виконується в канал синього кольору, так як до синього кольору система людського зору найменш чутлива [9]. Нехай біт який вбудовуємо, контейнер I={R,G,B}, p=(x,y) псевдовипадкова позиція, в якій виконується вкладення. Секретний біт вбудовується в канал синього кольору шляхом модифікації яскравості:

$$l(p) = 0{,}299r(p) + 0{,}587g(p) + 0{,}114b(p), \quad (1)$$

$$b'(p) = \begin{cases} b(p) + ql(p), & \text{якщо } s_i = 0, \\ b(p) - ql(p), & \text{якщо } s_i = 1 \end{cases} \quad (2)$$

де $q$ - коефіцієнт, що задає енергію біта даних, що вбудовується (задається виходячи з функціонального призначення і особливості стеганосистеми). Його значення залежить від призначення схеми. Чим більше q, тим вище робастність вкладення, але тим сильнішає його помітність.

Для реалізації програмного продукту була вирішена задача визначення позиції пікселів цифрового зображення, в які виконувалося вбудовування ЦВЗ.. Замість використання псевдовипадкової послідовності пікселів для вбудовування бітів цифрового водяного знаку запропоновано використовувати послідовність пікселів, що рівномірно розподілені по всьому зображенню. Рівномірне нанесення ЦВЗ та його десятикратне повторення дозволяють підвищити ефективність захисту цифрового зображення та ефективність вилучення вбудованої інформації не зважаючи на несиметричність процедур вбудовування.

Реалізовано перевірку зображення на наявність ЦВЗ та функціональну можливість викладати зображення з вбудованим ЦВЗ в Інтернет.

**Висновок**

Таким чином, в роботі програмно реалізований метод Куттера–Джордана–Боссена для Windows Phone, використання якого для вбудовування стійкого ЦВЗ знаку у зображення, створені та збережені на мобільному телефоні, значно підвищить ефективність захисту контенту мобільного пристрою.

**Список використаних джерел**


1. Грибунин, В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев; – М : СОЛОН-Пресс, 2002. – 261 с.
2. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю Пузыренко – К.: МК-Пресс, 2006. – 249 с.
3. Кустов, В. Н. Методы встраивания скрытых сообщений / В. Н. Кустов, А. А. Федчук // Защита информации. Конфидент.- 2000.- №3. – С. 34-37.



УДК 681.3


# УДОСКОНАЛЕННЯ АЛГОРИТМУ ЗАГАЛЬНОГО РЕШЕТА ЧИСЛОВОГО ПОЛЯ НА ОСНОВІ ПАРАЛЕЛЬНИХ ОБЧИСЛЕНЬ


**Кінах Я.І.[1)], Якименко І.З.[2)], Лаврик О.П.[3)]**

[1)] *Тернопільський національний технічний університет імені Івана Пулюя, к.т.н., доцент;*
[2)] *Тернопільський національний економічний університет, к.т.н., доцент*
[3)] *Тернопільський національний економічний університет, магістрант*


## І. Постановка задачі

Розробка й впровадження розподілених технологій у практику є актуальною задачею для підвищення рівня захисту інформації [1], раціонального використання інфраструктури установ різного відомчого підпорядкування, взаємодії з службами інших країн, розвитку виробництва засобів захисту інформації.

Головними вимогами до подібних систем є стабільність роботи, швидке відновлення в результаті збоїв програмного та апаратного забезпечення, робота в умовах повільних каналів зв'язку. Ці вимоги особливо ускладнюються у випадку необхідності проведення криптоаналізу в режимі реального часу та при застосуванні паралельних алгоритмів.

Слід зазначити, що стійкість сучасних систем захисту інформації ґрунтується на факторизації багаторозрядних чисел (алгоритм RSA), або на дискретному логарифмуванні (алгоритм Ель-Гамаля, використання математичного апарату еліптичних кривих).

Оскільки деякі методи факторизації можна розпаралелити, зокрема метод загального решета числового поля (ЗРЧП) (основною трудомісткою операцією якого є розв'язування суперрідкої системи лінійних алгебраїчних рівнянь великої розмірності), то розповсюдження персональних комп'ютерів веде до дискредитації системи шифрування RSA. Тому розробка паралельних методів вирішення задачі розв’язку СЛАР дозволить зменшити часову складність алгоритму ЗРЧП.

## II. Мета роботи

Метою досліджень є удосконалення методів паралельних обчислень шляхом скорочення часу криптоаналізу на основі використання алгоритму загального решета числового поля з використання розподілених обчислень.

## III. Паралельний метод розв’язання СЛАР

Розглянемо організацію процесу блокового розпаралелення просторово-розділеного розв'язання СЛАР великої розмірності на аснові прямих декомпозиційних методів, використовуючи викладене в роботах [2, 3, 4].

Розглянемо алгоритмічну структуру, що виникає під час розв’язання СЛАР методом Гауса. Дані представлені у вигляді суперрідкої матриці великої розмірності. Обчислення складаються з наступної послідовності операцій:

- декомпозиція та розподіл даних. Для суперрідких матриць застосовують різні стратегії: пострічкова, поколонкова, блокова. Останню стратегію доцільно [5] застосовувати під час виконання матричних операцій алгоритму ЗРЧП (рисунок 1);

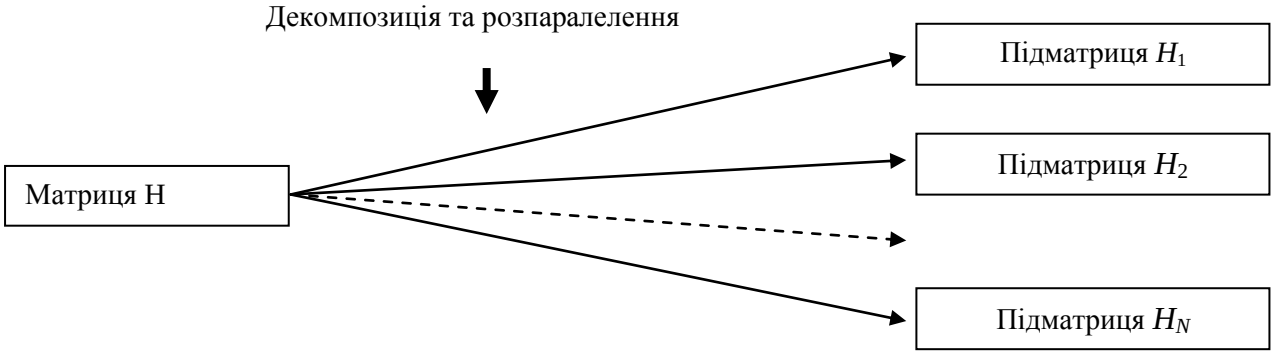


Рисунок 1 - Декомпозиція даних

- обробка кожної підматриці ведеться з використанням матриці звязку;

- обмін міжблоковими даними. На рисунку 2 показана схема взаємодії для матриці H. З метою оптимізації комунікацій до кожного блоку добавляються фіктивні елементи для збереження значень матриці зв’язку.

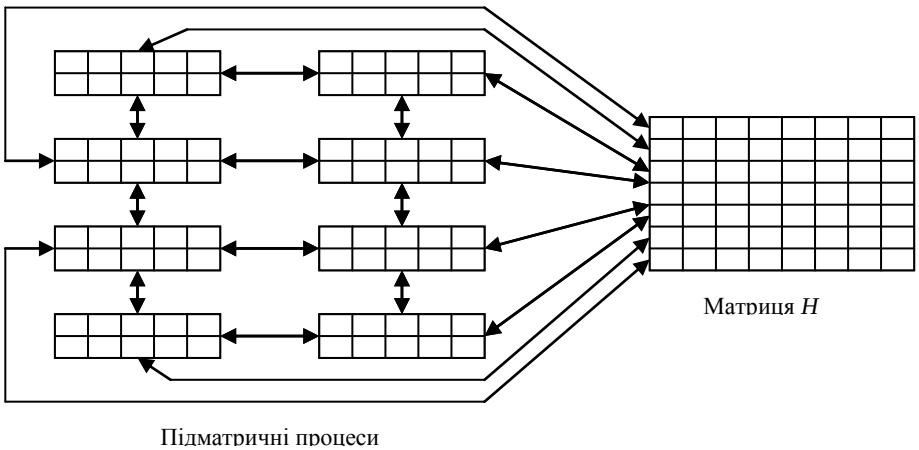


Рисунок 2 - Взаємодія між матричними процесами

- перевірка на завершення. Виконується операція глобальної редукції над маттицею H.

В композиційному плані структура описується діаграмою (рисунок 3)

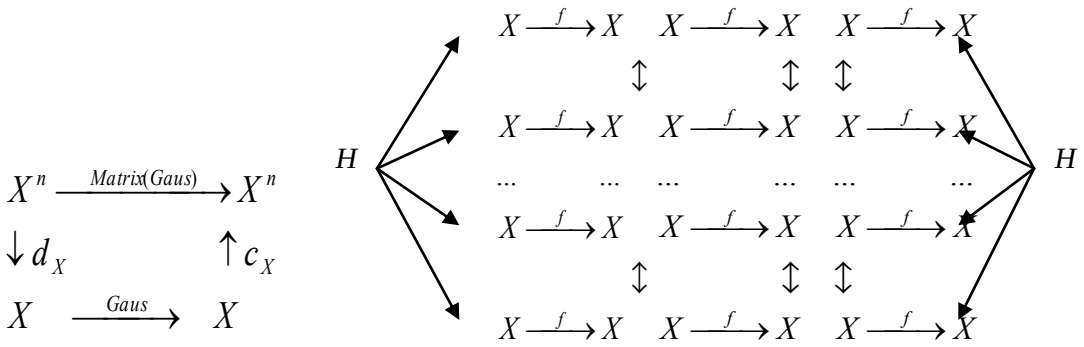


Рисунок 3 - Паралельна обробка матриці H

Розглянемо різні механізми композиції ТАС, що використовуються в процесі розробки паралельних програм. Найпростішим способом побудови паралельних програм є композиція послідовних модулів за допомогою ТАС. Глобальна структура програми цілком визначається алгоритмічною структурою методу ЗРЧП. В ієрархічному плані програма – це дворівневе дерево, в корені якого знаходиться ТАС, а листки дерева сформовані з послідовних модулів – параметрів ТАС.

Таким чином, в найпростішому випадку ТАС виступають в якості операторів композиції або конструкторів, що дозволяють збирати складні програми з послідовних модулів. Використання ТАС в якості єдиного способу композиції накладає жорсткі обмеження на структуру програми.

Якщо функціональні параметри ТАС не лише послідовні модулі, то можна будувати програми з вкладеною ієрархічною структурою. Ієрархічна структура програми – це дерево, в корені котрого знаходиться ТАС, що визначає глобальну структуру програми, нетермінальні вершини складаються з ТАС, листки дерева відповідають послідовним модулям.

Вкладеність ідеально відповідає методу розробки програм “зверху – вниз”, що дозволяє проводити ієрархічну декомпозицію матриці H на окремі підматриці $H_i$.

Отримані за допомогою вищезгаданих механізмів композиції програми, мають спільну рису. В ієрархічному представлені глобальна структура програми та всі її нетермінальні вершини відповідають одиничним ТАС, оскільки всі вони, за винятком послідовних, мають єдину регулярну структуру, що подана деякою ТАС.

Алгоритм ЗРЧП містить послідовні фрагменти. На одному рівні ієрархії програма може містити різні алгоритмічні структури. На практиці поряд з низхідними методами розробки широко застосовують висхідні методи. Тому необхідні додаткові механізми композиції, що дозволяють здійснювати представлення програм у вигляді лінійної композиції ТАС. Розглянемо такі додаткові механізми.

Нехай дано послідовну композицію ТАС. Діаграма для композиції двох ТАС, у яких область значень першої і область визначення другої алгоритмічної структури співпадають (рисунок 4), тобто *TAS(f1): Xn→Zn,TAS(f2): Zn→Yn*, виглядає так:

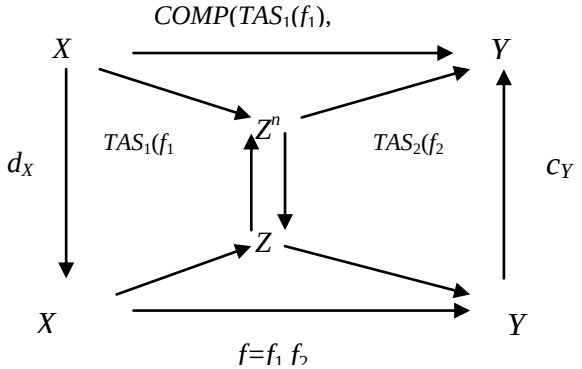


Рисунок 4 - Послідовна композиція двох ТАС

Основною задачею при реалізації керуючих конструкцій методу ЗРЧП є оптимізація інтерфейсу між алгоритмічними структурами, над якими виконується горизонтальна композиція. Зміст задачі полягає у виключені непотрібних етапів збору та декомпозиції проміжних рузультатів.

Модель паралельних обчислень між обчислювальними станціями базується на основі поняття підстановок станів деякої впорядкованої множини. Коли будемо говорити про застосовність правила, то під *(i,j)* будемо розуміти координати елементів матриці M. З поняттям застосовності правила

пов'язане поняття розбиття алгоритму ЗРЧП, де кожній його алгоритмічні структурі відповідає одне значення з деякої множини станів $Q$ [6]:

$$lM=\{((0,0),q_0), ((i_1,j_1),q_1), ..., ((i_m,j_m),q_m)\}. \quad (1)$$

Правилом перетворення $P$ на множині $Z_2 \times Q$ називається підстановка такого виду: $P: l_M \rightarrow r_M$, яка вказує, що множина станів $l_M$ замінюється на множину станів $r_M$.

Застосуванням правила $P$ (або перетворенням $P$) в комірці $(i,j)$ будемо вважати його $(i,j)$-варіацію, яка може бути виражена відображенням $P(i,j)$: $l_M(i,j) \rightarrow r_M(i,j)$.

Для кожного правила природнім чином визначається обернене до нього правило $P^{-1}$: $r_M \rightarrow l_M$ [7]. Для будь-якого правила існує обернене перетворення $P(i,j)^{-1}$: $r_M(i,j) \rightarrow l_M(i,j)$. Відносно $(i,j)$-варіацій операція обернення зберігає комутативність, оскільки від заміни місцями правої і лівої частини правила поняття $(i,j)$-варіації не залежить $(P(i,j))^{-1} = P^{-1}(i,j)$.

Якщо послідовно виконується два правила $P_1(i_1,j_1)$ і $P_2(i_2,j_2)$, то будемо позначати цей факт як композицію варіацій: [40]

$$P_3(i_1,j_1) = P_1(i_1,j_1) * P_2(i_2,j_2). \quad (2)$$

Відповідно, $P_3(i_1,j_1)$ будемо розглядати як варіацію правила $P_3$, яке утворилося в результаті композиції $P_3 = P_1 * P_2(i_2-i_1, j_2-j_1)$,оскільки композиція варіацій правил еквівалентна варіації їх композиції: [41]

$$P(i,j) * R(i,j) = (P * R)(i,j). \quad (3)$$

Обернення композиції варіацій в загальному вигляді [38]:

$$(P(i,j)*R(k,n))^{-1} = R^{-1}(k,n)*P^{-1}(i,j). \quad (4)$$

Такі перетворення можна розглядати як функцію: [41]

$$A(P): \quad QS \rightarrow QR, \quad (5)$$

де $R \subseteq S$ називається областю результату обчислень.

Система правил $P=\{P1, P2, ..., Pn\}$ мінімальна по кількості правил. Система $P$ мінімальна по кількості правил тоді і тільки тоді, коли жодне правило $Pi$ не можна виразити в системі $P\backslash\{Pi\}$. Таким чином, в мінімальній по кількості правил системі немає зайвих правил.

Система правил $P$ мінімальна по об'єму правил, якщо не існує такого правила $Pj$ з шаблоном Mj, який строго включається в шаблон $Mi$ одного з правил $Pi \in P$, і заміна $Pi$ на $Pj$ в системі $P$ не приведе до порушення функції. Цей варіант мінімальності говорить про те, що не можна зменшити обсягти пової алгоритмічної структури. Під загальним поняттям мінімальної системи правил розуміється система, що мінімальна як по кількості, так і по об'єму правил одночасно.

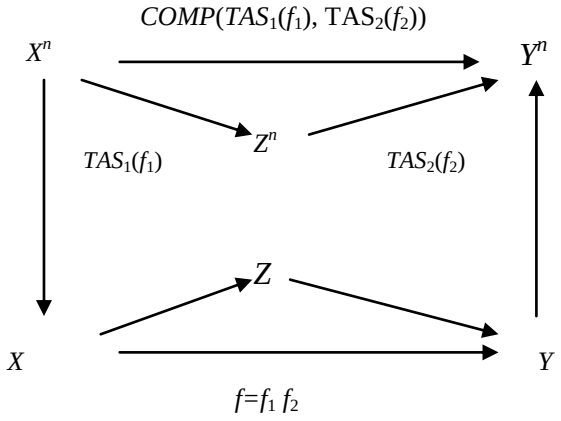


Рисунок 5 - Оптимізовані перетворення криптоалгоритму

Завершувальність системи правил, за звичай, означає, що не існує нескінченної послідовності застосувань правил, які належать даній системі. Якщо стан $QR$ довільної області $R \subseteq S$ в інтерпретувати як деяке число, то коректні типові алгоритмічні структури можна використовувати для арифметичних обчислень. [40]

Нехай дано послідовну композицію двох алгоритмічних структур *COMP(TAS1(f1), TAS2(f2)).* Оскільки *dZ ◦cZ=id*, то з останньої діаграми випливає наступна діаграма оптимізованих перетворень *COMP(TAS1(f1), TAS2(f2)) = TAS2(f2) ◦ TAS1(f1) = cY ◦ f2 ◦ dZ ◦ cZ ◦ f1 ◦ dX*

Для даного випадку легко відшукати набір оптимізуючих правил перетворень, що виключають лишні функції розсилки та збору проміжних результатів.

**Висновок**

У роботі запропоновано повну систему правил оптимізації, що дозволяє уникнути зайвих операцій пересилки даних та виключити обчислення взаємообернених функцій розв'язання суперрідких матриць великої розмірності в задачах криптоаналізу системи RSA з використанням алгоритму загального решета числового поля.

**Список використаних джерел**


1. Романец Ю. В. Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина.// Ю. В. Романец, П. А.Тимофеев, В. Ф. Шаньгин / – М.: Радио и связь, 1999 – 328 с.
2. Закон України «Про інформацію» //ВВР, 1992, № 48, ст. 650.
3. Закон України «Про державну таємницю» //ВВР, 1994, №16, ст. 94.
4. Закон України «Про Національну програму інформатизації» //ВВР, 1998, № 27-28, ст. 181.
5. Стэггерс Н. Історія і тенденції розвитку медичних інформаційних систем у США / (російський переклад).// Н. Стэггерс, Ч. Бэгли Томпсон, Р. Снайдер-Халперн/ – Journal of Nursing Scholarship. – 2001. – № 33. – С. 75–81.



УДК 004.492.2


# МЕТОДИ ЗАХИСТУ РОБОЧИХ СТАНЦІЙ ВІД DDOS-АТАК


**Шпінталь М.Я.[1)], Орловський Н.М.[2)]**

*Тернопільський національний економічний університет*

*[1)] к.т.н., доцент; [2)] магістрант*


## I. Постановка проблеми

Однією з найбільш актуальних задач у сфері послуг надання інформації є забезпечення стабільної роботи і можливості доступу до баз даних у будь-який час. При роботі в такому режимі так само необхідно забезпечення певної міри надійності і стресостійкості системи. Одним з найбільш серйозних і поширених способів атак є DDoS-атака (від англ. Distributed Denial of Service, розподілена атака типу "відмова в обслуговуванні").

Робота присвячена вивченню джерел шкідливого трафіку і їх параметрів, створення моделі мережі підприємства у якій є мережевий фільтр (обробляє запити ззовні), створення алгоритму для відмінності шкідливого трафіку генерованого атакуючими.

## II. Мета роботи

Мета дослідження є підвищення якості фільтрації трафіку від шкідливих навантажень шляхом розробки моделі обробки зовнішніх запитів, що поступають в мережу підприємства, та вдосконалення алгоритмів їх фільтрації.

Завдання:

- аналіз структури і параметрів моделі мережі підприємства;
- дослідження даних отриманих в процесі моделювання для створення алгоритму;
- створення алгоритму фільтрації шкідливого трафіку;
- оцінка ефективності роботи отриманого алгоритму.

## III. Методи захисту від DDoS-атак

Існують при основні рішення захисту від атак: програмні, апаратні, хмарні.

Програмні рішення - найпопулярніші на ринку, вони представляє собою набір засобів фільтрації трафіку, які складені розробником з використання особистого досвіду. Дане рішення досить простим у використанні, але допоможе тільки від малопомітних атак виду вандалізм.

Апаратні рішення - представляють собою створення розподіленої мережевної структури з великим запасом пропускного трафіку. Використовуються в масштабних мережевих структурах, таких як: точки обміну трафіком, дата-центри, великі регіональні провайдери.