УДК 004.056.53

DOI: 10.18372/2073-4751.80.19785

Русанова О.В., к.т.н.,
orcid.org/0000-0003-0145-3012,
e-mail: olga.rusanova@gmail.com,
Гуцуляк Н.А.,
orcid.org/0009-0009-0472-9695,
e-mail: nyancatandme0@gmail.com,
Скворцов П.С.,
orcid.org/0009-0004-9980-4654,
e-mail: ps.skvortsov@gmail.com

МЕТОД ШВИДКОЇ РЕАЛІЗАЦІЇ ПЕРЕТВОРЕННЯ ФУР'Є З ЗАХИЩЕНИМ ЗАЛУЧЕННЯМ ХМАРНИХ ОБЧИСЛЕНЬ

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

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 експо-ненціювання з 2048-розрядними операндами на 32-розрядному термінальному мікроконтролері вимагає близько 6 мільйонів процесорних операцій [5]. Для малопотужних мікроконтролерів виконання таких складних обчислень вимагає значних часових ресурсів, що протиречить 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.

Огляд процедур ДПФ та технологій їх захищеної реалізації на віддалених обчислювальних платформах.

Перетворення Фур'є виконується над масивом відліків вхідного сигналу $s_0, s_1, \ldots s_{n-1}$, які являють собою

дискретизовані по значенню і часу виміри реального сигналу. Результатом ДПФ є два масиви X і Y. Масив $X = \{x_0, x_1,\ldots,x_{n-1}\}$ містить в собі реальні компоненти комплексних чисел, що описують синусоїди з частотами ω, 2·ω, 3·ω,…n·ω та обчислюються за формулою [3] :

$$\forall i \in \{0,1,\cdots,n-1\}: x_i = \frac{1}{n} \cdot \sum_{q=0}^{n-1} s_q \cdot \cos\frac{q \cdot i \cdot 2 \cdot \pi}{n}. \quad (1)$$

В масиві $Y=\{y_0,y_1,\ldots,y_{n-1}\}$ формуються уявні компоненти зазначених вище комплексних чисел у відповідності з формулою:

$$\forall i \in \{0,1,\cdots,n-1\}: y_i = \frac{1}{n} \cdot \sum_{q=0}^{n-1} s_q \cdot \sin\frac{q \cdot i \cdot 2 \cdot \pi}{n}. \quad (2)$$

Аналіз формул (1,2) засвідчує, що косинусоїдальні та синуноїдальні їх компоненти не залежать від відліків вхідного сигналу $s_0,s_1,\ldots s_{n-1}$, а визначаються лише значеннями індексів q та i. Це означає, що їх значення для всіх індексів може бути порахувано заздалегідь і результати цих обчислень можуть розглядатися як залежні від індексів коефіцієнти, що обчислюються за такими формулами [3]:

$$\forall i,q \in \{0,1,\cdots,n-1\}: c_{q,i} = \frac{1}{n} \cdot \cos\frac{q \cdot i \cdot 2 \cdot \pi}{n}, \quad d_{q,i} = \frac{1}{n} \cdot \sin\frac{q \cdot i \cdot 2 \cdot \pi}{n}. \quad (3)$$

Пильний аналіз формул (3) дозволяє зробити висновок, що тригонометричні коефіцієнти ДПФ симетричні відносно головної діагоналі, що в теорії дозволяє прискорити обчислення формул (1) та (2). Така властивість відома на практиці цифрової обробки сигналів як швидке перетворення Фур'є (ШПФ). Його використання, в порівнянні з ДПФ дозволяє зменшити кількість операцій множення практично вдвічі.

З урахуванням передобчислень (3) розрахункові формули ДПФ (1,2) трансформуються до вигляду :

$$\forall i \in \{0,1,\cdots,n-1\} : x_i = \sum_{q=0}^{n-1} s_q \cdot c_{q,i}, \quad y_i = \sum_{q=0}^{n-1} s_q \cdot d_{q,i} \quad (4)$$

Таким чином, об'єм обчислень ДПФ має квадратичну залежність від кількості n вимірів вхідних сигналів, яка на практиці складає сотні чи тисячі, що вимагає виконання мільйонів операцій множення. Це створює проблеми реалізації ДПФ в режимі реального часу на термінальних мікроконтролерах (ТМК) з обмеженою обчислювальною потужністю [1].

Вирішення цієї проблеми за допомогою використання графічного процесору чи спеціальної мікросхеми для обчислення ДПФ, пов'язане зі значними складнощами зумовленими обмеженнями вартості та споживання потужності ТМК [4]. Таким чином, найбільш перспективним шляхом прискорення реалізації ДПФ на ТМК, в більшості яких присутній радіо модем, є залучення хмарних технологій. З іншого боку це породжує проблему запобіганню можливості відновлення вимірів реального сигналу за отриманих хмарою даних. Тому для реалізації цієї можливості прискорення ДПФ необхідно організувати спеціальне гомоморфне шифрування даних, що надсилаються в хмару [6].

Протягом багатьох років існувала думка, що створити універсальне гомоморфне шифрування, придатне для будь-яких перетворень над зашифрованими даними. І тільки в 2010 в роботі [7] було запропоновано першу модель універсального гомоморфного шифрування. Проте запропонований метод, в зв'язку з складністю обчислень, так і не знайшов до теперішнього часу практичного використання. Втім, на практиці активно застосовуються спеціалізовані схеми гомоморфного шифрування, в тому числі і для ДПФ.

Вважаючи на важливість гомоморфного шифрування в ДПФ до теперішнього часу розроблена низка методів для підвищення рівня його ефективності [8].

Найбільшого поширеним на практиці отримав метод адитивного

маскування вимірів сигналів [9]. Ідея полягає в використанні n-компонентної маски $M=\{m_0,m_1,\ldots,m_{n-1}\}$, для якої попередньо обчислюються масиви реальних $R=\{r_0,r_1,\ldots,r_{n-1}\}$ та уявних компонент $U=\{u_0,u_1,\ldots,u_{n-1}\}$ спектрального представлення. Ці масиви разом з маскою M зберігаються пам'яті ТМК. При виконанні ДПФ в хмарі гомоморфне шифрування вимірів $s_0,s_1,\ldots s_{n-1}$, зводиться до покомпонентного додавання до них маски:

$$\forall i \in \{0,1,\cdots,n-1\}: \gamma_i = s_i + m_i. \qquad (5)$$

Зашифровані сигнали $\gamma_0, \gamma_1,\ldots,\gamma_{n-1}$ надсилаються в хмару, де над ними здійснюється ДПФ з отриманням масивів реальних $\Theta=\{\theta_0,\theta_1,\ldots,\theta_{n-1}\}$ та уявних компонент $\Psi=\{\psi_0,\psi_1,\ldots,\psi_{n-1}\}$ спектрального представлення:

$$\forall i \in \{0,1,\cdots,n-1\}: \theta_i = \sum_{q=0}^{n-1} \gamma_q \cdot c_{q,i} = \\ = \sum_{q=0}^{n-1} s_q \cdot c_{q,i} + \sum_{q=0}^{n-1} m_q \cdot c_{q,i} = x_i + r_i \qquad (6)$$

$$\forall i \in \{0,1,\cdots,n-1\}: \psi_i = \sum_{q=0}^{n-1} \gamma_q \cdot d_{q,i} = \\ = \sum_{q=0}^{n-1} s_q \cdot d_{q,i} + \sum_{q=0}^{n-1} m_q \cdot d_{q,i} = y_i + u_i$$

Відповідно, процес гомоморфного дешифрування отриманих з хмари компонентів спектрального представлення сигналу полягає в відніманні від компонентів Θ та Ψ одноіменних компонентів R та U спектрального представлення маски.

Основний недолік адитивного маскування полягає в тому, що одна і та ж сама маска використовується для гомоморфного шифрування всіх сигналів. Це зумовлює небезпеку існування потенційної можливості відновлення маски через перехоплення відліків хоча б одного з вхідних сигналів.

В сучасних методах захищеного віддаленого перетворення Фур'є, усунення цієї небезпеки досягається за рахунок різних підходів до модифікації маски. Ці підходи можна розділити на три основні категорії:

- композитне маскування;
- довільний вибір маски з пулу;
- зміна маски з використанням даних з попередніх ДПФ

Методи з категорії композитного маскування передбачають утворення нових масок за допомогою комбінування вже існуючих [10]. Для цього в пам'яті ТМК зберігається набір з k масок $M = \{m_0,m_1,\ldots,m_{n-1}\}$ та результатів їх ДПФ в вигляді реального вектора $R=\{r_0,r_1,\ldots,r_{n-1}\}$ та уявного $U=\{u_0,u_1,\ldots,u_{n-1}\}$. Кожна нова маска MN формується як сума двох масок з набору, при цьому відповідні цим маскам вектори реальних та уявних компонент також додаються для утворення нового реального RN та уявного UN векторів: $MN = M_1 + M_2 = \{m_{10}+ m_{20}, m_{11}+ m_{21},\ldots, m_{1n} +m_{2n}\}$; $RN = R_1 + R_2 = \{r_{10}+ r_{20}, r_{11}+ r_{21},\ldots, r_{1n} +r_{2n}\}$; $UN = U_1 + U_2 = \{u_{10}+ u_{20}, u_{11}+ u_{21},\ldots, u_{1n} +u_{2n}\}$. Над вектором вимірів $s_0,s_1,\ldots s_{n-1}$ вхідного сигналу S проводиться адетивне маскування за допомогою утвореної маски MN. Проведене обчислення надсилається на хмару. Отриманий результат ДПФ розшифровується завдяки векторам RN та UN. Використана маска зберігається в пам'яті ТМК для формування нових масок. До недоліків цього підходу можна віднести обмежену в 2^k кількість комбінацій та необхідність зберігання великого, для ТМК, об'єму даних.

До другої категорії підходів до реалізації захищеного перетворення Фур'є в хмарах можна віднести довільний вибір маски з пулу [11]. Побудовані на цьому методи передбачають одноразове створення пулу з кількості k масок на етапі ініціалізації мікроконтролера. Гомоморфне шифрування вектору відліків вхідного сигналу, при такому підході, здійснюється за допомогою додавання до нього довільно вибраної маски з пулу. Головним недоліком таких методів виступає обмежений об'єму пулу пам'яттю ТМК.

Іншим відомим підходом є зміна маски з використанням даних з попередніх ДПФ. Для реалізації такого типу методу в

пам'яті ТМК зберігається початкова n-компонентна маска $M = \{m_0,m_1,\ldots,m_{n-1}\}$ та результат її ДПФ в вигляді двох масивів: реальні компоненти $R = \{r_0,r_1,\ldots,r_{n-1}\}$ та уявні $U = \{u_0,u_1,\ldots,u_{n-1}\}$ спектрального представлення. Гомоморфне шифрування відліків $s_0,s_1,\ldots s_{n-1}$ вхідного сигналу S реалізується як додавання до цих компонент відповідних значень маски M: $\forall i\in\{0,1,\ldots,n-1\}$: $\tau_i = s_i + m_i$. Отриманий масив $\tau_0, \tau_1,\ldots, \tau_{n-1}$ відправляється для обчислення ДПФ на хмару, в результаті чого ТМК отримує масив реальних компонент $\xi=\{\xi_0, \xi_1,\ldots, \xi_{n-1}\}$ та уявних $\eta=\{\eta_0,\eta_1,\ldots,\eta_{n-1}\}$. Гомоморфне дешифрування результату полягає в відніманні від отриманих векторів ξ та η одноіменних компонентів R та U. Масці M присвоюється значення відліків сигналу S: $M = \{s_0,s_1,\ldots s_{n-1}\}$, реальним та уявним компонентам присвоюються значення результату ДПФ над відліками $s_0,s_1,\ldots s_{n-1}$. Таким чином дані з попереднього ДПФ використовуються в якості маски. Головним недоліком цього методу є те, що дізнаючись виміри одного з сигналів, зловмисник зможе відтворити весь ланцюжок.

Проведений оглядовий аналіз відомих методів гомоморфного шифрування вимірів сигналів для їх захищеного виконання над ними ДПФ засвідчив, що найбільш ефективним з позицій часу реалізації шифрування-дешифрування є їх адитивне маскування. Виходячи з того, що головний недолік цієї технології полягає в слабкій захищеності, зумовленої незмінністю маски, запропоновано ряд методів її модифікації. Аналіз цих методів показує, що їх реалізація потребує значних ресурсів як пам'яті, так і часу виконання передбачених ними обчислювальних процедур.

Мета досліджень полягає в підвищенні ефективності захищеної реалізації ДПФ на віддалених комп'ютерних системах шляхом унеможливлення відновлення групи вхідних сигналів за наявності інформації про хоча б один із них за рахунок швидкої зміни маски після обробки кожного сигналу.

Організація гомоморфного шифрування даних для захищеної віддаленої реалізації ДПФ

Одним із можливих шляхів підвищення ефективності адитивного маскування, як засобу гомоморфного шифрування вимірів сигналу при віддаленому виконанні над ним ДПФ є спрощення процедури модифікації маски до рівня, який дозволяє реалізувати таку модифікацію на термінальному мікроконтролері.

В рамках реалізації цього підходу пропонується в якості маски M використовувати множину із h бітових модифікаторів. Номери бітів $\eta_1,\eta_2,\ldots,\eta_h$ вимірів сигналу, до яких при гомоморфному шифруванні додаються відповідні модифікатори утворюють множину ϑ. Іншими словами, множина ϑ містить h номерів бітів, для яких створені бітові модифікатори маски: $\vartheta=\{\eta_1,\eta_2,\ldots,\eta_h\}$, $\forall l\in\{1,2,\ldots,h\}$: $\eta_l\in\{0,1,\ldots,n-1\}$. Бітові модифікатори $B_1,B_2,\ldots,B_h$ складаються n двохрозрядних компонент, які приймаються три значення: мінус одиниця, нуль та одиниця: $\forall l\in\{1,2,\ldots,h\}$: $B_l = \{b_{l,0},b_{l,1},\ldots,b_{l,n-1}\}$, $\forall j\in\{0,1,\ldots,n-1\}$: $b_{l,j}\in\{-1,0,1\}$. Для кожного l-того з бітових модифікаторів маски обчислюються n значення $\delta_{l,0},\delta_{l,1},\ldots,\delta_{l,n-1}$ та $\lambda_{l,0}$, $\lambda_{l,1},\ldots,\lambda_{l,n-1}$ за наступними формулами:

$$\forall i \in \{0,\ldots,n-1\}: \delta_{l,i} = \sum_{q=0}^{n-1} b_{l,q}\cdot c_{q,i},$$
$$\lambda_{l,i} = \sum_{q=1}^{n-1} b_{l,q}\cdot d_{q,i} \quad . \qquad (7)$$

Аналіз формул (7) дозволяє зробити висновок про те, що модифікатори не залежать от конкретного розряду. Відповідно, вони можуть бути використані для гомоморфного шифрування будь-якого із двійкових розрядів кодів вимірів вхідного сигналу.

Можливі різні конфігурації реалізації запропонованого підходу. В найбільш розвиненій конфігурації кожному із двійкових розрядів, що складають множину ϑ, ставиться у відповідність окремий модифікатор. В більш простих конфігураціях для

гомоморфного шифрування декількох розрядів кодів вимірів вхідного сигналу може застосовуватися один і той же модифікатор. Вибір конфігурації використання бітових модифікаторів визначається характеристиками обчислювальних можливостей термінального мікроконтролера та вимогами до рівня захищеності.

Елементами забезпечення захисту вхідного сигналу від його реконструкції за шифрованими даними, що передаються через хмару на непідконтрольні і, відповідно, потенційно небезпечні віддалені комп'ютерні системи виступають:

- випадково обрані для кожного сеансу шифрування номери розрядів, що утворюють множину ϑ;
- випадковим вибором для кожного сеансу шифрування розрядів вимірів вхідного сигналу бітових модифікаторів;
- невідомими для атакуючої сторони компонентами бітових модифікаторів, які випадковим чином для кожного сеансу шифрування розподіляються по множині розрядів ϑ;
- зміною бітових модифікаторів від одного сеансу шифрування вхідного сигналу до іншого.

Запропонований метод захищеної реалізації ДПФ з залученням хмарних обчислень в конфігурації, коли для шифрування кожного розряду використовується свій бітовий модифікатор, включає в себе наступні процедури:

- процедуру формування бітових модифікаторів, що виконується на етапі підготовки системи до роботи;
- процедуру гомоморфного шифрування вимірів вхідного сигналу перед їх надсиланням в хмару для віддаленої реалізації ДПФ, а також дешифрування отриманих результатів для отримання складових реальних та уявним компонент спектрального представлення вхідного сигналу;
- процедуру зміни бітових модифікаторів за наявності часового резерву в роботі термінального мікроконтролера.

Процедура формування бітових модифікаторів $B_1,B_2,\ldots,B_h$ здійснюється на підготовчому етапі налагодження системи. Процедура полягає в формуванні як самих бітових модифікаторі, так і обчислення для кожного l-го із таких модифікаторів n-компонентних векторів $\Delta_l = \{\delta_{l,0},\delta_{l,1},\ldots,\delta_{l,n-1}\}$ та $\Lambda_l=\{\lambda_{l,0}, \lambda_{l,1},\ldots,\lambda_{l,n-1}\}$. В формалізованому вигляді процедура полягає в виконанні наступної послідовності дій:

1. Номер l поточного бітового модифікатора встановлюється в одиницю: l=1.
2. Поточне значення індексу j компоненти бітового модифікатора B_l встановлюється в нуль: j=0.
3. Компоненті модифікатора $b_{l,j}$ присвоюється значення випадкового цілого числа, яке з рівною ймовірністю приймає значення з множини {-1,0,1).
4. Значення поточного індексу j компоненти бітового модифікатора B_l збільшується на одиницю: $j=j+1$; якщо $j<n$, здійснюється повергнення на повторне виконання п.3.
5. Для поточного l-го бітового модифікатора B_l за формулою (7) обчислюються компоненти векторів $\Delta_l = \{\delta_{l,0},\delta_{l,1},\ldots,\delta_{l,n-1}\}$ та $\Lambda_l=\{\lambda_{l,0}, \lambda_{l,1},\ldots,\lambda_{l,n-1}\}$.
6. Збільшується на одиницю значення поточного номеру l бітового модифікатора: $l=l+1$; якщо $l<h+1$, здійснюється повергнення на повторне виконання п.2.

Процедура може реалізовувати як на термінальному мікроконтролері, так і на центральному комп'ютері системи віддаленого моніторингу стану об'єктів реального світу.

Процедура гомоморфного шифрування вимірів вхідного сигналу перед їх надсиланням в хмару для віддаленої реалізації ДПФ, а також дешифрування отриманих результатів для отримання складових реальних та уявним компонент спектрального представлення вхідного сигналу передбачає виконання наступної послідовності дій:

1. Випадковим чином обирається множина $\vartheta=\{\eta_1,\eta_2,\ldots,\eta_h\}$ номерів розрядів двійкового представлення відліків $s_0,s_1,\ldots,s_{n-1}$ вхідного сигналу, над яким здійснюється ДПФ.

2. Здійснюється гомоморфне шифрування відліків $s_0,s_1,\ldots,s_{n-1}$ вхідного сигналу у відповідності з наступним перетворенням:

$$\forall i \in \{0,1,\cdots,n-1\}: s_i' = s_i + \sum_{l=1}^{h} 2^{\eta_l} \cdot b_{l,i} \ . \quad (8)$$

3. Отримані в результаті гомоморфного шифрування відліки $s_0',s_1',\ldots,s_{n-1}'$ зашифрованого вхідного сигналу надсилаються на віддалену комп'ютерну систему.

4. В хмарі, на віддалених комп'ютерних системах над кодами відліків $s_0',s_1',\ldots,s_{n-1}'$ виконується ДПФ з отриманням масивів реальних $\Theta=\{\theta_0,\theta_1,\ldots,\theta_{n-1}\}$ та уявних компонент $\Psi=\{\psi_0,\psi_1,\ldots,\psi_{n-1}\}$ спектрального представлення у відповідності з наступними формулами:

$$\forall i \in \{0,1,\cdots,n-1\}: \theta_i = \sum_{q=0}^{n-1} s_q' \cdot c_{q,i} = \\ = \sum_{q=0}^{n-1} s_q \cdot c_{q,i} + \sum_{q=0}^{n-1}\sum_{l=1}^{h} 2^{\eta_l} \cdot b_{l,q} \cdot c_{q,i} \quad . \quad (9)$$

$$\forall i \in \{0,1,\cdots,n-1\}: \psi_i = \sum_{q=0}^{n-1} s_q' \cdot d_{q,i} = \\ \sum_{q=0}^{n-1} s_q' \cdot d_{q,i} + \sum_{q=0}^{n-1}\sum_{l=1}^{h} 2^{\eta_l} \cdot b_{l,q} \cdot d_{q,i}$$

5. По завершенні формування результатів ДПФ на віддалених комп'ютерній системі, результати у вигляді масивів реальних $\Theta=\{\theta_0,\theta_1,\ldots,\theta_{n-1}\}$ та уявних компонент $\Psi=\{\psi_0,\psi_1,\ldots,\psi_{n-1}\}$ спектрального представлення зашифрованого вхідного сигналу надсилаються на термінальний мікроконтролер.

6. Одержані з хмари термінальним мікроконтролером масиви реальних $\Theta=\{\theta_0,\theta_1,\ldots,\theta_{n-1}\}$ та уявних компонент $\Psi=\{\psi_0,\psi_1,\ldots,\psi_{n-1}\}$ спектрального представлення сигналу $s_0',s_1',\ldots,s_{n-1}'$ дешифруються з у відповідності з наступними формулами:

$$\forall i \in \{0,1,\cdots,n-1\}: x_i = \theta_i - \sum_{l=1}^{h} 2^{\eta_l} \cdot \delta_{l,i}, \\ y_i = \psi_i - \sum_{l=1}^{h} 2^{\eta_l} \cdot \lambda_{l,i} \quad . \quad (10)$$

Процедура оновлення бітових модифікаторів полягає в здійсненні однієї із двох опцій:

- видалення одного бітового модифікатора, що співвідноситься з певним двійковим розрядом і створення натомість нового бітового модифікатора, який співвідноситься з іншим розрядом кодів вимірів вхідного сигналу;
- зміна к компонентів одного із бітових модифікаторів.

Перша із наведених опцій реалізується у наступному порядку:

1. Випадковим чином обирається номер u із номерів множини $\vartheta=\{\eta_1,\eta_2,\ldots,\eta_h\}$ розрядів вимірів вхідного сигналу, для яких існує бітовий модифікатор: $u \in \vartheta$.

2. Модифікатор B_u видаляється шляхом виконання такої послідовності дій: всі n його компонентів встановлюються нуль: $\forall j \in \{0,1,\ldots,n-1\}$: $b_{u,j}=0$. Всі n компонент відповідних модифікатору B_u векторів Δ_u та Λ_u обнуляються: $\forall j \in \{0,1,\ldots,n-1\}$: $\delta_{u,j}=0$, $\lambda_{u,j}=0$.

3. Випадковим чином обирається номер розряду у, що не належить множині ϑ: $y \notin \{\eta_1,\eta_2,\ldots,\eta_h\}$.

4. Поточне значення індексу j компоненти обраного бітового модифікатора B_y встановлюється в нуль: $j=0$.

5. Компоненті модифікатора $b_{y,j}$ присвоюється значення випадкового цілого числа, яке з рівною ймовірністю приймає значення з множини {-1,0,1).

6. Значення поточного індексу j компоненти бітового модифікатора B_y збільшується на одиницю: $j=j+1$; якщо $j<n$, здійснюється повергнення на повторне виконання п.3.

7. Для створеного у-го бітового модифікатора B_y за формулою (7) обчислюються компоненти векторів $\Delta_y = \{\delta_{y0},\delta_{y,1},\ldots,\delta_{y,n-1}\}$ та $\Lambda_y=\{\lambda_{y0}, \lambda_{y,1},\ldots,\lambda_{y,n-1}\}$:

$$\forall j \in \{0,1,...,n-1\}: \delta_{y,j} = \sum_{q=0}^{n-1} b_{y,q} \cdot c_{q,j},$$
$$\lambda_{y,j} = \sum_{q=1}^{n-1} b_{y,q} \cdot d_{q,j} \quad . \qquad (11)$$

8. Компонента u множини 9 замінюється на номер *y*.

Опція зміни κ компонентів одного із бітових модифікаторів складається з наступної послідовності дій:

1. Випадковим чином обирається номер $l \in \{1,2,\ldots,h\}$ модифікатора B_l, що змінюється. Лічильник c кількості модифікованих компонентів модифікатора B_l встановлюються в нуль: c=0.

2. Випадковим чином обирається номер j$\in \{0,1,\ldots,n\text{-}1\}$ компоненти $b_{l,j}$ модифікатора B_l, яка оновлюється.

3. Генерується випадкове ціле число g, яке з рівною ймовірністю приймає значення з множини {-1,0,1). Якщо $g = b_{l,j}$, виконання п.2 процедури повторюється.

4. Здійснюється корекція компонентів векторів $\Delta_y = \{\delta_{y0},\delta_{y,1},\ldots,\delta_{y,n\text{-}1}\}$ та $\Lambda_y=\{\lambda_{y0}, \lambda_{y,1},\ldots,\lambda_{y,n\text{-}1}\}$ за наступними формулами:

$$\forall i \in \{0,1,...,n-1\}: \delta_{l,i} = \delta_{l,i} - c_{j,i} \cdot (b_{l,j} - g),$$
$$\lambda_{l,i} = \lambda_{l,i} - d_{j,i} \cdot (b_{l,i} - g)$$

5. Значення $b_{l,j}$ кладеться рівним g : $b_{l,j} = g$. Значення лічильника c збільшується на одиницю: c=c+1. Якщо $c<\kappa$, то виконується повернення на повторне виконання п. 2.

З наведеного опису запропонованої процедури видно, що вона дозволяє в широких межах варіювати час.

Аналіз ефективності

Основна перевага запропонованого методу захищеної реалізації ДПФ з залученням хмарних технологій полягає в можливості зміни маски з використанням обчислювальних потужностей, об'єм яких дозволяє робити це в інтервалі між обробкою сигналів. Як видно з наведеного вище опису, запропонована процедура оновлення маски має багато опцій та налаштувань, які дозволяють ефективно адаптувати її в залежності від наявних часових ресурсів ТМК між обробкою сигналів. В мінімальній конфігурації змін оновлення маски потребує n операцій додавання для зміни бітового модифікатора, а також $4 \cdot n$ операцій додавання для зміни спектральних характеристик маски. Тобто, на відміну від існуючих методів, для зміни маски і її спектральних характеристик не потрібно використовувати ресурсоємких мультиплікативних операцій. Крім того, як видно з опису процедур оновлення маски обчислювальна складність цієї операції в запропонованому методі лінійно залежить від n – кількості вимірів вхідного сигналу і, відповідно, кількості синусоїд спектрального представлення маски. В відомих методах обчислювальна складність виконання модифікації маски залежить від n квадратично, тобто $O(n^2)$, або $O(n \cdot log_2\, n)$.

Таким чином, запропоноване рішення дозволяє вирішити задачу зміни маски з використанням меншої кількості ресурсів в порівнянні з відомими методами. При цьому кількість варіантів модифікації маски визначається формулою:

$$N = \binom{n}{u} \cdot 3^n . \qquad (12)$$

Цілком очевидно, що ця кількість на порядки більша в порівнянні з відомим методами [9, 10]. Проведений аналіз показав, що визначена формулою (12) кількість варіантів практично виключає можливість повторення маски. В цьому сенсі, запропонований метод гомоморфного шифрування вимірів сигналів, над якими здійснюється ДПФ, забезпечує суттєво більший рівень захищеності від спроб реконструкції вхідного сигналу за даними які надаються в хмару.

Процедура гомоморфного шифрування в запропонованому методі значно простіша в порівнянні з адитивним маскуванням в форматі з плаваючою точкою, оскільки вона дозволяє працювати з окремими бітовими зрізами кодів відліків. Це зумовлено тим, що для гомоморфного шифрування використовуються логічні операції та операція зсуву. Повною мірою це стосується і операцій гомоморфного

дешифрування результатів спектрального представлення сигналів. В результаті проведених експериментальних досліджень доведено, що швидкість гомоморфного шифрування при використанні запропонованого методу практично в 2.4 рази вища в порівнянні з адитивним маскуванням вимірів.

Висновки

В результаті досліджень, направлених на прискорення реалізації ДПФ на малопотужних ТМК в реальному часу, створено метод, який забезпечує це обчислення з залученням хмарних технологій.

Запропонований метод швидкої реалізації ДПФ з захищеним залученням хмарних обчислень, який відрізняється тим, що адитивна маска, яка використовується для гомоморфного шифрування відліків сигналу, оновлюється після кожної такої операції шляхом зміни окремих бітових шарів з відповідною корекцією спектральних представлень маски, за рахунок чого досягається прискорення оновлення маски.

Теоретично доведено та експериментально підтверджено, що обчислювальна складність оновлення маски лінійно залежить від n, на відміну від відомих методів, де модифікація маски залежить від n квадратично, відповідно це породжує можливість зміни маски при обробці кожного сигналу. За рахунок збільшення оперативності модифікації маски досягається прискорення шифрування практично в 2.4 рази в порівнянні з відомими методами адитивного маскування вимірів.

Запропонований метод орієнтовано на використання в системах віддаленого моніторингу об'єктів реального світу, аналіз спектральних характеристик яких виконується на малопотужних ТМК в режимі реального часу, завдяки перенесенню обчислення ДПФ на хмарні технологій.

Література

1. Kumar G., Sahoo S. K., Meher P. 50 Years of FFT Algorithms and Applications *Computer Science. Circuits, systems and processing*. 2019. Vol. 38, no. 12. P. 5651–5664.

2. Nakonechny A. J., Pazan P. G. Signal processing using modern cloud technologies. *Visnik of the National University «Lviv Polytechnic», series Automation, measurement and control*. 2015. Vol. 821. P. 8–16.

3. Sundararajan D. The Discrete Fourier Transform. Theory, Algorithm and Applications. Word Scientific Publishing Co, 2001. 456 p.

4. Togo M. R. Low PowerVLSI Implementation of Fast Fourier Transform. *International Journal of Engineering Research &Technology (IJERT)*. 2022. Vol. 11, no. 5. P. 673–677. DOI: 10.17577/IJERTV11IS 050066.

5. Bardis N. et al. Accelerate Approach for Public Key Cryptography Implementation on IoT Terminal Platforms. *2023 13th International Conference on Dependable Systems, Services and Technologies (DESSERT)* : proceedings, Athens, Greece, 13–15 October 2023 / IEEE. 2023. P. 678–681. DOI: 10.1109/ DESSERT61349. 2023.10416516.

6. Markovskyi O. P. et al. The method of accelerated secure image filtering on remote computer systems. *Telecommunication and information technology*. 2019. Vol. 65, no. 4. P. 99–110.

7. Gentry C., Helevi S. Implementing Gentry's fully-homomorphic encryption scheme. Annual international conference on the theory and applications of cryptographic techniques. 2011. Berlin : Springer, 2011. 29 p.

8. Yao Q. et al. Color image encryption based on discrete trinion Fourier transform and random-multiresolution singular value decomposition. *Multimedia Tools, and Applications*. 2020. P. 27555–27581.

9. Bianchi T., Piva A., Barni M. On the Implementation of the Discrete Fourier Transform in the Encrypted Domain. *IEEE Transactions on Information Forensics and Security*. 2009. Vol. 4. P. 86–97.

10. Mirataei A., Khalil H., Markovskyi O. Protected discrete Fourier transform implementation on remote computer systems. *Information, Computing and Intelligent systems*, 2020. № 1. P. 27–33.

11. Sandeep G., Rao S. S. Radix 4 fast fourier transform using new distributive arithmetic. *International Journal of Recent Technology and Engineering*. 2019. Vol. 8. P. 11–15.

Русанова О.В., Гуцалюк Н.А., Скворцов П.С.

МЕТОД ШВИДКОЇ РЕАЛІЗАЦІЇ ПЕРЕТВОРЕННЯ ФУР'Є З ЗАХИЩЕНИМ ЗАЛУЧЕННЯМ ХМАРНИХ ОБЧИСЛЕНЬ

В статті запропоновано метод швидкої реалізації дискретного перетворення Фур'є (ДПФ) на термінальному мікроконтролері (ТМК), який має за основу адетивне маскування сигналів і відрізняється тим, що здійснює оновлення маски шляхом зміни її бітових шарів, що дозволяє реалізувати оновлення маски перед обробкою кожного вхідного сигналу. Теоретично обґрунтовані та в деталях описані базові процедури ме-тоду. Виконано аналіз ефективності запропонованого методу гомоморфного шифру-вання відліків сигналу з реального об'єкту. Показано, що завдяки використанню більш швидкої процедури оновлення маски зміною її бітових шарів - суттєво підвищується рівень захищеності відліків сигналу від спроб їх незаконного відновлення в хмарі. Це досягається за рахунок зміни маски для кожного сигналу.

Також показано, що запропонований метод дозволяє скоротити в два рази час шифрування та дешифрування. Проведені експериментальні дослідження в цілому підтвердили отримані теоретичним шляхом оцінки ефективності.

***Ключові слова**: дискретне перетворення Фур'є; системи віддаленого моніторингу стану об'єктів реального світу; гомоморфне шифрування; захищення залучення віддалених обчислювальних потужностей.*

Rusanova O.V., Hutsuliak N.A., Scvorcov P.S.

A METHOD FOR FAST IMPLEMENTATION OF FOURIER TRANSFORM WITH SECURED USE OF CLOUD COMPUTING

The article proposes a method for fast implementation of the discrete Fourier trans-form (DFT) on a terminal microcontroller (TMC), which is based on additive masking of signals and is distinguished by the fact that it updates the mask by changing its bit layers, which allows to update the mask before processing each input signal. The basic procedures of the method are theoretically justified and described in detail. An analysis of the effec-tiveness of the proposed method of homomorphic encryption of signal readings from a real object was performed. It is shown that due to the use of a faster procedure for updating the mask by changing its bit layers, the level of protection of signal readings against attempts to illegally restore them in the cloud is significantly increased. This is achieved by changing the mask for each signal.

It is also shown that the proposed method can reduce the time of encryption and decryption by two times. The conducted experimental studies generally confirmed the results obtained by theoretical evaluation of efficiency.

***Keywords**: discrete Fourier transformation; systems for remote monitoring of the state of real-world objects; homomorphic encryption; protection using of remote computing power.*