1)(a+b)}^2\ mod\ M$, $D_{(i\text{-}1)(a+b)+2} = D_{(i\text{-}1)(a+b)+1}^2\ mod\ M$, …, $D_{i(a+b)} = D_{i(a+b)\text{-}1}^2\ mod\ M$. Крім того, з використанням молодших b розрядів сегменту, здійснюється обчислення значення Q_i:

$$Q_i = \left(\prod_{k=1}^{b} D_{k+(i-1)(a+b)-1}^{\,f_{k+(i-1)(a+b)}}\right) mod\ M. \quad (3)$$

Наступний етап запропонованого методу передбачає обчислення множини Θ_i часткових експонент $\Theta_i = \{W_{i,0}, W_{i,1}, \ldots W_{i,Y}\}$, $\forall\ Y \in \{0,1,\ldots, 2^a\text{-}1\}$ у відповідності до всіх 2^a варіантів a-розрядних двійкових кодів Y: $Y = y_1 \cdot 2^0 + y_2 \cdot 2^1 + \ldots + y_m \cdot 2^{a-1}$, де $\forall\ m \in \{1,2,\ldots, a\}$: $y_m \in \{0,1\}$. Значення $W_{i,Y}$ обчислюються за наступною формулою:

$$\forall Y \in \{0,1,\ldots,2^a-1\}: W_{i,Y} = \left(Q_i \cdot \prod_{m=1}^{a} D_{m+ib+(i-1)a-1}^{\,y_m}\right) mod\ M. \quad (4)$$

Технологічно, більш ефективним вбачається наступний порядок обчислення формули (4). Паралельна обробка 2^a варіантів a-розрядних експонент здійснюється в порядку зростання кількості одиниць в їхніх двійкових кодах. Тоді кожне зі значень $W_{i,Y}$ отримується шляхом виконання модулярного множення одного з обчислених раніше результатів $W_{i,0}$, …, $W_{i,Y\text{-}1}$ на відповідне значення D. Таким чином першим кроком є обчислення значення $W_{i,0}$, яке фактично дорівнює числу Q_i. Далі реалізується обрахунок тих a варіантів кодів, в яких a-1 розрядів дорівнюють нулю і один розряд дорівнює 1, шляхом обчислення для кожного з цих кодів модулярного добутку числа $W_{i,0}$ та відповідного одиничному розряду значення D. За аналогічним принципом реалізується поетапна обробка всіх інших 2^a-a-1 варіантів кодів експоненти, поки не отримується множина значень $\Theta_i = \{W_{i,0}, W_{i,1}, \ldots W_{i,Y}\}$. Після обробки i-того сегменту, множина Θ_i результатів обчислень у кількості 2^a значень надсилається на термінальний мікроконтролер, на якому виконується модулярне множення змінної R та значення $W_g = \{W_{i,0}, W_{i,1}, \ldots W_{i,Y}\}$, $g = p_{(i\text{-}1)a+i\cdot b+1} \cdot 2^0 + p_{(i\text{-}1)a+i\cdot b+2} \cdot 2^1 + \ldots + p_{(a+b)i} \cdot 2^{a-1}$: $R = R \cdot W_g\ mod\ M$. Кінцевий результат обчислень формується на термінальному мікроконтролері у змінній R після отримання результатів обробки на віддаленій комп'ютерній системі h-того сегменту та виконання останнього модулярного добутку.

Числовий приклад

Робота запропонованого методу може бути проілюстрована наступним числовим прикладом. Нехай обчислюється модулярна експонента $A^E mod M = 463^{22895} mod 30551 = 1786$. Тобто $A = 463_{10} = 111001111_2$, $E = 22895_{10} = 101100101101111_2$, $M = 30551_{10} = 111011101010111_2$, відповідно в рамках поточного прикладу розрядність експоненти $n = 15$. Окрім цього обираються значення кількості фрагментів поділу $(n\text{-}1)=14$-розрядної експоненти $h = 2$, а також розрядності $a = 3$ та $b = 4$. Згідно з описаним порядком обчислень, першим кроком є виконання гомоморфного

шифрування компоненти A шляхом піднесення її значення до модулярного квадрату: $B = A^2 \ mod \ M = 463^2 \ mod \ 30551 = 512$. Тоді код P дорівнює $P = E/2 = 11447_{10} = 10110010110111_2$, а змінній R на термінальному мікроконтролері присвоюється початкове значення A: $R = A = 463$. Далі відбувається поділ коду P на 2 сегменти, де 1-ий молодший сегмент має вигляд 0110111_2, а 2-ий – 1011001_2. Схематично поділ коду P в рамках розглянутого прикладу показано на рис. 1:

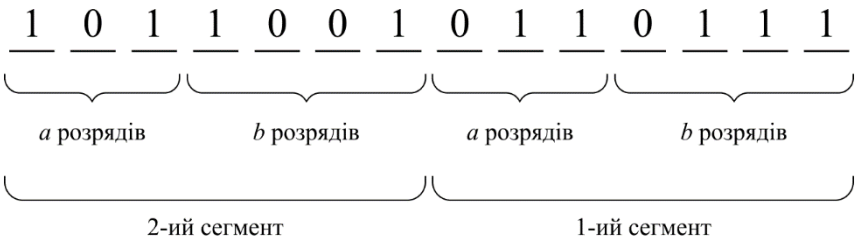

Рис. 1. Приклад поділу коду P на $h = 2$ сегментів

З 14-ти розрядів коду P експоненти, $a \cdot h = 6$ розрядів є секретними для хмари, тому на віддалену комп'ютерну систему здійснюється відправка коду F, отриманого в ході модифікації експоненти P, вигляду: $F = 00010010000111_2$. Окрім цього в хмару надсилаються число $B = 512$ та модуль $M = 30551$. На віддаленій комп'ютерній системі змінній D_0 присвоюється значення B: $D_0 = B = 512$, після чого починається обробка першого сегменту експоненти F. Організовується обчислення відповідних першому сегменту значень модулярних квадрати $D_1, \ldots, D_7$. Результати обчислень представлені у вигляді табл. 1.

Таблиця 1. Приклад обчислення $D1,\ldots, D7$ для першого сегменту

Номер розряду експоненти F	Значення модулярного квадрату
1	$D_1 = 512^2 \ mod \ 30551 = 17736$
2	$D_2 = 17736^2 \ mod \ 30551 = 12600$
3	$D_3 = 12600^2 \ mod \ 30551 = 17004$
4	$D_4 = 17004^2 \ mod \ 30551 = 1352$
5	$D_5 = 1352^2 \ mod \ 30551 = 25395$
6	$D_6 = 25395^2 \ mod \ 30551 = 4966$
7	$D_7 = 4966^2 \ mod \ 30551 = 6499$

Далі при обробці чотирьох ($b = 4$) молодших розрядів коду F, значення яких дорівнюють $f_1 = 1$, $f_2 = 1$, $f_3 = 1$, $f_4 = 0$, обчислюється число Q_1 у вигляді модулярного добутку тих із значень $D_0, \ldots, D_3$, яким відповідають рівні одиниці розряди з f_1-f_4, тобто $Q_1 = (D_0 \cdot D_1 \cdot D_2) \ mod \ M$. Отже значення Q_1 розраховується як $Q_1 = (512 \cdot 17736 \cdot 12600) \ mod \ 30551 = 8387$. З використанням отриманого числа $Q_1 = 8387$, здійснюється обчислення множини Θ_1 значень $W_{1,0}, W_{1,1}, \ldots, W_{1,Y}, \forall \ Y \in \{0,1,\ldots, 2^a\text{-}1\}$. Відповідно до розрядності $a = 3$, множина кодів Y складає $2^3 = 8$ значень: $\{0,1,\ldots,7\}_{10} = \{000, 001, \ldots, 111\}_2$. Згідно з описаним вище оптимізованим порядком обчислення множини Θ_i часткових експонент, розрахунок кожного із чисел $W_{i,Y}$ здійснюється в порядку зростання кількості одиниць у двійковому коді Y. Тобто в рамках поточного прикладу обчислення значень $W_{i,Y}$ проводиться в такому порядку кодів Y: $000_2, 001_2, 010_2, 100_2, 011_2, 101_2, 110_2, 111_2$. Тоді розрахунок кожного із чисел $W_{1,Y}$ потребує виконання одного модулярного множення, як показано у табл. 2.

Таблиця 2. Обчислення множини Θ_1 значень W_{1Y}

Двійковий код $Y = y_3y_2y_1$	Значення W_{1Y}
000	$W_{1,0} = Q_1 = 8387$
001	$W_{1,1} = (Q_1 \cdot D_4) \bmod M = (8387 \cdot 1352) \bmod 30551 = 4803$
010	$W_{1,2} = (Q_1 \cdot D_5) \bmod M = (8387 \cdot 25395) \bmod 30551 = 16844$
100	$W_{1,4} = (Q_1 \cdot D_6) \bmod M = (8387 \cdot 4966) \bmod 30551 = 8829$
011	$W_{1,3} = (W_{1,1} \cdot D_5) \bmod M = (4803 \cdot 25395) \bmod 30551 = 12593$
101	$W_{1,5} = (W_{1,1} \cdot D_6) \bmod M = (4803 \cdot 4966) \bmod 30551 = 21918$
110	$W_{1,6} = (W_{1,2} \cdot D_6) \bmod M = (16844 \cdot 4966) \bmod 30551 = 29217$
111	$W_{1,7} = (W_{1,6} \cdot D_4) \bmod M = (29217 \cdot 1352) \bmod 30551 = 29492$

Після проведення розрахунків, множина Θ_1 надсилається на термінальний мікроконтролер, де виконується модулярне множення значення $W_{1,3}$, яке відповідає розрядам p_1-p_7 експоненти P, та числа R: $R = R \cdot W_{1,3}$ *mod* 30551 = 463 · 12593 *mod* 30551 = 25869. В той же час на віддаленій комп'ютерній системі запускається процес обробки другого сегменту коду експоненти F. Обчислюються відповідні другому сегменту модулярні піднесення до квадрату $D_8,\ldots, D_{14}$. Результати обчислень наведені у вигляді табл. 3.

Таблиця 3. Приклад обчислення $D_8,\ldots, D_{14}$ для другого сегменту

Номер розряду експоненти F	Значення модулярного квадрату
8	$D_8 = 6499^2$ *mod* 30551 = 15519
9	$D_9 = 15519^2$ *mod* 30551 = 5828
10	$D_{10} = 5828^2$ *mod* 30551 = 23423
11	$D_{11} = 23423^2$ *mod* 30551 = 2071
12	$D_{12} = 2071^2$ *mod* 30551 = 11901
13	$D_{13} = 11901^2$ *mod* 30551 = 29916
14	$D_{14} = 29916^2$ *mod* 30551 = 6062

Для f_8-f_{11} розрядів коду F, значення яких дорівнюють $f_8 = 1$, $f_9 = 0$, $f_{10} = 0$, $f_{11} = 1$, обчислюється значення Q_2 у вигляді модулярного добутку тих із значень $D_7, \ldots, D_{10}$, яким відповідають рівні одиниці розряди з f_8-f_{11}: $Q_2 = (D_7 \cdot D_{10})$ *mod M*, $Q_2 = (6499 \cdot 23423)$ *mod* 30551 = 20995. З використанням числа Q_2= 20995 проводиться розрахунок множини значень $\Theta_2 = \{W_{2,0}, W_{2,1}, \ldots, W_{2,7}\}$ на основі відповідних кодів $Y = \{0,1,\ldots,7\}_{10} = \{000, 001, \ldots, 111\}_2$. Аналогічно першому сегменту, розрахунок кожного із чисел $W_{2,Y}$ потребує виконання одного модулярного множення. Результати обчислень наведені у вигляді табл. 4:

Таблиця 4. Обчислення множини Θ_2 значень W_{2Y}

Двійковий код $Y= y_3y_2y_1$	Значення W_{2Y}
000	$W_{2,0} = Q_2 = 20995$
001	$W_{2,1} = (Q_2 \cdot D_{11}) \bmod M = (20995 \cdot 2071) \bmod 30551 = 6572$
010	$W_{2,2} = (Q_2 \cdot D_{12}) \bmod M = (20995 \cdot 11901) \bmod 30551 = 15417$
100	$W_{2,4} = (Q_2 \cdot D_{13}) \bmod M = (20995 \cdot 29916) \bmod 30551 = 18962$
011	$W_{2,3} = (W_{2,1} \cdot D_{12}) \bmod M = (6572 \cdot 11901) \bmod 30551 = 2812$
101	$W_{2,5} = (W_{2,4} \cdot D_{11}) \bmod M = (18962 \cdot 2071) \bmod 30551 = 12267$
110	$W_{2,6} = (W_{2,4} \cdot D_{12}) \bmod M = (18962 \cdot 11901) \bmod 30551 = 17076$
111	$W_{2,7} = (W_{2,6} \cdot D_{11}) \bmod M = (17076 \cdot 2071) \bmod 30551 = 16889$

Після завершення обчислень здійснюється відправка множини $\Theta_2 = \{W_{2,0}, W_{2,1}, \ldots, W_{2,7}\}$ на термінальну платформу. Останнім етапом модулярного експоненціювання є обчислення на мікроконтролері модулярного добутку числа R та отриманого з хмари значення $W_{2,5}$, яке відповідає розрядам p_8-p_{14} експоненти P: $R = R \cdot W_{2,5}$ *mod* 30551 = 25869 · 12267 *mod* 30551 = 1786. Отримане число R = 1786 є кінцевим результатом модулярного експоненціювання.

Оцінка ефективності

Оцінка ефективності запропонованого методу проводиться за двома базовими критеріями. Першим із них виступає рівень захищеності від незаконної реконструкції секретного коду експоненти в хмарі за надісланими на неї даними. В якості другого критерію ефективності використовується коефіцієнт прискорення реалізації модулярного експоненціювання за рахунок залучення віддалених комп'ютерних потужностей.

Рівень захищеності визначається об'ємом обчислювальних ресурсів для реконструкції експоненти. Однією з найбільш ефективних тактик такого зламу вбачається перебір усіх можливих варіантів кодів експоненти. Це зумовлено тим фактом, що операція модулярного експоненціювання найчастіше використовується в системах *IoT* для реалізації механізмів цифрового підпису, який передається по мережі [8]. Відповідно можна припустити, що зловмисник може мати доступ до кодів A та $L = A^E \bmod M$, через моніторинг пересилки повідомлень у потенційно вразливому середовищі Інтернет. Таким чином, в ході перебору кодів експоненти, сторона, що здійснює злам, може впевнитись у правильності підібраного коду шляхом порівняння обчисленої експоненти зі значенням L. Така тактика зламу передбачає перебір 2^γ можливих кодів, де γ – це кількість невідомих для зловмисника розрядів E, значення яких не надсилаються на віддалену комп'ютерну систему. На практиці параметр γ вибирається таким чином, щоб виходячи із вимог конкретного застосування, зробити перебір недоцільним, з огляду на вартісну оцінку потрібних для його здійснення ресурсів. В рамках запропонованого методу кількість розрядів E, значення яких не передаються в хмару, визначається як $a \cdot h$. Тобто граничний об'єм перебору значень W складає при цьому 2^{a+b}. Відповідно належний рівень захищеності досягається при виконанні такої умови:

$$a \cdot h = \gamma. \qquad (5)$$

Цілком очевидно, що умова (5) забезпечує можливість гнучкого вибору параметрів реалізації h, a та b, а отже дозволяє адаптувати систему залежно від вимог до безпеки, що визначаються параметром γ.

Другим чинником ефективності запропонованого методу виступає прискорення реалізації модулярного експоненціювання. В рамках методу обчислення

організовуються у вигляді трьох взаємопов'язаних процесів: обчислень на віддаленій системі, передачі їх результатів на термінальний мікроконтролер, а також обробки на останньому секретних кодів експоненти. Швидкість обчислення модулярної експоненти в запропонованому методі повністю залежить від часу роботи термінального мікроконтролера, часові характеристики якого вважаються заданими. Відповідно прикорення модулярного експоненціювання може бути досягнене за рахунок виконання двох чинників: зменшення кількості операцій на мікроконтролері та забезпечення безперервності його роботи.

Оскільки у запропонованому методі обробка h сегментів коду експоненти здійснюється за однаковим алгоритмом, аналіз часових характеристик трьох вказаних процесів може бути проведений в межах одного із сегментів. Якщо вважати, що час здійснення розрахунків на віддаленій системі перевищує час пересилки даних, то схематично послідовність процесів в запропонованому методі можна представити у вигляді рис. 2:

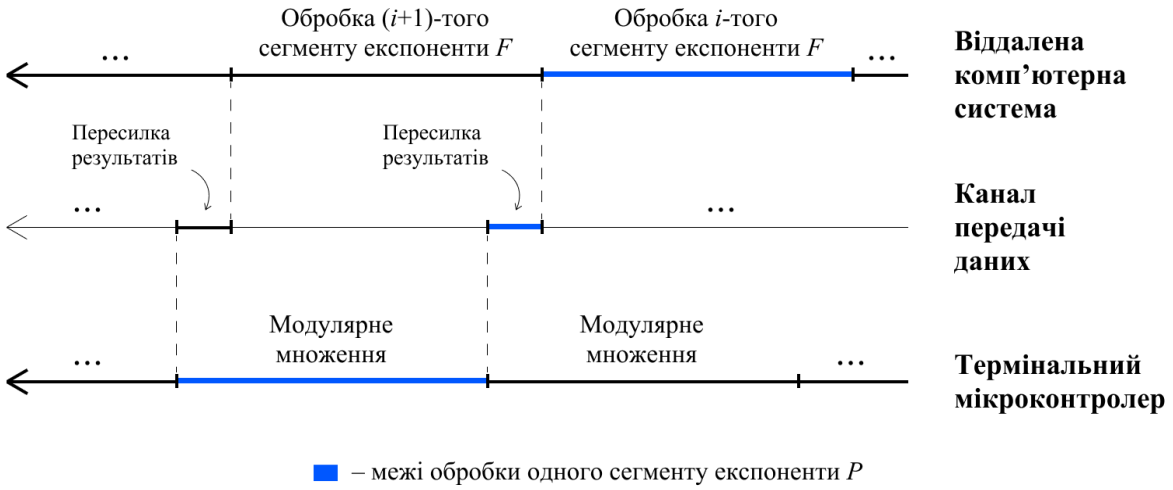

Рис. 2. Схематичне представлення часової послідовності виконання процесів

Найбільша часова ефективність запропонованого методу досягається за умови, якщо критичний шлях обчислювального процесу визначається часом t_{mm} виконання модулярного множення на термінальному мікроконтролері у кількості h разів (відповідно до кількості сегментів коду експоненти). Для забезпечення вказаної умови, об'єм обчислень, які виконуються в хмарі, має бути таким, щоб момент завершення пересилки на термінальну платформу результатів віддаленої обробки поточного сегменту коду експоненти практично співпадав з моментом завершення на мікроконтролері виконання модулярного множення в рамках попереднього сегменту.

Для створення адекватної математичної моделі запропонованого методу, доцільно показати, що для реальних систем час виконання обчислень в хмарі значно перевищує час пересилки їх результатів на термінальну платформу, а отже він не впливає на часову ефективність методу. Згідно з описаною вище послідовністю обчислень в запропонованому методі, в межах обробки одного сегменту експоненти F в хмарі, передбачається виконання $2^a + 1.5 \cdot b + a$ модулярних множень. Якщо позначити час реалізації такої операції як t_{mc}, то тривалість виконання у хмарі всіх обчислень в межах одного з h сегментів експоненти F визначається як $(2^a + 1.5 \cdot b + a) \cdot t_{mc}$. В переважній більшості випадків такі системи оснащені криптопроцесором, який дозволяє ефективно виконувати модулярне множення на апаратному рівні. За умови залучення до обчислень можливостей зазначених систем, час модулярного множення визначається часовими характеристиками, відповідними для конкретного криптопроцесора. Зокрема якщо

використовувати криптопроцесор *CryptoSwift* 600, то типовий час обчислення одного модулярного добутку на ньому становить приблизно 0.05 мс [2], тобто t_{mc} = 0.05 мс. За результатами попереднього аналізу можна вважати, що значення розрядності a лежить в межах від 3 до 6, а розрядність b при цьому дорівнює 61, 56, 45 чи 24 відповідно. Тоді для типової, в рамках запропонованого методу, пари значень a = 6 та b = 24 час здійснення обробки одного сегменту експоненти F на віддаленій системі розраховується як $(2^6 + 1.5 \cdot 24 + 6) \cdot 0.05 = 5.3$ мс.

Як показано на рис. 2, після віддаленої обробки кожного сегменту коду експоненти F, організовується пересилка результатів в розмірі 2^a значень на термінальний мікроконтролер через Інтернет. Час передачі блоку інформації з використанням Інтернету складається з часу встановлення мережевого з'єднання t_C та власне часу t_S пересилки даних. Тривалість встановлення мережевого з'єднання залежить від багатьох чинників, проте за даними [9] в оціночному плані, її середній час становить близько 40 мс. З іншого боку, орієнтовне значення швидкості Інтернету за умови використання радіоканалу для пересилки даних, становить 100 *Mbps* [9]. Тоді, при значенні a = 6, визначеному в ході попереднього аналізу, час t_S передачі по такому каналу 2^a = 64 результатів, після обробки в хмарі одного сегменту експоненти, оцінюється в 1.28 мс. Таким чином показано, що час віддаленого виконання всіх обчислення в межах одного h з сегментів коду F значно перевищує час пересилки результатів цих обчислень на термінальну платформу. Відповідно останній з них не впливає на часові характеристики методу. Звідси стає очевидним, що для забезпечення безперервної роботи термінального мікроконтролера потрібно, щоб час $(2^a + 1.5 \cdot b + a) \cdot t_{mc}$ виконання в хмарі всіх обчислень в межах одного сегменту коду експоненти F не перевищував час t_{mm} здійснення на мікроконтролері одного модулярного множення:

$$(2^a + 1.5 \cdot b + a) \cdot t_{mc} \le t_{mm}. \qquad (6)$$

Якщо позначити як φ співвідношення часу модулярного множення на термінальному мікроконтролері до часу виконання цієї операції в хмарі: $\varphi = t_{mm}/t_{mc}$, то нерівність (6) можна представити у вигляді:

$$(2^a + 1.5 \cdot b + a) \le \varphi. \qquad (7)$$

Таким чином, вибір параметрів реалізації h, a та b запропонованого методу має задовольняти наступні системі нерівностей:

$$\begin{cases} a \cdot h \ge \gamma \\ 2^a + 1.5 \cdot b + a \le \varphi \end{cases}. \qquad (8)$$

Значення параметрів γ та φ визначаються конкретикою застосування методу, їхні значення встановлюються перед початком модулярного експоненціювання. З огляду на те, що кількість невідомих параметрів системи (8) більше за кількість нерівностей в ній, очевидно, що дана система не може бути розв'язана без введення додаткового рівняння. В силу того, що (n-1)-розрядний код експоненти P складається з h сегментів, кожен з яких містить a+b розрядів, система (8) може бути розширена до вигляду:

$$\begin{cases} a \cdot h \ge \gamma \\ 2^a + 1.5 \cdot b + a \le \varphi \\ h \cdot (a + b) = n - 1 \end{cases}. \qquad (9)$$

Оскільки на практиці число n вимірюється тисячами, можна вважати, що $n - 1 \approx n$. Тоді для спрощення розрахунків третє рівняння може бути змінене до вигляду $h \cdot (a + b) = n$:

$$\begin{cases} a \cdot h \ge \gamma \\ 2^a + 1.5 \cdot b + a \le \varphi \\ h \cdot (a + b) = n \end{cases}. \qquad (10)$$

Якщо перше рівняння системи (10) представити як $h = \gamma/a$, то третє рівняння після очевидних перетворень може бути видозмінене у такий спосіб:

$$\gamma + \frac{\gamma \cdot b}{a} = n. \qquad (11)$$

Звідси значення b може бути представлене як:

$$b = \frac{n \cdot a}{\gamma} - a. \qquad (12)$$

Тоді другу нерівність із системи (10) після простих перетворень можна звести до вигляду:

$$2^a + a \cdot (1.5 \cdot \frac{n}{\gamma} + 0.5) \le \varphi. \qquad (13)$$

Оскільки співвідношення n/γ для практичних застосувань має порядок більше одиниці, останньою компонентою 0.5 можна знехтувати:

$$2^a + a \cdot \frac{1.5 \cdot n}{\gamma} \le \varphi. \qquad (14)$$

Цілком очевидно, що нерівність (14) не може бути розв'язана у явному вигляді. Відповідно максимальне ціле значення a, яке задовольняє зазначеній нерівності, може бути отримане лише шляхом підбору. Нижньою границею числа a можна вважати одиницю: $a \ge 1$, а верхня межа перебору на практиці може бути встановлена як $a < log_2\varphi$. Таким чином перебір проводиться починаючи від $a = \lfloor \log_2 \varphi \rfloor$, зі зменшенням його значення на одиницю до тих пір, поки воно не буде задовольняти нерівності (14). Після отримання числа a, визначаються значення h та b, згідно з першою нерівністю із системи (10) та формулою (12) відповідно.

Розроблена процедура визначення параметрів реалізації h, a та b може бути проілюстрована наступним прикладом. Нехай, розрядність чисел, над якими здійснюється модулярне експоненціювання, становить 4096: $n = 4096$. Виходячи із специфіки конкретного практичного застосування, рівень захищеності від спроб несанкціонованої реконструкції коду експоненти за даними, які передаються на віддалені системи, визначається об'ємом обчислень 2^{256} модулярних експонент. Тобто вартість обчислення 2^{256} модулярних експонент над числами розрядністю 4096 перевищує вартісну оцінку вигоди від отримання доступу до секретного коду експоненти для конкретного застосування. Звідси значення $\gamma = 256$. Окрім цього, виходячи з характеристик технічних засобів реалізації, параметр φ задається як $\varphi = 100$. В рамках першого етапу здійснюється підбір відповідного цим параметрам та умові (14) значення a. Згідно з описаним вище, підбір числа a виконується шляхом поступового його зменшення на одиницю, починаючи від $\lfloor \log_2 100 \rfloor = 6$. При значенні $a = 6$, ліва частина нерівності (14) дорівнює $2^6 + 6 \cdot 1.5 \cdot 4096/256 = 208$, що перевищує задане значення параметру $\varphi = 100$. Відповідно, здійснюється перевірка меншого на одиницю цілого значення $a = 5$: $2^5 + 5 \cdot 1.5 \cdot 4096/256 = 152$. Аналогічний результат для $a = 4$ складає 112, тоді як для $a = 3$ він дорівнює 80. Отже значення $a = 3$ є максимальним цілим числом, при якому дотримується нерівність (14). Наступним етапом є обчислення значень h та b, за умови що a дорівнює 3. Із формули (12) число b визначається як $b = 4096 \cdot 3/256 - 3 = 45$, а згідно з третім рівнянням системи (10) число h розраховується як $h = 4096/(3+45) \approx 85$.

Час T_{me} здійснення модулярного експоненціювання за запропонованим методом повністю визначається часом T_{mc} роботи мікроконтролера, тому можна вважати, що $T_{me} = T_{mc}$. В рамках розробленого підходу, час виконання розрахунків на мікроконтролері визначається такими складовими: часом одного модулярного множення для шифрування компоненти A, часом отримання першої множини результатів з віддаленої системи, який дорівнює тривалості одного модулярного множення, а також часом проведення h модулярних множень. Таким чином час T_{me} модулярного експоненціювання обчислюється як:

$$T_{me} = T_{mc} = (h + 2) \cdot t_{mm}. \qquad (15)$$

Значення t_{mm} виконання модулярного множення на мікроконтролері може бути

отримане із співвідношення $\varphi = t_{mm}/t_{mc}$, тобто для $t_{mc} = 0.05$ мс та значення $\varphi = 100$, час t_{mm} дорівнює $t_{mm} = 0.05 \cdot 100 = 5$ мс. Відповідно, час здійснення всіх обчислень за запропонованим методом в рамках прикладу вище складає $T_{me} = T_{mc} = (85 + 2) \cdot 5 = 435$ мс.

Важливою складової оцінки ефективності виступає порівняльний аналіз часових характеристик запропонованого методу з аналогічними відомими показниками при забезпеченні однакового рівня захищеності. Такий аналіз доцільно проводити на основі двох показників:

- коефіцієнту α_1, який характеризує часову ефективність залучення зовнішніх обчислювальних потужностей для прискорення модулярного експоненціювання;
- коефіцієнту α_2, який характеризує часову ефективність розробленого методу по відношенню до аналогічних відомих рішень.

Коефіцієнт α_1 визначається співвідношенням часу обчислень експоненти повністю на термінальній платформі до аналогічного показника в рамках використання віддалених потужностей за запропонованим методом. Час реалізації модулярного експоненціювання за алгоритмом з молодших розрядів повністю на термінальному мікроконтролері визначається часом виконання $1{,}5 \cdot n$ модулярних множень. Це зумовлено тим, що на кожному біті n-розрядної експоненти передбачається здійснення одного модулярного піднесення до квадрату, а також з ймовірністю 0,5 одного модулярного множення. Звідси перший показник розраховується наступним чином:

$$\alpha_1 = \frac{(1.5 \cdot n) \cdot t_{mm}}{h \cdot t_{mm} + 2 \cdot t_{mm}} = \frac{1.5 \cdot n}{h+2}. \qquad (16)$$

Тоді, в рамках типового для практики прикладу, розглянутого вище, шляхом підстановки значень n=4096 та h = 85, отримується коефіцієнт $\alpha_1 = 1.5 \cdot 4096/87 \approx 71$. Тобто, застосування запропонованого методу із залученням хмарних систем дозволяє прискорити обчислення модулярної експоненти у 71 раз.

Проведені експериментальні дослідження показали, що реальне прискорення, яке досягається в рамках використання запропонованого методу, у порівнянні з реалізацією обчислень повністю на термінальній платформі, складає 67 разів. Таке значення в цілому близьке до вищенаведеної теоретичної оцінки.

Другий показник α_2 визначається співвідношенням часу проведення операції модулярного експоненціювання у відомих рішеннях із залученням віддалених комп'ютерних систем до аналогічного показника при реалізації обчислень за запропонованим методом. Для отримання формули обчислення α_2, доцільно обрати один з найефективніших відомих підходів, в якому передбачається розподіл обчислень між термінальною платформою та віддаленими потужностями. Одним із таких методів, існуючих на сьогоднішній день, вважається [7], розглянутий вище, який базується на мультиплікативно-адитивному розкладенні коду експоненти. У цьому рішенні в оціночному плані об'єм обчислень визначається як $1.5 \cdot \delta + k + 2$, де δ – кількість розрядів експоненти, які повністю оброблюються на мікроконтролері, а k – кількість сегментів на які поділяється експонента. Відповідно показник α_2 для запропонованого методу визначається як:

$$\alpha_2 = \frac{(1.5 \cdot \eta + k + 2) \cdot t_{mm}}{h \cdot t_{mm} + 2 \cdot t_{mm}} = \frac{1.5 \cdot \eta + k}{h+2}. \qquad (17)$$

За умови, що об'єм перебору, який потрібно здійснити для відновлення секретного коду експоненти, становить 2^{256}, коефіцієнти δ та k у рішенні [7] дорівнюють 128 та 54 відповідно. Тоді при розрядності експоненти n = 4096 та обчисленому вище значенні h = 85, коефіцієнт α_2 складає $(1.5 \cdot 128 + 54)/85 \approx 3$. Таким чином запропонований метод дозволяє прискорити реалізацію модулярного експоненціювання у 3 рази, порівняно з відомими підходами. Ефект прискорення досягається за рахунок такої організації розподілу обчислень, яка дозволяє скоротити критичний шлях обчислювального процесу, за рахунок зменшення навантаження на малопотужний термінальний мікроконтролер зі

збільшенням при цьому об'єму обчислень на віддалених потужностях.

Висновки

В результаті проведення досліджень, направлених на підвищення ефективності комп'ютерної реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання на термінальних пристроях *IoT* з захищеним залученням хмарних обчислень отримані наступні результати.

Теоретично показано, що підвищення швидкості модулярного експоненціювання, як складової ефективності, може бути досягнуто за рахунок зменшення обчислювального навантаження на термінальний мікроконтролер.

Запропоновано метод розподіленого модулярного експоненціювання на термінальних мікроконтролерах *IoT* з захищеним залученням віддалених комп'ютерних систем, який відрізняється тим, що послідовності операцій модулярного множення, що співвідносяться з розрядами коду експоненти, які оброблюються на термінальному мікроконтролері заміняється вибором із всіх можливих результатів, обчислених на віддаленій системі, за рахунок чого зменшується обчислювальне навантаження на нього і, відповідно, досягається прискорення розподіленого обчислення модулярної експоненти.

Запропоновано математичну модель розробленої організації розподілених обчислень, яка дозволяє оптимізувати вибір її параметрів.

Теоретично доведено і експериментально підтверджено, що запропонований метод дозволяє в 3-4 рази прискорити реалізацію базової операції криптографії з відкритим ключем в порівнянні з відомими методами її реалізації на термінальних пристроях *IoT* з залученням хмарних обчислень.

Література

1. Kumar S., Tiwari P., Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data*. 2019. No. 6. P.63–71.

2. Русанова О. В., Гайдукевич М. А., Міратаеї А. Метод безпечного розподіленого обчислення модулярної експоненти для прискорення реалізації механізмів захисту даних в IoT. *Проблеми автоматизації та управління*. 2023. Т. 4, № 76. С. 74–87.

3. Markovskyi O. et al. Secure Modular Exponentiation in Cloud Systems. *The Congress on Information Technology, Computational and Experimental Physics (CITCEP 2015) :* proceedings, 18–20 December 2015, Krakow, Poland / P. 266–269.

4. Menezes A. et al. Handbook of Applied Cryptography. Boca Raton : CRC Press, 2001. 780 p.

5. Bardis N. Secure, Green Implementation of Modular Arithmetic Operations for IoT and Cloud Applications. *Green IT Engineering: Components, Networks and System Implementation* / ed. by V. Kharchenko, Y. Kondratenko, J. Kacprzyk. Cham, 2017. P. 43–64.

6. Bardis N., Markovskyi O. Secure Implementation of Modular Exponentiation on Cloud Computing Resources. *International Conference Applied Mathematics, Computational Science and Systems Engineering (AMCSE 2017) :* proceedings, 06–08 October 2017, Athens, Greece / P. 90–96.

7. Borges J. et al. A Secure Cloud Computing Method for Rapid Implementation of Cryptographic Data Protection in IoT. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* : proceedings, Athens, Greece, 13–15 October 2023 / IEEE. 2023. P. 50–53.

8. Unal D., Ali-Ali A., Catak F. O. A secure and efficient Internet of Things cloud encryption scheme with forensics investigation compatibility based on identity-based encryption. *Future Generation Computer Systems*. 2021. V. 125. P. 433–445.

9. Jialing Chen, Jiancheng Wang. The impact of broadband speed on innovation: City-level evidence from China. *Heliyon*. 2023. Vol. 9, no. 1. e12692.

Русанова О.В., Гайдукевич М.А.

МЕТОД РОЗПОДІЛЕНОГО МОДУЛЯРНОГО ЕКСПОНЕНЦІЮВАННЯ НА ТЕРМІНАЛЬНИХ МІКРОКОНТРОЛЕРАХ IoT ІЗ ЗАХИЩЕНИМ ЗАЛУЧЕННЯМ ХМАРНИХ ОБЧИСЛЕНЬ

Теоретично обґрунтовано, розроблено та досліджено метод розподіленого модулярного експоненціювання на термінальних мікроконтролерах IoT з захищеним залученням віддалених комп'ютерних систем, використання якого дозволяє прискорити реалізацію цю базову операцію криптографії з відкритим ключем.

Прискорення досягається за рахунок зменшення обчислювального навантаження на термінальну обчислювальну платформу. В роботі теоретично обґрунтована така можливість шляхом збільшення навантаження на хмарні обчислення, наведено детальний опис методу, робота якого ілюстрована числовим прикладом, представлена розгорнута оцінка ефективності.

Теоретично та експериментально показано. що запропонований метод дозволяє в 3-4 рази прискорити модулярне експоненціювання в порівнянні з відомими методами її реалізації на термінальних пристроях IoT з залученням хмарних обчислень.

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

Rusanova O.V., Haidukevych M.A.

METHOD OF DISTRIBUTED MODULAR EXPONENTIATION ON IoT TERMINAL MICROCONTROLLERS WITH PROTECTED INVOLVEMENT OF CLOUD COMPUTING

The method of distributed modular exponentiation on IoT terminal microcontrollers with secure involvement of remote computer systems is theoretically justified, developed and researched, the use of which allows to accelerate the implementation of this basic operation of public key cryptography.

Acceleration is achieved by reducing the computing load on the terminal computing platform. The paper theoretically substantiates this possibility by increasing the load on cloud computing, provides a detailed description of the method, the work of which is illustrated by a numerical example, and presents a detailed assessment of efficiency.

Theoretically and experimentally shown. that the proposed method allows to speed up modular exponentiation by 3-4 times compared to known methods of its implementation on IoT terminal devices with the involvement of cloud computing.

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