УДК 004.052.42

DOI: 10.18372/2073-4751.76.18243

Русанова О.В., к.т.н.,
orcid.org/0000-0003-0145-3012,
Гайдукевич М.А.,
orcid.org/0000-0003-2334-2401,
Міратаеї Аліреза,
orcid.org/0000-0002-4732-7030

МЕТОД БЕЗПЕЧНОГО РОЗПОДІЛЕНОГО ОБЧИСЛЕННЯ МОДУЛЯРНОЇ ЕКСПОНЕНТИ ДЛЯ ПРИСКОРЕННЯ РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ЗАХИСТУ ДАНИХ В IoT

**Національний технічний університет України
“Київський політехнічний інститут імені Ігоря Сікорського”**

mgrnchnk@gmail.com,
alirezaataei@gmail.com

Вступ

Динамічний прогрес технологій Інтернету Речей (*Internet of Things – IoT*) стимулює їх впровадження в широкий спектр систем віддаленого моніторингу та керування об’єктами реального світу [1]. Це зумовлено перевагами зазначених технологій: низькою вартістю побудови складних систем на їхній основі, простотою конфігурування та гнучкістю реконфігурування [2]. Разом з тим, використання Інтернету як потенційно вразливого середовища обміну даними створює загрози інформаційній безпеці. Проведений аналіз показав, що найбільші загрози становлять спроби підробки даних про стан об’єктів, які надсилаються з термінальних мікроконтролерів, а також команд систем керування ними, тобто атаки на ідентичність та автентичність повідомлень [3].

Для запобігання атакам цього типу переважно використовуються механізми цифрового підпису [4]. Такі механізми, зокрема *DSA*, базуються на реалізації операції модулярного експоненціювання. З метою забезпечення належного рівня захисту, обчислення цієї операції проводиться над числами великої розрядності. На сьогоднішній день ця розрядність становить 2048, з перспективою зростання до 4096 в найближчі роки [5]. Здійснення операції модулярного експоненціювання з 2048-розрядними операндами на 32-розрядному термінальному мікроконтролері вимагає близько 6 мільйонів процесорних операцій [5]. Для портативних малопотужних мікроконтролерів виконання таких складних обчислень вимагає значних часових ресурсів, що протирічить концепції управління в режимі реального часу.

Одним з перспективних варіантів вирішення цієї задачі є залучення віддалених комп’ютерних потужностей, обладнаних криптопроцесорами, що дозволяє зменшити навантаження на термінальні мікроконтролери. При цьому необхідно забезпечити такий розподіл обчислень між віддаленими системами та мікроконтролером, при якому за даними, що надсилаються на хмарні системи, відновлення секретних компонентів операції модулярного експоненціювання є практично неможливим.

Таким чином наукова задача ефективного розподілу обчислень між термінальною та віддаленими платформами при модулярному експоненціюванні з унеможливленням реконструкції коду експоненти на віддалених комп’ютерних системах забезпеченням захисту є актуальною з огляду на сучасний стан розвитку інформаційних технологій.

Аналітичний огляд відомих підходів до організації розподілених обчислень модулярної експоненти

Здійснення операції модулярного експоненціювання $A^E \bmod M$ на термінальному мікроконтролері з використанням

хмарних технологій має бути організоване таким чином, щоб практично унеможливити відновлення секретних компонентів A і E за даними, що передаються на віддалену комп'ютерну систему, а також прискорити обчислення для реалізації цифрового підпису в режимі реального часу [6]. Відповідно, базовими критеріями для визначення ефективності обчислення модулярної експоненти на термінальному мікроконтролері із залученням хмарних технологій виступають:

- рівень захищеності операндів A та E від спроб їх несанкціонованої реконструкції на хмарній системі;
- прискорення виконання модулярного експоненціювання завдяки використанню можливостей віддалених обчислювальних потужностей.

Здійснення операції модулярного експоненціювання відбувається за одним з двох алгоритмів [7]. Обидва з них полягають у виконанні n-ітераційного циклу, причому, на кожній ітерації здійснюються операції, які залежать від значення поточного двійкового розряду коду експоненти. Алгоритми відрізняються порядком, в якому здійснюється обробка коду експоненти: перший проводить аналіз, починаючи зі старших розрядів, натомість другий передбачає модулярне експоненціювання починаючи з молодших розрядів коду експоненти. Алгоритм модулярного експоненціювання зі старших розрядів полягає у реалізації n-ітераційного циклу модифікацій змінної R, початкове значення якої дорівнює одиниці. Під час кожної ітерації передбачається послідовне виконання операцій модулярного піднесення числа R до квадрату та модулярного множення R на постійне число A. При цьому обчислення останньої операції – модулярного добутку – здійснюється на тих ітераціях циклу, на яких значення поточного розряду двійкового коду експоненти дорівнює одиниці. Кінцевий результат обчислень формується в змінній R: $R = A^E \bmod M$, отримане на останній ітерації циклу. Очевидно, що цей алгоритм має строго послідовну структуру, тобто під час його реалізації послідовно здійснюється модифікація однієї змінної. Це не дозволяє організувати його паралельну реалізацію. Суть алгоритму з молодших розрядів полягає у виконанні n ітерацій циклу модифікацій двох змінних D та R, значення яких на початку алгоритму дорівнюють A та одиниці відповідно. На кожній ітерації передбачено виконання двох операцій: модулярного множення $D{\cdot}R \bmod M$, із збереженням результату у змінну R, та модулярного піднесення до квадрату $D = D^2 \bmod M$, із записом результату у змінну D. Модифікація значення R здійснюється у випадку, коли поточний біт коду експоненти рівний одиниці, в той час як обчислення модулярного піднесення до квадрату реалізується на кожній ітерації циклу незалежно від значення поточного розряду коду експоненти. Кінцевим результатом модулярного експоненціювання є значення модулярного добутку, записане на останній ітерації циклу в змінну R. Цілком очевидно, що описаний алгоритм модулярного експоненціювання дозволяє організувати одночасну реалізацію модулярного множення $D{\cdot}R \bmod M$ та модулярного піднесення до квадрату $D^2 \bmod M$. Тобто ступінь паралелізму алгоритму модулярного експоненціювання з молодших розрядів дорівнює двом.

Потреба в реалізації швидкого обчислення модулярної експоненти як основної операції цифрового підпису в *IoT* стимулювала створення низки методів розподілення обчислень між термінальним мікроконтролером та хмарою. Всі існуючі підходи можна розділити на два класи: ті, в яких обмін даними між мікроконтролером та хмарою здійснюється лише на початку та в кінці обчислень [8] і ті, в яких наявний обмін проміжними результатами [9]. В основу більшості відомих методів покладено принцип адитивного чи мультиплікативно-адитивного розкладення коду експоненти. При такій організації частина розрядів коду експоненти оброблюється на термінальній платформі, а решта – на віддалених. Рівень захищеності обчислень залежить від кількості розрядів коду

експоненти, які оброблюються на термінальному мікроконтролері, тому швидкість реалізації модулярного експоненціювання принципово обмежена кількістю цих розрядів, яка, в свою чергу, визначається заданим рівнем захисту. Відповідно, єдина можливість підвищення часової ефективності залучення хмарних систем полягає у прискоренні обробки тих розрядів коду експоненти, які визначають рівень криптографічного захисту. Мета досліджень полягає у підвищенні ефективності обчислення модулярної експоненти з залученням хмарних технологій за рахунок прискорення обробки частини розрядів коду експоненти на термінальних платформах *IoT*.

Організація розподілених обчислень модулярної експоненти за принципом нульової секретності

Для досягнення поставленої мети пропонується метод швидкого захищеного обчислення модулярної експоненти $A^E \bmod M$ на термінальному мікроконтролері з організацією двох віддалених обчислювальних процесів.

Згідно з викладеним вище, чисельними компонентами модулярного експоненціювання $A^E \bmod M$ виступають: інформаційна складова A, закритий ключ E та значення модуля M, який є частиною відкритого ключа. Цілком очевидно, що обробка ключа E на віддалених непідконтрольних комп'ютерних системах вимагає значно вищого рівня захищеності, ніж значення A. Це пов'язано з тим, що закритий ключ E використовується багатократно протягом тривалого часу, тобто отримання до нього доступу надає можливості для його подальшого несанкціонованого використання з метою підробки даних. Натомість інформаційна компонента A змінюється в кожному сеансі шифрування даних. Крім того, для багатьох застосувань інформаційна компонента A використовується у відкритому вигляді, зокрема в механізмах цифрового підпису пакетів даних з термінальних мікроконтролерів.

Ефективність реалізації модулярного експоненціювання з залученням хмарних технологій визначається двома чинниками: прискоренням обчислення модулярної експоненти на термінальному мікроконтролері за рахунок залучення віддалених обчислювальних потужностей та рівнем захищеності від несанкціонованого відновлення секретного ключа за даними, що надаються на віддалену комп'ютерну систему. Значний ефект в контексті прискорення обчислення модулярної експоненти із залученням віддалених комп'ютерних систем може бути досягнений за рахунок:

- найбільшого суміщення в часі обчислювальних процесів на віддалених комп'ютерних системах та термінальному мікроконтролері;
- ефективного використання можливостей організації декількох паралельних процесів на віддаленій комп'ютерній системі.

Проведений аналіз показав, що рівень захищеності обчислень модулярної експоненти з використанням можливостей віддалених обчислювальних процесів визначається кількістю розрядів секретного коду експоненти, обробка яких здійснюється на термінальному мікроконтролері. Іншими словами, для підвищення рівня захищеності потрібно, щоб якомога більше розрядів секретного коду експоненти не надсилалися в хмару, а оброблювалися на термінальній обчислювальній платформі. При цьому вказана кількість розрядів обмежена низькою продуктивністю термінального мікроконтролера.

Один із можливих варіантів ефективного вирішення проблеми підвищення рівня захищеності за рахунок збільшення кількості розрядів коду експоненти, що оброблюються на термінальному мікроконтролері, без втрати швидкодії, полягає в зменшенні на нього обчислювального навантаження. Це може бути досягнуто шляхом розділення обчислювального процесу на дві частини, одна з яких, безпосередньо пов'язана з секретними розрядами коду експоненти, оброблюється на термінальній обчислювальній платформі, а інша – на віддалених комп'ютерних платформах. У відомих рішеннях такий розподіл

обчислювального процесу модулярного експоненціювання реалізується лише на рівні ітерацій. Це означає, що частина із n ітерацій виконується на термінальній обчислювальній платформі, а інша – на віддалених потужностях. Зокрема, найчастіше на практиці використовується варіант, за яким d молодших розрядів коду експоненти оброблюються на термінальному мікроконтролері, а n-d старших – в хмарі. Значення d вибирається при цьому таким чином, щоб досягти найбільшого суміщення в часі роботи термінальних та віддалених платформ і забезпечити при цьому рівень захищеності, визначений специфікою застосування системи віддаленого управління на базі технології Інтернету речей. Якщо позначити через g кількість розрядів коду експоненти, інформація про які в тій чи іншій формі не передається на віддалені обчислювальні потужності, яка визначається потрібним для конкретного застосування рівнем захищеності, то $d \geq g$. При цьому, якщо час обробки g розрядів коду експоненти на термінальній платформі виявиться меншим за час опрацювання n-g старших в хмарі, то значення d збільшується, щоб урівняти час роботи термінальної та віддалених платформ. Якщо час обробки g розрядів коду експоненти на термінальній платформі більшим за час обчислення модулярної експоненти від n-g старших розрядів в хмарі, то суміщення в часі роботи термінальної та віддалених комп'ютерних платформ не може бути досягнуте.

У відомих методах розділення обчислювального процесу між віддаленими потужностями та термінальним мікроконтролером обробка кожного біту коду експоненти передбачає реалізацію на останньому обох операцій, що регламентовані в кожній із n ітерацій алгоритмами модулярного експоненціювання.

Базова ідея, покладена в основу пропонованого методу полягає в тому, щоб розділення обчислювального процесу на дві частини здійснювалося не тільки на рівні окремих ітерацій, а й на рівні операцій, що виконуються в рамках однієї ітерації. Для реалізації такого підходу принциповим є використання алгоритму обчислення модулярної експоненти з молодших розрядів, оскільки лише цей різновид алгоритму модулярного експоненціювання передбачає виконання в рамках кожної ітерації двох незалежних операцій: модулярного множення $R \cdot D \bmod M$ та модулярного піднесення до квадрату $D^2 \bmod M$. Згідно з цим алгоритмом, операція модулярного множення реалізується за умови, що поточний розряд коду експоненти рівний одиниці. Таким чином, факт здійснення модулярного множення на ітераціях алгоритму надає інформацію щодо значень двійкового коду секретної експоненти. Тому, з двох операцій, які виконуються в межах однієї ітерації експоненціювання з молодших розрядів, саме модулярне множення $R \cdot D \bmod M$ має здійснюватися на термінальній обчислювальній платформі. Натомість операцію модулярного піднесення до квадрату $D^2 \bmod M$, яка незалежна від секретного коду експоненти, доцільно реалізувати на віддалених обчислювальних платформах.

В рамках повномасштабної реалізації ідеї розділення обчислень модулярного експоненціювання між віддаленою та термінальною комп'ютерними платформами на рівні вказаних двох операцій, що виконуються в рамках однієї ітерації, весь процес обробки секретного коду експоненти здійснюється на термінальний платформі. При цьому фактично формуються два паралельні обчислювальні процеси: перший, на термінальній платформі, для обчислення ланцюжка модулярних множень з використанням значень розрядів коду експоненти та другий, на віддаленій комп'ютерній системі, для здійснення незалежного від коду експоненти обчислень ланцюжка модулярних піднесень до квадрату. В інформаційному плані перший процес залежить від другого: для виконання модулярного добутку в кожній i-тій ітерації на термінальному мікроконтролері, $i \in \{1,2,\ldots,n\text{-}1\}$ потрібно видавати значення $D_{i\text{-}1}$ результату (i-1)-ї ітерації другого процесу.

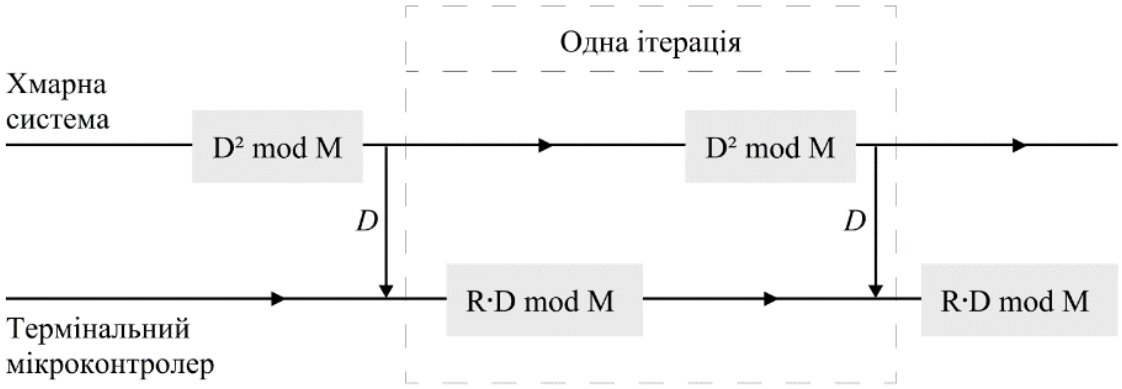

Рис. 1. Схематичне представлення розподілу обчислень на рівні ітерації

Варто зазначити, що обчислювальна потужність віддаленої комп'ютерної системи значно перевищує можливості термінального мікроконтролера, тому, при такому підході, тривалість процесу обчислення ряду значень D є в рази меншою за тривалість процесу обчислення ряду значень R. Водночас, завдяки незалежності згаданих процесів в рамках кожної ітерації, відсутня потреба синхронності виконання ітерацій на термінальному мікроконтролері та віддаленій хмарній системі. Окрім того, оскільки в якості середовища обміну даними у розглянутому підході використовується Інтернет, пересилку послідовності значень D з віддаленої системи на термінальний мікроконтролер недоцільно здійснювати на кожній ітерації. Це пояснюється особливостями функціонування Інтернету: формування стандартного пакету даних вимагає значно більше часових ресурсів, ніж разове здійснення модулярного піднесення до квадрату. Таким чином, раціональним рішенням є організувати разову передачі цілого набору значень D. Застосування вищерозглянутого підходу забезпечує абсолютний рівень захищеності, оскільки всі обчислення, пов'язані з обробкою секретного коду експоненти, здійснюються на термінальному мікроконтролері.

Ефективність обчислень модулярної експоненти із залученням віддалених комп'ютерних систем визначається коефіцієнтом прискорення β, який є співвідношенням часу T_0 повного обчислення модулярної експоненти на термінальному мікроконтролері до часу виконання модулярного експоненціювання із залученням можливостей віддалених комп'ютерних систем. Якщо позначити час виконання модулярного експоненціювання з використанням одного віддаленого обчислювального процесу в рамках описаної організації обчислень як T_1, то коефіцієнт прискорення β може бути представлений у вигляді:

$$\beta = \frac{T_0}{T_1}. \qquad (1)$$

Час T_0 реалізації модулярного експоненціювання на термінальному мікроконтролері визначається середньою кількістю $1.5 \cdot n$ операцій модулярного множення n–розрядних чисел для виконання алгоритму. Тобто $T_0 = 1.5 \cdot n \cdot t_m$, де t_m – час виконання модулярного множення n-розрядних чисел на m-розрядному термінальному мікроконтролері. На практиці $n>>m$.

Оскільки розглянутий підхід базується на залученні до обчислень віддаленої комп'ютерної системи, то час T_1 визначається максимальним значенням з часу T_{T1} виконання обчислень на термінальному мікроконтролері та часу T_{X1} виконання обчислень на хмарній системі: $T_1 = max(T_{T1}, T_{X1})$.

Зважаючи на те, що швидкодія потужної віддаленої комп'ютерної системи на порядки вища за аналогічний показник малопотужного мікроконтролера, то $max(T_{T1}, T_{X1}) = T_{T1}$, тобто $T_1 = T_{T1}$. Час T_{T1}, який потрібен термінальному мікроконтролеру для здійснення обчислень, за описаним підходом фактично визначається кількістю $0.5 \cdot n$ модулярних множень, оскільки ця операція виконується на мікроконтролері протягом n ітерацій з ймовірністю 0.5 на кожній із них. Тому $T_1 = T_{T1} = 0.5 \cdot n \cdot t_m$. Відповідно, коефіцієнт β прискорення обчислень при використанні розглянутого методу визначається як:

$$\beta = \frac{1.5 \cdot n \cdot t_m}{0.5 \cdot n \cdot t_m} = 3 \quad . \qquad (2)$$

Таким чином доведено, що розглянута організація захищеного обчислення модулярної експоненти з залученням віддалених комп'ютерних систем дозволяє втричі прискорити реалізацію цієї операції в порівнянні з використанням лише термінальної обчислювальної платформи. Разом з тим, з огляду на сучасні вимоги до систем керування об'єктами реального світу, такий рівень прискорення реалізації модулярного експоненціювання, в порівнянні з відомими рішеннями, не є достатнім.

Тому, для забезпечення потрібного, з точки зору сучасних вимог до систем керування, рівня швидкості реалізації протоколів цифрового підпису пропонується використання комбінованого способу розділення обчислень між термінальним мікроконтролером та віддаленими комп'ютерними системами. Такий спосіб передбачає розділення обчислень як на рівні ітерацій, так і всередині однієї ітерації за описаною вище схемою. Для цього пропонується на віддалених комп'ютерних системах організувати два паралельних обчислювальних процеси: один для здійснення обрахунку всіх значень D модулярного піднесення до квадрату, а другий для безпосереднього виконання модулярного експоненціювання з використанням частини секретного коду експоненти. Одночасно з цим на термінальному мікроконтролері пропонується обчислювати послідовність значень R модулярного множення для тих розрядів коду експоненти, які не задіяні в обчисленнях на другому віддаленому обчислювальному процесі. Співвідношення кількості розрядів коду експоненти для обробки на мікроконтролері та віддаленій комп'ютерній системі визначається виходячи з потрібного для конкретного застосування рівня захищеності. Такий підхід дозволяє, в порівнянні з існуючими рішеннями, значно збільшити кількість оброблюваних на термінальній обчислювальній платформі розрядів секретного коду експоненти без втрати при цьому швидкодії.

Відповідно, запропонований метод базується на новому підході до ефективного розподілу обчислень між термінальним мікроконтролером та віддаленими комп'ютерними системами, що дозволяє збільшити кількість розрядів експоненти для обробки на мікроконтролері зі збереженням належного рівня швидкодії.

Запропонований метод передбачає представлення секретного n-розрядного коду експоненти у вигляді:

$$E = 2 \cdot (H + S + L) + 1, \qquad (3)$$

де L це h-розрядний код $q=2^{h-2} \cdot e_{h-2} + 2^{h-3} \cdot e_{h-2} + \ldots + 2 \cdot e_2 + e_1$. Старші b розрядів коду середньої складової S співпадають з однойменними розрядами зсунутого праворуч коду експоненти, а h молодші розряди дорівнюють нулю. Формально код S може бути представлений у вигляді: $S=2^{h+b-2} \cdot e_{h+b-2} + 2^{h+b-2} \cdot e_{h-+b-2} + \ldots + 2^{h+1} \cdot e_{h+1} + 2^{h-1} \cdot e_{h-1}$. Код старшої компоненти адитивного розкладення H, в свою чергу, складається з $a=n-b-h-1$ старших розрядів зсунутого праворуч коду експоненти E та $b+h$ нульових розрядів, і визначається як $H=2^{n-2} \cdot e_{n-2} + 2^{n-3} \cdot e_{n-3} + .. + 2^{n-a} \cdot e_{n-a} + 2^{n-a-1} \cdot e_{n-a-1}$.

Значення a, b та h, сума яких дорівнює $n-1$: $a + b + h = n-1$, визначається наступним чином. Виходячи з вимог до рівня захищеності для конкретного застосування визначається значення g кількості розрядів коду експоненти, які мають

залишатися секретними і не передаватися на віддалені комп'ютерні системи. В силу цього, розряди a та h, які оброблюються на мікроконтролері, мають в сумі бути не менше значення g. Тобто, з точки зору інформаційної безпеки, вибір значень a та h має задовольняти такій умові:

$$a + h \geq g \,. \qquad (4)$$

З огляду на необхідність досягнення найбільшого прискорення обчислень модулярної експоненти, співвідношення a, b та h мають забезпечити ефективну паралельну роботу всіх трьох обчислювальних платформ: термінального мікроконтролера та двох віддалених обчислювальних процесів. Базовою обчислювальною операцією, яка реалізується в усіх зазначених процесах виступає модулярне множення n-розрядних чисел. Для подальшого аналізу, час здійснення цієї операції на термінальній платформі позначено як t_m, а на віддалених системах через t'_m. Дієвим чинником при визначенні часу реалізації рознесеного модулярного експоненціювання є t_T – час формування і передачі пакету даних обміну між обчислювальними платформами через Інтернет.

Схематично, послідовність виконання трьох обчислювальних процесів: термінальнім (ТП) и першим (ВП1) та другим (ВП2) віддаленими процесами з урахуванням їх часових характеристик показана на рис.2.

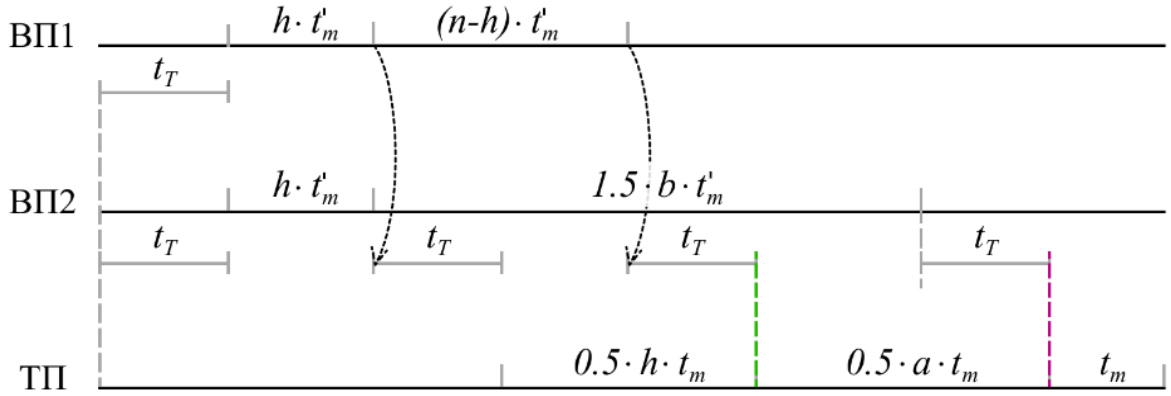

Рис. 2. Послідовність виконання трьох обчислювальних процесів

Цілком зрозуміло, що для за безпечення вимог щодо рівня захищеності, необхідно щоб термінальний мікроконтролер обробляв не менше g розрядів, відповідно найбільш доцільною представляється така організація обчислень, при якій забезпечується безперервна робота термінального мікроконтролера.

При виконанні цієї умови час T_{TP} роботи термінального мікроконтролера складається з таких складових: очікування часу $h \cdot t_m'$ обчислення h перших значень $D_1, D_2, \ldots, D_h$ першим віддаленим обчислювальним процесом, очікування часу (t_T) передачі цих даних з хмари та часу $0.5 \cdot g \cdot t_m$ обробки мінімум g розрядів коду експоненти. Тобто значення мінімального часу T_{TP} роботи термінального мікроконтролера визначається наступною формулою:

$$T_{TP} = h \cdot t_m' + t_T + 0.5 \cdot g \cdot t_m \,. \qquad (5)$$

Оскількі значення всіх, крім h, параметрів, що входять в формулу (5) фіксовані, то очевидно, що мімімальне значення часу T_{TP} роботи термінального мікроконтролера досягається при мінімальному значенні h. З іншого боку, нижня границя значення h для забезпечення безперервної роботи термінального мікроконтролера визначається із умови того, що час $(n\text{-}h\text{-}1) \cdot t'_m$ обчислення першим віддаленим обчислювальнім процесом всіх $n\text{-}h\text{-}1$ значень $D_{h+1}, D_{h+2}, \ldots, D_{n-h-1}$ має бути меншим за час $0.5 \cdot h \cdot t_m$ обробки h розрядів коду експоненти на термінальному мікроконтролері:

$$(n - h - 1) \cdot t_m' \leq 0.5 \cdot h \cdot t_m \,. \qquad (6)$$

Якщо позначити через γ співвідношення t_m до t'_m: $\gamma = t_m/t'_m$ то перше рівняння із системи (6) можна представити у вигляді:

$$n-1 \le h \cdot (0.5 \cdot \gamma + 1). \quad (7)$$

Враховуючи, що швидкодія віддалених потужних комп'ютерних систем на порядки вища ніж термінальних мікроконтролерів, а чисельне значення n складає для сучасних систем криптографічного захисту вимірюється тисячами, значення об'єму h першої групи розрядів коду експоненти, що оброблюється на термінальному мікроконтролері може бути визначена як:

$$h \ge \frac{2 \cdot n}{\gamma}. \quad (8)$$

Оскільки загальна кількість розрядів, що оброблюються на термінальному мікроконтролері має бути не меншою за g, то чисельне значення кількості a старших розрядів коду експоненти, які оброблюються на термінальному мікроконтролері визначається формулою:

$$a \ge g - h = g - \frac{2 \cdot n}{\gamma} \quad (9)$$

З урахуванням значення h з формули (8) формула мінімального часу T_{TP} роботи термінального мікроконтролера трансформується до вигляду:

$$T_{TP} = \frac{2 \cdot n}{\gamma} \cdot t_m' + t_T + 0.5 \cdot g \cdot t_m. \quad (10)$$

Час T_2 функціонування другого віддаленого обчислювального процесу по обробці середньої компоненти M розкладення коду експоненти визначається формулою:

$$T_2 = h \cdot t_m' + 1.5 \cdot b \cdot t_m' = h \cdot t_m' + 1.5 \cdot (n-a-h) \cdot t_m' = t_m' \cdot (1.5 \cdot n - 1.5 \cdot a - \frac{2 \cdot n}{\gamma}) =$$

$$= t_m' \cdot (n \cdot (1.5 - \frac{2}{\gamma}) - 1.5 \cdot a) \approx 1.5 \cdot t_m' \cdot (n-a) \quad (11)$$

Якщо $T_{TP} \le T_2$, то загальний час обчислення модулярної експоненти з організацією двох обчислювальних процесів на віддалених комп'ютерних системах за запропонованим методом дорівнює T_{TP}. Якщо $T_2 > T_{TP}$, то здійснюється їх вирівнювання шляхом збільшення значення a до величини a' чисельна значення якої визначається із умови:

$$t_m' \cdot 1.5 \cdot (n-a') = \frac{2 \cdot n}{\gamma} \cdot t_m' + t_T + 0.5 \cdot (\frac{2 \cdot n}{\gamma} + a') \cdot t_m. \quad (12)$$

Викладений підхід до визначення параметрів розрядності може бути ілюстрований наступним прикладом. Нехай розрядність n чисел, над якими здійснюється експоненціювання становить 2048: n=2048. Якщо прийняти, що для конкретного застосування рівень захищеності від незаконного підбору секретного коду експоненти визначається об'ємом ресурсів, потрібним для перебору 10^{20} варіантів, то кількість g розрядів коду експоненти, що мають оброблюватися на термінальному мікроконтролері становить $63 = log_2 10^{20}$. Для 32-розрядного мікроконтролера сімейства *PIC* час t_m виконання модулярного множення 2048-розрядних чисел, в оціночному плані, становить 5 мс.: t_m = 5 мс. Ця ж операція на потужному криптопроцесорі виконується приблизно на два порядки швидше, тобто t_m'= 0.05 мс. а γ=100. Час t_T пересилки пакету даних оцінюється як 50 мс.: t_T = 50 мс. Тоді, згідно формули (8) значення $h > 2 \cdot n/\gamma = 41$. Відповідно, за формулою (9) $a > g-h = 63-41 = 22$. Обчислений за формулою (10) час T_{TP} роботи термінального мікроконтролера становить: $T_{TP} = 41 \cdot 0.05 + 50 + 0.5 \cdot 63 \cdot 5 = 210$ мс. Час T_2 виконання другого віддаленого обчислювального процесу, який обчислюється за

формулою (11) складає T_2 =1.5·0.05·(2048-22) = 152 мс. Оскільки $T_2 \le T_{TP}$, то загальний час обчислення модулярної експоненти з організацією двох обчислювальних процесів на віддалених комп'ютерних системах за запропонованим методом дорівнює T_{TP} = 210 мс.

Для виключення можливості відновлення на віддалених обчислювальних потужностях секретної інформаційної компоненти A операції модулярного експоненціювання $A^E \bmod M$ пропонується здійснювати її гомоморфне шифрування шляхом модулярного піднесення до квадрату.

У формалізованому вигляді запропонований метод обчислення $A^E \bmod M$ може бути представлений наступною послідовністю дій:

1. На термінальному мікроконтролері обчислюється значення B: $B = A^2 \bmod M$, яке надсилається разом зі значенням M на обидва віддалені обчислювальні процеси. Окрім цього, на другий віддалений процес надсилається складова S коду експоненти.

2. В рамках другого віддаленого процесу змінній D' присвоюється початкове значення B: $D'_0 = B$, стартове значення змінної R_0 встановлюється в одиницю: $R'_0 = 1$. Здійснюється послідовне обчислення значень $D'_1, \ldots, D'_{b+h-1}$, а також значень $R'_1, \ldots, R'_{b+h-1}$ на тих розрядах коду S, значення яких рівне одиниці: $\forall i \in \{1, b+h-1\} : D'_i = D'^{\,2}_{i-1} \bmod M, R'_i = R'_{i-1} \cdot (D'_{i-1})^{e_i} \bmod M$. По завершенні циклу, значення R'_{b+h-1} надсилається на термінальний мікроконтролер.

3. В рамках першого віддаленого процесу змінній D присвоюється початкове значення B: $D_0 = B$. Здійснюється послідовний підрахунок значень $D_1, \ldots, D_{h-1}$: $D_i = D^{\,2}_{i-1} \bmod M, \forall i \in \{1, h-1\}$. Отримана послідовність значень $D_1, \ldots, D_{h-1}$ накопичується та надсилається на термінальний мікроконтролер після закінчення обчислення D_{h-1}.

4. На термінальному мікроконтролері встановлюється початкове значення $R_0 = 1$ та обчислюється $R_1 = R_0 \cdot B \bmod M$. Після отримання з хмари значень $D_1, \ldots, D_{h-1}$, виконується цикл $\forall i \in \{2, h\}$, в кожній ітерації якого реалізується операція модулярного множення на тих розрядах коду експоненти, значення яких рівне одиниці: $R_i = R_{i-1} \cdot (D'_{i-1})^{e_i} \bmod M$. Результат цих обчислень R_{h-1} зберігається в змінній Q.

5. Після завершення обчислення та відправки на термінальний мікроконтролер значень $D_1, \ldots, D_{h-1}$, перший віддалений процес продовжує обчислення значень $D_h, \ldots, D_{n-1}$: . По закінченню циклу, останні a з обчислених результатів: $D_{n-a-1}, \ldots, D_{n-1}$ відправляються на термінальний мікроконтролер.

6. Після отримання значень $D_{n-a-1}, \ldots, D_{n-1}$ і завершення обчислення R_{h-1}, на термінальному мікроконтролері змінній R_{n-a-1} присвоюється значення Q. Реалізується цикл $\forall i \in \{n-a, n\}$, на кожній ітерації якого проводиться обчислення $R'_i = R'_{i-1} \cdot (D'_{i-1})^{e_i} \bmod M$. Результатом цих обчислень є значення R_a.

7. На термінальному мікроконтролері після отримання R'_{b+h-1}, здійснюється модулярне множення значень R_a та R'_{b+h-1}, результат записується в змінну R: $R = R_a \cdot R'_{b+h-1} \bmod M$.

8. Після отримання результату R, на термінальному мікроконтролері обчислюється модулярний добуток $Res = R \cdot A \bmod M$.

Робота запропонованого методу може бути ілюстрована наступним числовим прикладом. На етапі конфігурації системи, за викладеною вище методикою, визначено розрядності $a = 4$, $b = 5$ та $h = 3$ і відповідно три складові H, S, L незмінного коду експоненти E. В двійковому представленні $H = 100100000000_2$, $S = 11010000_2$, $L = 101_2$. Нехай потрібно обчислити $A^E \bmod M = 53^{5035} \bmod 2347 = 2015$, тобто A=53, E=5035, M=2347.

Згідно п.1 методу виконується гомоморфне шифрування компоненти A шляхом її піднесення до модулярного квадрату: $B = A^2 \bmod M = 53^2 \bmod 2347 = 462$ та

надсилається разом з модулем $M = 2347$ на обидва віддалені обчислювальні процеси. Крім цього, на другий віддалений процес відправляється складова $S=11010000_2=208_{10}$ коду експоненти.

Початкове значення D_0 на першому віддаленому процесі встановлюється як $D_0 = 462$. На другому віддаленому процесі початкові значення R'_0 та D'_0 дорівнюють 1 та 462 відповідно.

Числові результати покрокової реалізації модулярного експоненціювання на трьох обчислювальних процесах представлені у вигляді табл. 1. Кожна з колонок: ТП, ВП1 та ВП2, містить номер ітерації та результати, отриманий на ній.

Таблиця 1. Покрокові результати паралельних обчислень на трьох процесах в рамках числового прикладу

Обчислювальні процеси						
ТП		ВП1		ВП2		
№ ітерації	R	№ ітерації	D	№ ітерації	R'	D'
1	$R_1 = 462$	1	$D_1 = 2214$	1		$D'_1 = 2214$
2	$R_3 = 64$	2	$D_2 = 1260$	2		$D'_2 = 1260$
3	$R_9 = 1727$	3	$D_3 = 1028$	3		$D'_3 = 1028$
4	$R_{12} = 1725$	4	$D_4 = 634$	4		$D'_4 = 634$
5	**$R = 348$**	5	$D_5 = 619$	5	$R'_5 = 634$	$D'_5 = 619$
		6	$D_6 = 600$	6		$D'_6 = 600$
		7	$D_7 = 909$	7	$R'_7 = 186$	$D'_7 = 909$
		8	$D_8 = 137$	8	$R'_8 = 90$	
		9	$D_9 = 2340$			
		10	$D_{10} = 49$			
		11	$D_{11} = 54$			

Згідно п.2, на другому віддаленому процесі встановлюється значення $R'_0 = 1$ та послідовно обчислюється 462^{208} *mod* 2347. Покрокові результати представлені на ітераціях 1-8 колонки «ВП2» табл. 1. В ході обчислень на другому віддаленому процесі отримується значення R'_8: $R'_8 = B^S \bmod M = 462^{208} \bmod 2347 = 90$ та відправляється на термінальний мікроконтролер. В рамках першого віддаленого процесу згідно п.3 методу обчислюються перші h-1 значення $D_1 = 2214$, $D_2 = 1260$ модулярного піднесення до квадрату та надсилаються на термінальний мікроконтролер. Поетапні результати цих обчислень представлені на ітераціях 1-2 колонки «ВП1» табл. 1. Після отримання значень D_1, D_2, ТП здійснює модулярне множення на 3-ому розряді коду L, оскільки e_3=1. Результатом цих обчислень є значення R_3=64 наведене на ітерації 3 колонки «ТП». Відповідно до п.5 після завершення обчислення та відправки на термінальний мікроконтролер значень D_1, D_2, перший віддалений процес продовжує обчислення решти n-h значень D_3, ..., D_{11}, числові результати цих обчислень наведені на ітераціях 3-11 колонки «ВП1» табл. 1. Після завершення обчислень, на термінальний процес відправляються значення $D_8 = 137$, $D_9 = 2340$, $D_{10} = 48$, $D_{11} = 54$. Згідно п.6 на термінальному мікроконтролері з використанням отриманих з першого віддаленого процесу значень D_8, ..., D_{11}, реалізується послідовне обчислення модулярних добутків, в ході якого отримується значення $R_{12} = 1725$. Покрокові результати, визначені в ході обчислення на термінальному мікроконтролері значення R_{12}, представлені на ітераціях 3-4 колонки «ТП» табл. 1. Одночасно, відповідно до п.6, на мікроконтролері здійснюється обчислення модулярного добутку $R = R'_8 \cdot R_{12} \bmod M =$

$90 \cdot 1725 \ mod\ 2347 = 348$ (ітерація 5 колонки «ТП» таблиці 1). Для отримання кінцевого результату модулярного експоненціювання $A^E \ mod\ M = 53^{5035} \ mod\ 2347$, згідно п.8 методу, на термінальному мікроконтролері обчислюється модулярний добуток Res: $Res = R \cdot A \ mod\ M = 348 \cdot 53 \ mod\ 2347 = 2015$.

Отже, в рамках числового прикладу отримано код $Res = 2015$.

Таким чином, наведеним прикладом продемонстровано, що модулярне експоненціювання, організоване за запропонованим методом з використанням трьох обчислювальних процесів забезпечує отримання правильного результату.

Аналіз ефективності

Ефективність запропонованого методу визначається за двома базовими критеріями: рівнем захищеності та прискоренням модулярного експоненціювання за рахунок залучення віддалених обчислювальних потужностей. В розглянутому контексті рівень захищеності полягає у невразливості до спроб відновлення секретних компонентів модулярної експоненти за даними, які оброблюються на віддаленій комп'ютерній системі. Вважається, що потенційний зловмисник має доступ до обчисленого на термінальному мікроконтролері результату модулярного експоненціювання $A^E \ mod\ M$, а також до значень модуля M, зашифрованого представлення інформаційної компоненти B та підмножини реальних бітів коду експоненти, що задається кодом S. З позицій інформованості зловмисника потенційно доступне йому значення $Y=A^E \ mod\ M$ обчислюється у вигляді:

$$Y = (B^{H+S+L} \bmod M \cdot A) \bmod M, \quad (13)$$

де невідомими для зловмисника компонентами виступають код H, що містить a значущих двійкових розрядів, h-розрядний код L, а також n-розрядний код A, про який відомо, що $A^2 \ mod\ M=B$. Цілком очевидно, що якщо сторона, що здійснює злам захисту не знає коду A, задача підбору кодів H, L та A, сумарна кількість значущих розрядів яких становить $a+h+n$, виходить за рамки технічних можливостей. Проте, якщо стороні, що здійснює злам, певним чином вдасться отримати значення A, її очевидною тактикою стає підбір правильних значень для множин із $a + h$ розрядів експоненти, обробка яких здійснюються на термінальній платформі. Такий підбір потребує перебору 2^{a+h} можливих значень вказаних розрядів. Для кожного з цих можливих значень потрібно здійснити операцію модулярного експоненціювання згідно (13) щоб порівняти отриманий результат зі значенням Y. Очевидно, що зазначений підбір потребує обчислювальних ресурсів, об'єм яких в грошовому еквіваленті може бути оцінений як ϑ. Відповідно, кількість g розрядів секретного коду, які потрібно підбирати, має, для кожного конкретного застосування, бути такою, щоб вигода Θ в грошовому еквіваленті від отримання незаконного доступу до ключа термінального пристрою системи управління була меншою за ϑ: $\Theta < \vartheta$.

Очевидно, що запропонований метод надає широкі можливості для гнучкого вибору кількості розрядів експоненти, обробку яких здійснює термінальний мікроконтролер, тобто забезпечує можливість адаптації конфігурації системи під будь-які вимоги щодо рівня захищеності.

Прискорення реалізації базової операції криптографії з відкритим ключем – модулярного експоненціювання – на термінальному мікроконтролері за рахунок залучення хмарних технологій можна розглядати з точки зору двох аспектів. В рамках першого з них, порівнюється час обчислення модулярної експоненти виключно на термінальному мікроконтролері та час виконання цієї задачі із залученням хмарних технологій за запропонованим методом. Відповідно, коефіцієнт β_1 визначається за формулою (14). Час T здійснення модулярного експоненціювання за запропонованим методом визначається часом роботи термінального мікроконтролера за умови його повного завантаження, тобто

тривалістю часткової обробки на ньому g розрядів коду експоненти:

$$\beta_1 = \frac{T_0}{T} = \frac{1.5 \cdot n \cdot t_m}{0.5 \cdot g \cdot t_m} = 3 \cdot \frac{n}{g}. \quad (14)$$

Для викладеного вище прикладу вибору розрядностей адитивних фрагментів експоненти при заданому об'ємі ресурсів для порушення захисту значення β_1 дорівнює згідно (14): $\beta_1 = 3 \cdot 2048/63 = 96.4$. Це означає, що в рамках цього прикладу залучення до модулярного експоненціювання хмарних обчислень за запропонованим методом дозволяє прискорити виконання базової операції криптографії з відкритим ключем майже на два порядки.

Другий аспект аналізу прискорення модулярного експоненціювання полягає у порівнянні часу виконання цієї операції за відомими підходами із залученням віддалених комп'ютерних потужностей та аналогічного показника для запропонованого методу. Порівняння швидкодії різних підходів при ідентичному рівні захищеності, тобто при однаковому значенні g, може бути здійснене шляхом обчислення коефіцієнту прискорення β_2, представленого у вигляді:

$$\beta_2 = \frac{T_E}{T_M}. \quad (15)$$

де T_E – час модулярного експоненціювання за відомими схемами, а T_M – час обчислення модулярної експоненти за запропонованим методом.

Всі відомі підходи, зокрема ті, що базуються на мультиплікативно-адитивному чи адитивному розкладенні коду експоненти, пропонують такий розподіл обчислень між термінальним мікроконтролером та хмарними системами, при якому повна обробка всіх g секретних розрядів коду експоненти здійснюється на мікроконтролері. Цілком очевидно, що швидкість виконання обчислень на віддалених комп'ютерних системах значно перевищує швидкість роботи малопотужних термінальних мікроконтролерів. Тому вважається, що тривалість виконання модулярного експоненціювання при залученні хмарних систем визначається часом роботи термінальної платформи, на якій виконується тобто:

$$T_E = 1.5 \cdot g \cdot t_m. \quad (16)$$

В розробленому методі запропоновано принципово новий підхід до розподілу обчислень між термінальною та віддаленою платформами: він здійснюється не тільки на рівні ітерацій, а і всередині кожної ітерації. За розробленим методом, на мікроконтролері виконується лише модулярне множення, в той час як, незалежне від секретного коду експоненти, модулярне піднесення до квадрату повністю обчислюється віддалено. Таким чином, на відміну від відомих рішень, час роботи мікроконтролера визначається сумарним часом виконання операцій модулярного добутку поточного результату на постійне число при обробці g бітів коду експоненти:

$$T_M = 0.5 \cdot g \cdot t_m. \quad (17)$$

Тоді, згідно з (15), коефіцієнт прискорення β_2 для запропонованого методу визначається наступним чином:

$$\beta_2 = \frac{1.5 \cdot g \cdot t_m}{0.5 \cdot g \cdot t_m} = \frac{1.5}{0.5} = 3. \quad (18)$$

З отриманого виразу (18) можна зробити висновок, що запропонований метод дозволяє значно прискорити обчислення модулярної експоненти в порівнянні з відомими методами залучення хмарних обчислень при однаковому рівні захищеності від реконструювання коду експоненти на віддалених платформах. Трикратне прискорення досягається при будь-яких значеннях розрядності g, якою визначається необхідний рівень захищеності та часу t_m виконання модулярного множення на термінальному мікроконтролері.

Висновки

В результаті проведених досліджень теоретично обґрунтовано та розроблено метод захищеного модулярної експоненціювання для швидкої реалізації алгоритмів криптографічного захисту з залученням

хмарних обчислень в системах моніторингу та управління на базі технологій *IoT*. Відмінність запропонованого методу полягає в тому, що він реалізує розподілення обчислення модулярної експоненти на рівні операції обробки поточного біту коду експоненти. В порівнянні з відомими методами розподілення обчислень між віддаленими та термінальною платформами, запропонований підхід дозволяє втроє зменшити обчислювальне навантаження на останню, в результаті чого втроє підвищена швидкість модулярного експоненціювання над числами великої розрядності для криптографічних застосувань. Таке прискорення обчислень досягнуто за рахунок збільшення об'єму даних, що передаються з віддалених обчислювальних потужностей на термінальну комп'ютерну платформу систем управління об'єктами реального світу.

Література

1. Elgazzar K., et al. Revisiting the internet of things: New trends, opportunities and grand challenges. *Frontiers in Internet of Things*. 2022. Vol. 1. P. 1–18.
2. 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. 111.
3. Jurcut A.D., Ranaweera P., Xu L. Introduction to IoT Security. *IoT Security: Advances in Authentication*. John Wiley & Sons Ltd, 2020. P. 27–64.
4. Unal D., Al-Ali A., Catak F.O., Hammoudeh M. 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.
5. Bardis N. Secure, Green Implementation of Modular Arithmetic Operations for IoT and Cloud Applications. *Green IT Engineering: Components, Networks and System Implementation*. Springer, 2017. P. 43–64.
6. Meneghello F., Calore M., Zucchetto D., Polese M., Zalella A. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices. *IEEE Internet of Things Journal*. 2019. V. 6. No. 5. P. 8182–8201.
7. Alfred Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press, 2001. 780 p.
8. Markovskyi O., Bardis N., Doukas N., Kirilenko S. Secure Modular Exponentiation in Cloud Systems. *Proceedings of The Congress on Information Technology, Computational and Experimental Physics (CITCEP 2015)* / Krakow, Poland, 2015. P. 266–269.
9. Jose Alberto de Jesus Borges, Haidukevych Oleksandra, Mirataei Alireza, Nikos Doukas. A Secure Cloud Computing Method for Rapid Implementation of Cryptographic Data Protection in IoT. *Proceeding of The 13th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2023* / Athens, Greece, 2023. P. 50–53.

Русанова О.В., Гайдукевич М.А., Міратаеї Аліреза

МЕТОД БЕЗПЕЧНОГО РОЗПОДІЛЕНОГО ОБЧИСЛЕННЯ МОДУЛЯРНОЇ ЕКСПОНЕНТИ ДЛЯ ПРИСКОРЕННЯ РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ЗАХИСТУ ДАНИХ В IoT

У статті пропонується метод захищеного модулярного експоненціювання на термінальних платформах IoT з залученням хмарних обчислень для швидкої реалізації алгоритмів криптографічного захисту з відкритим ключем. Метод реалізує новий принцип

розподілення обчислень між термінальною та віддаленими платформами при реалізації модулярного експоненціювання – на рівні обробки кожного окремого біту коду експоненти. Це дозволяє втроє зменшити обчислювальне навантаження на термінальну платформу і, відповідно, втроє прискорити обчислення базової операції криптографії з відкритим ключем в порівнянні з відомими методами розподіленого обчислення модулярної експоненти.

***Ключові слова**: модулярне експоненціювання, захищені обчислення в хмарі, безпека IoT, гомоморфне шифрування, цифровий підпис.*

Rusanova O.V., Haidukevych M.A., Mirataei Alireza

METHOD OF MODULAR EXPONENT SECURE DISTRIBUTED COMPUTATION FOR ACCELERATED IMPLEMENTATION OF DATA PROTECTION MECHANISMS IN IoT

The article proposes a method of secure modular exponentiation on IoT terminal platforms involving cloud computing for fast implementation of public key cryptographic protection algorithms. The method implements a new principle of distribution of calculations between the terminal and remote platforms when implementing modular exponentiation - at the level of processing each individual bit of the exponent code. This makes it possible to reduce the computing load on the terminal platform by three times and, accordingly, to speed up the calculation of the basic operation of public key cryptography by three times compared to the known methods of distributed calculation of the modular exponent.

***Keywords**: modular exponentiation, secure cloud computing, IoT security, homomorphic encryption, digital signature.*