УДК 510.52

ОПТИМІЗАЦІЯ БАГАТОРОЗРЯДНОГО МНОЖЕННЯ НА ОСНОВІ ШПФ У ПАРАЛЕЛЬНІЙ МОДЕЛІ ОБЧИСЛЕНЬ

Андрій Терещенко

Розглядається операція багаторозрядного множення у паралельній моделі обчислень, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів. Наведено модифікацію алгоритму реалізації операції множення двох N-розрядних чисел на основі ШПФ та попереднім обчисленням коефіцієнтів ДПФ. У новому алгоритмі операції виконуються над сигналами розрядності N, у противагу стандартному алгоритму, який оперує сигналами розрядністю 2N. Даний алгоритм дозволяє зменшити у два рази кількість задіяних паралельних процесорів, зберігаючи обчислювальну складність для кожного з процесорів, у порівняні зі стандартним алгоритмом. Наведений алгоритм є ефективним також і в послідовній моделі обчислень.

Ключові слова: *паралельна модель обчислень, асиметрична криптографія, багаторозрядна арифметика, багаторозрядне множення, ДПФ, ШПФ.*

Вступ. На даний час мікропроцесорна техніка розвивається дуже швидко. Якщо декілька десятиліть назад кластери з великою кількістю процесорів були доступні тільки потужним фінансовим організаціям для проведення надобчислень, то зараз кластери з кількістю процесорів більше ніж 2000 можливі в домашніх умовах на персональних комп'ютерах на основі графічних прискорювачів. Поряд з подальшим розвитком алгоритмів у послідовній моделі обчислень, необхідних для енергоекономних нешвидких пристроїв, таких як смарткарти, є потреба в розробці нових методів ефективних у паралельній моделі обчислень.

Зрозуміло, що методи ефективні у послідовній моделі обчислень можуть програвати методам у паралельній моделі обчислень. Методи, які мають тісно пов'язані між собою кроки, навіть у паралельній моделі обчислень повинні виконуватися послідовно.

Шляхи оптимізації:

1. Розв'язання пов'язаних кроків за рахунок заміни їх більш простими та однотипними, але непов'язаними операціями, що в більшості випадків збільшує кількість задіяних процесорів, але дає можливість зменшити загальну кількість операцій, виконуваних кожним з паралельних процесорів.

2. Зменшення обсягу (розрядності) оброблюваних даних, що дозволяє зменшити кількість задіяних паралельних процесорів, зберігаючи загальну кількість операцій, виконувану кожним з паралельних процесорів.

3. Динамічний паралелізм [1].

4. Використання резервів оптимізації обчислень(не збільшуючи кількість кроків).

В даній роботі розглядається оптимізація, яка направлена на зменшення розрядності оброблюваних даних у два рази з $2N$ до N, для реалізації операції множення двох N-розрядних чисел на основі ШПФ та передобчислених коефіцієнтах ДПФ.

Постановка задачі. Розглянемо обчислення $R_{2N} = U_N \cdot V_N$, де U_N, V_N – N-розрядні цілі додатні числа, а R_{2N} – $2N$-розрядне число. Такі числа можна представити у вигляді: $U_N = (u_{N-1}u_{N-2}...u_0) = \sum_{i=0}^{N-1} u_i 2^{\omega i}$, $V_N = (v_{N-1}v_{N-2}...v_0) = \sum_{i=0}^{N-1} v_i 2^{\omega i}$, $R_{2N} = (r_{2N-1}r_{2N-2}...r_0) = \sum_{i=0}^{2N-1} r_i 2^{\omega i}$, де ω – довжина машинного слова у бітах (далі будемо вважати ω=16, 24, 32 чи 64 біта), $0 \le u_i, v_i, r_i < 2^{\omega}$.

Необхідно зменшити розрядність оброблюваних даних у два рази з $2N$ до N, при реалізації операції множення двох N-розрядних чисел на основі ШПФ та передобчислених коефіцієнтах ДПФ, побудувати ефективний алгоритм обчислення R_{2N} у паралельній моделі обчислень, знайти кількість однорозрядних операцій виконуваних кожним з паралельних процесорів.

Скорочення та позначення: N-розрядний сигнал – послідовність з N комплексних чисел, дійсна та комплексна чистини яких не перевищують довжини машинного слова у бітах. N-розрядне число можна представити у вигляді N-розрядного сигналу, де комплексна чистина кожного розряду дорівнює нулю, тобто додавання нульової комплексної частини до кожного розряду багаторозрядного числа переводить число у сигнал. Надалі під N-розрядним числом будемо вважати дійсний N-розрядний сигнал, щоб не виділяти окремо операцію представлення багаторозрядного числа у вигляді дійсного багаторозрядного сигналу, та навпаки.

ДПФ – дискретне перетворення Фур'є (в даній роботі термін ДПФ використовується, коли гово-

риться про перетворений сигнал на основі методу ДПФ, тобто надалі слід розуміти як ДПФ сигналу).

ОДПФ – обернене ДПФ.

ШПФ – швидке перетворення Фур'є (швидкий алгоритм обчислення ДПФ сигналу).

ОШПФ – швидкий алгоритм обчислення оберненого ДПФ.

ШПФ-N, ШПФ-$2N$ – алгоритми ШПФ для сигналів різної розрядності N та $2N$.

ДПФ-N, ДПФ-$2N$ – сигнали, перетворені на основі ДПФ, розрядністю N та $2N$.

$X_N, Y_N, Z_N, X_{2N}, Y_{2N}, Z_{2N}$ – вектори-стовпчики з кількістю елементів N та $2N$, відповідно.

$\hat{X}_N, \hat{Y}_N, \hat{Z}_N, \hat{X}_{2N}, \hat{Y}_{2N}, \hat{Z}_{2N}$ – ДПФ сигналів $X_N, Y_N, Z_N, X_{2N}, Y_{2N}, Z_{2N}$, відповідно.

$E(X_{2N}), O(X_{2N}))$ – знаходження парних (*Even*) та непарних (*Odd*) елементів вектора X_{2N}. Нумерація починається з нуля, тому $E(X_{2N})$ повертає елементи з індексами 0, 2, 4, і т.д. $O(X_{2N})$ – елементи з індексами 1, 3, 5, і т.д.

$Z_N \leftarrow X_N \otimes Y_N$ – означає, що результат операції $X_N \otimes Y_N$ записується в елементи вектора Z_N. Зрозуміло, що кількість елементів результату операції та вектора-приймача повинні співпадати.

$E(R_{2N}) \leftarrow T_N$ – елементи T_N записуються в елементи R_{2N} з парними індексами 0, 2, 4, і т.д. Кількість елементів T_N повинна бути в 2 рази меншою за кількістю елементів R_{2N}.

$O(R_{2N}) \leftarrow T_N$ – аналогічно попередньому позначенню, тільки елементи T_N записуються в елементи R_{2N} з непарними індексами 1, 3, 5 і т.п.

$Z_N = X_N \otimes Y_N$ – значення співпадають з обох сторін поелементно.

$W_{2N}^r = e^{-\frac{2\pi i}{2N}r} = e^{-\frac{\pi i}{N}r}$, $r = \overline{0, 2N-1}$; $W_N^r = e^{-\frac{2\pi i}{N}r}$, $r = \overline{0, N/2-1}$.

$W_{N,N}$ – квадратна матриця елементів $W_N^{\langle k \cdot r \rangle_N} = e^{-\frac{2\pi i}{N}k \cdot r}$, $k, r = \overline{0, N-1}$.

Примітка. Для представлення N-розрядного сигналу використовується вектор (вектор-стовбець) з N елементів, кожен з яких є комплексним числом. N-розрядне число записується у вектор з N дійсних елементів.

Базовий алгоритм (ШПФ-$2N$, ДПФ-$2N$) [2]. В даному алгоритмі до N-розрядних чисел додаються N старших нулів. Отримані $2N$-розрядні числа представляється у вигляді дійсних $2N$-розрядних сигналів, які можна використовувати як вхідні параметри у ШПФ. Перехід від N- до $2N$-розрядних чисел та використання ШПФ для сигналів розрядністю $2N$ пояснюється тим, що результатом множення двох N-розрядних чисел буде число розрядністю $2N$.

Алгоритм 1. Множення двох N-розрядних чисел з обчисленням трьох **ШПФ** для сигналів **розрядністю** $2N$, поелементним множенням **ДПФ** сигналів **розрядністю** $2N$ та попереднім обчисленням коефіцієнтів ДПФ у паралельній моделі обчислень.

1. Додавання старших нулів:

$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0$, $r = \overline{0, N-1}$.

2. Обчислення **ШПФ** для сигналів **розрядністю** $2N$: $\hat{X}_{2N} \leftarrow W_{2N.2N} \cdot X_{2N}$, $\hat{Y}_{2N} \leftarrow W_{2N,2N} \cdot Y_{2N}$.

3. Перемноження **ДПФ** сигналів **розрядністю** $2N$: $\hat{Z}_{2N}(r) \leftarrow \hat{X}_{2N}(r) \cdot \hat{Y}_{2N}(r)$, $r = \overline{0, 2N-1}$.

4. Обчислення ОШПФ: $Z_{2N} \leftarrow \frac{1}{2N} \cdot W_{2N.2N} \cdot \hat{Z}_{2N}^*$.

5. Обчислення результату:

$Z_{2N}(r) \leftarrow \mathrm{Re}\, Z_{2N}(r)$, $r = \overline{0, 2N-1}$.

Перед розглядом Леми 1 розглянемо рівні розпаралелювання:

1. Кроки 1, 3, 5 – на рівні розрядів багаторозрядного числа (сигналу).

2. Крок 4 – на рівні кроків ітерації. ШПФ є багатоітераційним алгоритмом, де кожна ітерація має декілька кроків, які можна обчислювати одночасно.

3. Крок 3 – на рівні ШПФ. Два ШПФ обчислюються одночасно для двох вхідних сигналів.

4. Кроки 2, 3, 4 – на рівні обчислення дійних та комплексних частин розрядів сигналів.

Лема 1. Алгоритм 1 множення двох N-розрядних чисел на основі ШПФ для сигналів розрядності $2N$ в паралельній моделі обчислень задіє не більше $2N$ паралельних процесорів на будь-якому кроці, кожний з яких виконає не більше $3 + 2\log_2 N$ комплексних операцій множення.

Доведення. При обчисленні одного перетворення сигналу розрядністю $2N$ на основі ШПФ для сигналів розрядністю $2N$ на кроці 2 та 4 Алгоритму 1 необхідно задіяти в два рази меншу кількість паралельних процесорів, тобто N процесорів, так як достатньо однієї операції комплексного множення для обчислення двох виразів $\pm W_{2N}^r \cdot \hat{X}_{2N}(r)$, які відрізняються лише знаком. Кожний з процесорів буде задіяний на $\log_2 2N = 1 + \log_2 N$ ітераціях. На кроці 2 вхідні сигнали можна обчислювати одночасно, але це потребує додатково N паралельних процесорів. Тобто при одночасному обчисленні двох сигна-

лів на кроці 2 необхідно не більше $2N$ процесорів. Для одночасного перемноження двох ДПФ сигналів розрядністю $2N$ необхідно задіяти $2N$ процесорів, які виконають комплексне множення за один крок. Операції множення на $1/2$, $1/2N$, j, $-j$ не враховуються, так як їх можна замінити операціями зсуву, та обміну між комірками пам'яті. Лема доведена.

Примітка: Для обчислення однієї операції однорозрядного комплексного множення необхідні 4 дійсні однорозрядні операції множення (або 3 операції при використанні оптимізації), тобто для одночасного множення всіх дійсних чисел необхідно не більше $8N$ (або $6N$ з використанням оптимізації) паралельних процесорів. Враховуємо тільки кількість комплексних операцій множення для спрощення подальшого порівняння з алгоритмами наведеними далі. Будемо вважати, що при реалізації базового алгоритму та алгоритмів, наведених надалі, використовуються однакові підходи та методи оптимізації. Тобто кількість резервів оптимізації немає значення, якщо вони використані у всіх методах, які порівнюються, а кількість використаних процесорів наведена для полегшення сприйняття матеріалу для порівняння базового та нового алгоритмів.

1-А оптимізація (ШПФ-N, ДПФ-$2N$). Алгоритм множення двох N-розрядних чисел [3] задіє також не більше $2N$ паралельних процесорів на основі ШПФ для сигналів розрядністю N, але кількість кроків, на яких необхідно виконувати комплексне множення, більша ніж $3+2\log_2 N$ за рахунок додаткових кроків розпакування та пакування.

Далі наводиться алгоритм множення, який дозволяє зменшити кількість операцій, виконуваних кожним з паралельних процесорів, за рахунок спрощення кроків розпакування та пакування алгоритму [3] за кількістю операцій комплексного множення.

Примітка: Кажучи про зменшення кількості комплексних операцій множення маємо на увазі загальну кількість всіх операцій, включаючи операції комплексного додавання, віднімання, обміну елементів, і т.д., так як їх кількість напряму залежить від кількості операцій комплексного множення.

Алгоритм 2. Множення двох N-розрядних чисел з обчисленням трьох **ШПФ** для сигналів **розрядністю** N, поелементним множенням **ДПФ** сигналів **розрядністю** $2N$ та попереднім обчисленням необхідних коефіцієнтів ДПФ у паралельній моделі обчислень.

1. Додавання старших нулів:

$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r = \overline{0, N/2-1}.$$

Обчислення ШПФ для сигналів **розрядністю** N: $E(X_{2N}) + j \cdot O(X_{2N})$, $E(Y_{2N}) + j \cdot O(Y_{2N})$:

$$\hat{X}_N \leftarrow W_{N.N} \cdot (E(X_{2N}) + j \cdot O(X_{2N})),$$
$$\hat{Y}_N \leftarrow W_{N,N} \cdot (E(Y_{2N}) + j \cdot O(Y_{2N})).$$

2. Розпакування сигналу $\hat{X}_N$ в сигнал $\hat{X}_{2N}$:

$$E\hat{X}_N(r) \leftarrow \frac{1}{2}(\hat{X}_N(r) + \hat{X}_N^*(\langle N-r \rangle_N)),$$
$$E\hat{Y}_N(r) \leftarrow \frac{1}{2}(\hat{Y}_N(r) + \hat{Y}_N^*(\langle N-r \rangle_N)),\ r = \overline{0, N-1}. \quad (1)$$

$$O\hat{X}_N(r) \leftarrow (-j) \cdot (\hat{X}_N(r) - E\hat{X}_N(r)),$$
$$O\hat{Y}_N(r) \leftarrow (-j) \cdot (\hat{Y}_N(r) - E\hat{Y}_N(r)),\ r = \overline{0, N-1}. \quad (2)$$

$$\hat{X}_{2N}(r) \leftarrow E\hat{X}_N(r) + W_{2N}^r \cdot O\hat{X}_N(r),$$
$$\hat{Y}_{2N}(r) \leftarrow E\hat{Y}_N(r) + W_{2N}^r \cdot O\hat{Y}_N(r),$$
$$\hat{X}_{2N}(N+r) \leftarrow E\hat{X}_N(r) - W_{2N}^r \cdot O\hat{X}_N(r),$$
$$\hat{Y}_{2N}(N+r) \leftarrow E\hat{Y}_N(r) - W_{2N}^r \cdot O\hat{Y}_N(r),$$
$$W_{2N}^r = e^{-\frac{2\pi i}{2N}r},\ r = \overline{0, N-1}. \quad (3)$$

3. Перемноження **ДПФ** сигналів **розрядністю** $2N$:

$$\hat{Z}_{2N}(r) \leftarrow \hat{X}_{2N}(r) \cdot \hat{Y}_{2N}(r),\ r = \overline{0, 2N-1}. \quad (4)$$

4. Знаходження оберненого сигналу: $Z_{2N} \leftarrow \hat{Z}_{2N}^*$.

5. Пакування сигналу $\hat{Z}_{2N}$ в сигнал $\hat{Z}_N$:

$$E\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (\hat{Z}_{2N}(r) + \hat{Z}_{2N}(N+r)),$$
$$O\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot \frac{1}{W_{2N}^r} \cdot (\hat{Z}_{2N}(r) - \hat{Z}_{2N}(N+r)),$$
$$\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) + j \cdot O\hat{Z}_N(r),\ W_{2N}^r = e^{-\frac{2\pi i}{2N}r},$$
$$r = \overline{0, N-1}. \quad (5)$$

6. Обчислення оберненого сигналу:

$$Z_N \leftarrow \frac{1}{N} \cdot W_{N.N} \cdot \hat{Z}_N.$$

7. Обчислення результату:

$E(Z_{2N}(r)) \leftarrow \mathrm{Re}\, Z_N(N-r-1)$, $O(Z_{2N}(r)) \leftarrow \mathrm{Im}\, Z_N(N-r-1)$, $r = \overline{0, N-1}$.

Пояснення до Алгоритму 2.

Формули (1) та (2) отримані з формул:

$$E\hat{X}_N(r) = \frac{1}{2}(\hat{X}_N(r) + \hat{X}_N^*(\langle N-r \rangle_N)),$$
$$O\hat{X}_N(r) = \frac{1}{2j}(\hat{X}_N(r) - \hat{X}_N^*(\langle N-r \rangle_N)),\ r = \overline{0, N-1}.$$
$$\hat{X}_N(r) = E\hat{X}_N(r) + j \cdot O\hat{X}_N(r),\ r = \overline{0, N-1},$$

де $E\hat{X}_N(r)$ та $O\hat{X}_N(r)$ – ДПФ дійсних сигналів $EX_N(r)$ та $OX_N(r)$, які формують комплексний сигнал $X_N(r) = EX_N(r) + j \cdot OX_N(r)$, $r = \overline{0, N-1}$.

Співвідношення (3) є модифікацією, запропонованою Кулі та Т'юкі [2], яка отримала назву децимації за часом. Зрозуміло, що достатньо однієї операції комплексного множення для обчислення виразів, які відрізняються лише знаком $\pm W_{2N}^r \cdot O\hat{X}_N(r)$.

Вирази для Y отримані аналогічно X. Співвідношення (5) отримані з (3) після заміни X на Z. Зверніть увагу, що на кроці 8 результат отримується в зворотному порядку.

2-А оптимізація (ШПФ-N, ДПФ-$2N$). Операцію знаходження комплексно спряженого сигналу на кроці 5 Алгоритму 2 можна перенести на крок 7 Алгоритму 2 (крок 6 Алгоритму 3).

Алгоритм 3. Множення двох N-розрядних чисел з обчисленням трьох **ШПФ** для сигналів **розрядністю** N, поелементним множенням **ДПФ** сигналів **розрядністю** $2N$ та попереднім обчисленням коефіцієнтів ДПФ.

1-4. Алгоритму 2.

5. Пакування сигналу $\hat{Z}_{2N}$ в сигнал $\hat{Z}_N$:

$$E\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (\hat{Z}_{2N}(r) + \hat{Z}_{2N}(N+r)),$$

$$O\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot \frac{1}{W_{2N}^r} \cdot (\hat{Z}_{2N}(r) - \hat{Z}_{2N}(N+r)),$$

$$\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r),$$

$$W_{2N}^r = e^{-\frac{2\pi i}{2N} r},\ r = \overline{0, N-1}. \qquad (6)$$

6. Обчислення оберненого сигналу: $Z_N \leftarrow \frac{1}{N} \cdot W_{N.N} \cdot \hat{Z}_N^*$.

7. Обчислення результату: $E(Z_{2N}) \leftarrow \mathrm{Re}\, Z_N$, $O(Z_{2N}) \leftarrow \mathrm{Im}\, Z_N$.

Зверніть увагу, що на кроці 5 знак у виразі $\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r)$ змінився, та на кроці 7 результат отримується у звичайному порядку.

3-А оптимізація (ШПФ-N, ДПФ-N). Використаємо (4) у співвідношенні (6):

$$E\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (\hat{X}_{2N}(r) \cdot \hat{Y}_{2N}(r) + \hat{X}_{2N}(N+r) \cdot \hat{Y}_{2N}(N+r)),$$

$$O\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot \frac{1}{W_{2N}^r} \cdot (\hat{X}_{2N}(r) \cdot \hat{Y}_{2N}(r) - \hat{X}_{2N}(N+r) \cdot \hat{Y}_{2N}(N+r)), \qquad (7)$$

$$\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r),\ r = \overline{0, N-1}. \qquad (8)$$

Далі в (7) використаємо (3):

$$E\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (E\hat{X}_N(r) + W_{2N}^r \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) + W_{2N}^r \cdot O\hat{Y}_N(r)) + (E\hat{X}_N(r) - W_{2N}^r \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) - W_{2N}^r \cdot O\hat{Y}_N(r)),$$

$$O\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot \frac{1}{W_{2N}^r} \cdot ((E\hat{X}_N(r) + W_{2N}^r \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) + W_{2N}^r \cdot O\hat{Y}_N(r)) - (E\hat{X}_N(r) - W_{2N}^r \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) - W_{2N}^r \cdot O\hat{Y}_N(r))),$$

$$\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r),\ W_{2N}^r = e^{-\frac{2\pi i}{2N} r},\ r = \overline{0, N-1}.$$

Отримуємо:

$$E\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (E\hat{X}_N(r) \cdot E\hat{Y}_N(r) + (W_{2N}^r)^2 \cdot O\hat{X}_N(r) \cdot O\hat{Y}_N(r)),$$

$$O\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot \frac{W_{2N}^r}{W_{2N}^r} \cdot (E\hat{X}_N(r) \cdot O\hat{Y}_N(r) + E\hat{Y}_N(r) \cdot O\hat{X}_N(r)),$$

$$\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r),\ W_{2N}^r = e^{-\frac{2\pi i}{2N} r},\ r = \overline{0, N-1}.$$

Зробимо заміну $E\hat{Z}_N(r)$ та $O\hat{Z}_N(r)$ в $\hat{Z}_N(r) \leftarrow E\hat{Z}_N(r) - j \cdot O\hat{Z}_N(r)$:

$$\hat{Z}_N(r) \leftarrow \frac{1}{2} \cdot (E\hat{X}_N(r) \cdot E\hat{Y}_N(r) - j \cdot E\hat{X}_N(r) \cdot O\hat{Y}_N(r) - j \cdot E\hat{Y}_N(r) \cdot O\hat{X}_N(r)) + \frac{1}{2} \cdot (W_{2N}^r)^2 \cdot O\hat{X}_N(r) \cdot O\hat{Y}_N(r), W_{2N}^r = e^{-\frac{2\pi i}{2N} r},$$

$r = \overline{0, N-1}$.

Використаємо формули $(E\hat{X}_N(r) - j \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) - j \cdot O\hat{Y}_N(r))$:

$$\hat{Z}_N(r) \leftarrow (-1) \cdot (E\hat{X}_N(r) - j \cdot O\hat{X}_N(r)) \cdot (E\hat{Y}_N(r) - j \cdot O\hat{Y}_N(r)) + O\hat{X}_N(r) \cdot O\hat{Y}_N(r) + (W_N^r)^2 \cdot O\hat{X}_N(r) \cdot O\hat{Y}_N(r), W_{2N}^r = e^{-\frac{2\pi i}{2N} r},$$

$r = \overline{0, N-1}$.

Попередню формулу можна спростити використовуючи (8):

$$\hat{Z}_N(r) \leftarrow \hat{X}_N(r)\cdot\hat{Y}_N(r) + O\hat{X}_N(r)\cdot O\hat{Y}_N(r) + (W_{2N}^r)^2\cdot O\hat{X}_N(r)\cdot O\hat{Y}_N(r),\quad W_N^r = e^{-\frac{2\pi i}{N}r},\ r=\overline{0,N-1}, \tag{9}$$

де $\hat{X}_N(r) = E\hat{X}_N(r) - j\cdot O\hat{X}_N(r)$, $\hat{Y}_N(r) = E\hat{Y}_N(r) - j\cdot O\hat{Y}_N(r)$, $r=\overline{0,N-1}$.

Зрозуміло, що комплексні сигнали X_N та Y_N повинні формуватися по-іншому для отримання (9):

$$X_N(r) \leftarrow EX_N(r) - j\cdot OX_N(r),\ Y_N(r) \leftarrow EY_N(r) - j\cdot OY_N(r),\ r=\overline{0,N-1}.$$

Після групування (9) отримуємо:

$$\hat{Z}_N(r) \leftarrow \hat{X}_N(r)\cdot\hat{Y}_N(r) + (1+(W_{2N}^r)^2)\cdot O\hat{X}_N(r)\cdot O\hat{Y}_N(r),\ W_{2N}^r = e^{-\frac{2\pi i}{2N}r},\ r=\overline{0,N-1}. \tag{10}$$

З врахуванням (10) Алгоритм 3 можна записати наступним чином.

Алгоритм 4. Множення двох N-розрядних чисел з обчисленням трьох **ШПФ** для сигналів **розрядністю** N, поелементним множенням **ДПФ** сигналів **розрядністю** N та попереднім обчисленням коефіцієнтів ДПФ у паралельній моделі обчислень.

1. Додавання старших нулів:

$$X_{2N}(N+r) \leftarrow Y_{2N}(N+r) \leftarrow 0,\ r=\overline{0,N/2-1}.$$

2. Обчислення ШПФ для сигналів **розрядністю** N: $E(X_{2N}) - j\cdot O(X_{2N})$, $E(Y_{2N}) - j\cdot O(Y_{2N})$:

$$\hat{X}_N \leftarrow W_{N.N}\cdot(E(X_{2N}) - j\cdot O(X_{2N})),$$

$$\hat{Y}_N \leftarrow W_{N,N}\cdot(E(Y_{2N}) - j\cdot O(Y_{2N})).$$

3. Обчислення ДПФ непарних елементів сигналів X_{2N} та Y_{2N}:

$$O\hat{X}_N(r) \leftarrow (-j)\cdot\frac{1}{2}\cdot(\hat{X}_N(r) - \hat{X}_N^*(\langle N-r\rangle_N)),$$

$$O\hat{Y}_N(r) \leftarrow (-j)\cdot\frac{1}{2}(\hat{Y}_N(r) - \hat{Y}_N^*(\langle N-r\rangle_N)),\ r=\overline{0,N-1}.$$

4. Обчислення **ДПФ** сигналів **розрядністю** N:

$$\hat{Z}_N(r) \leftarrow \hat{X}_N(r)\cdot\hat{Y}_N(r) + (1+(W_{2N}^r)^2)\cdot O\hat{X}_N(r)\cdot O\hat{Y}_N(r),$$

$$W_{2N}^r = e^{-\frac{2\pi i}{2N}r},\ r=\overline{0,N-1}.$$

5. Обчислення оберненого сигналу:

$$6.\quad Z_N \leftarrow \frac{1}{N}\cdot W_{N.N}\cdot\hat{Z}_N^*.$$

7. Обчислення результату: $E(Z_{2N}) \leftarrow \mathrm{Re}\,Z_N$, $O(Z_{2N}) \leftarrow \mathrm{Im}\,Z_N$.

Примітка: Для отримання коректного результату при зміні знаку (з мінуса на плюс) на кроці 2 Алгоритму 4 крок 5 буде виглядати складніше, де додатково необхідно знати $E\hat{X}_N$ та $E\hat{Y}_N$:

$$\hat{Z}_N(r) \leftarrow 2\cdot E\hat{X}_N(r)\cdot E\hat{Y}_N(r) - \hat{X}_N(r)\cdot\hat{Y}_N(r) + $$
$$+((W_{2N}^r)^2 - 1)\cdot O\hat{X}_N(r)\cdot O\hat{Y}_N(r),$$
$$W_{2N}^r = e^{-\frac{2\pi i}{2N}r},\ r=\overline{0,N-1}.$$

Лема 2. Алгоритм 4 в паралельній моделі обчислень задіє не більше N паралельних процесорів на будь-якому кроці, кожний з яких виконає не більше $2+2\log_2 N$ комплексних операцій множення.

Доведення. Вважаємо, що кількість доступних паралельних процесорів достатня для виконання необхідної кількості операцій комплексного множення на кожному кроці. При обчисленні одного перетворення сигналу довжини N на основі ШПФ довжини N на кроках 2 та 5 задіяти в два рази меншу кількість паралельних процесорів, тобто $N/2$, так як достатньо однієї операції комплексного множення для обчислення двох виразів $\pm W_N^r\cdot\hat{X}_N(r)$, які відрізняються лише знаком. На кроці 2 вхідні сигнали обчислюються одночасно, що потребує $N/2$ додаткових паралельних процесорів. Тобто при одночасному обчисленні двох сигналів на кроці 2 необхідно не більше N процесорів. Кожний з процесорів виконає $\log_2 N$ комплексні операції множення на кожному кроці, виконуючи $2\log_2 N$ операції на кроках 2 та 5. Обчислення $\hat{X}_N(r)\cdot\hat{Y}_N(r)$ та $O\hat{X}_N(r)\cdot O\hat{Y}_N(r)$, $r=\overline{0,N-1}$, виконуються одночасно на N процесорах. $(1+(W_{2N}^r)^2)$, виконується після обчислення $O\hat{X}_N(r)\cdot O\hat{Y}_N(r)$. Тому для завершення кроку 4 необхідно 2 операції комплексного множення, виконані кожним з паралельних процесорів. Операції множення на $1/2$, $1/N$, j, $-j$ не враховуються, аналогічно Лемі 1. Лема доведена.

Переваги алгоритму 4 у порівнянні з алгоритмами 2, 3 та [3, 4]. Кроки пакування та розпакування виключені за рахунок введення доданку $(1+(W_{2N}^r)^2)\cdot O\hat{X}_N(r)\cdot O\hat{Y}_N(r)$ на кроці 4.

З врахуванням того, що $O\hat{X}_N(r)$ та $O\hat{Y}_N(r)$, $r=\overline{0,N-1}$ – ДПФ дійсних сигналів, достатньо $N/2+1$ (замість N) операцій комплексного множення для отримання $O\hat{X}_N(r)\cdot O\hat{Y}_N(r)$, $r=\overline{0,N-1}$. Це дає можливість зменшити ще на $N/2-1$ опе-

рацій комплексного множення, розглядаючи додатково Лему 2.

Для множення двох 4-розрядних чисел, використовуючи Алгоритм 4, необхідно передобчислити 6 значень: W_4^r, $r=\overline{0,1}$ $(1,-j)$; $1+(W_8^r)^2$, $r=\overline{0,3}$, $(2,0,1-j,1+j)$. Після біт-інверсного упорядкування отримуємо: $(1,-j)$ та $(2,1-j,0,1+j)$, відповідно. Тобто, при множенні двох 4-розрядних чисел на основі Алгоритму 4 немає потреби використовувати операції з плаваючою комою.

Послідовна модель обчислень. Лема 3. Кількість операцій комплексного множення Алгоритму 4 становить $3N\cdot(1+\log_2 N)$ у послідовній моделі обчислень.

Доведення. Кількість операцій комплексного множення на кроках 2, 5 становить $3N\cdot\log_2 N$. На кроці 4 необхідно $3N$ множення. Значення $1+(W_{2N}^r)^2$, $r=\overline{0,N-1}$, можна обчислити до початку алгоритму, так як вони залежать тільки від N. Операції множення на $1/2$, $1/N$, j, $-j$ не враховуються, аналогічно Лемі 1. Лема доведена.

Порівняльний аналіз у послідовній моделі обчислень.

Таблиця 1

Порівняльний аналіз Алгоритмів 2, 3, 4 з базовим Алгоритмом 1

Алгоритм	*Коефіцієнт прискорення*
Алгоритм 2	0,85
Алгоритм 3	1,11
Алгоритм 4	0,53

Примітка: Алгоритм 4 майже у два рази ефективніший Алгоритму 1.

Алгоритм 4 обчислює тільки N-розрядні сигнали у порівнянні з Алгоритмами 1, 2, 3, які обчислюють $2N$-розрядні сигнали (Алгоритм 1), або виконується перехід до $2N$-розрядних сигналів (Алгоритм 2, 3).

Висновки. В даній роботі наведено модифікацію алгоритму, який реалізує операцію множення двох N-розрядних чисел на основі ШПФ та передобчисленими коефіцієнтами ДПФ у паралельній моделі обчислень. Наведена модифікація дозволяє зменшити у два рази кількість задіяних паралельних процесорів за рахунок виконання операцій тільки над N-розрядними сигналами замість використання $2N$-розрядних сигналів у порівнянні зі стандартним метод (Алгоритм 1). Алгоритм 4 є також ефективним у послідовній моделі обчислень. Наведені переваги Алгоритму 4 у порівнянні з алгоритмами 2, 3 та [3, 4]. Розроблено програми FFTMainComplex2NEven, FFTMainComplex2NEven2, FFTMainComplex2NEven 8a, які реалізують Алгоритми 2, 3, 4 відповідно, на мові програмування APL.

ЛИТЕРАТУРА

[1]. Задирака В.К. О требованиях к параллельной обработке данных в спецпроцессоре БПФ // Оптимизация алгоритмов и программного обеспечения ЭВМ. – Киев.: Ин-т кибернетики им. В.М. Глушкова АН УССР, 1985. – С. 3–10.

[2]. Задірака В., Олексюк О. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання. – Київ. – 2003. – 263 с.

[3]. Терещенко А.Н. Умножение больших N-разрядных чисел с вычислением только N-разрядных ДПФ // Компьютерная математика. – 2008. – № 1. – С. 122–130.

[4]. Терещенко А.Н., Задирака В.К. Оптимизация умножения больших N-разрядных чисел на основе N-разрядных ДПФ // Проблеми програмування. – 2012. – № 4. – С. 116–130.

REFERENCES

[1]. Zadiraka V.K. (1985) «About requirements for parallel data processing in FFT processor» Algorithm and computer software optimization, Kyiv.: V.M. Glushkov Institute of Cybernetics of NAS of Ukraine, P. 3-10.

[2]. Zadiraka V., Oleksyuk O. (2003) «Computer multidigit arithmetic: Naukove vidanya», Kyiv, 263 p.

[3]. Tereshchenko A.N. (2008) «Multiplication of big numbers of the length of N with computing only DTF of the length of N», Computer mathematics, № 1, P. 122-130.

[4]. Tereshchenko A.N., Zadiraka V.K. (2012) «Optimization of big numbers of the length of N multiplication based on DTF of the length of N», Programming problems, № 4, P. 116-130.

ОПТИМІЗАЦІЯ БАГАТОРОЗРЯДНОГО МНОЖЕННЯ НА ОСНОВІ ШПФ У ПАРАЛЕЛЬНІЙ МОДЕЛІ ОБЧИСЛЕНЬ

Розглядається операція багаторозрядного множення для паралельної моделі обчислень, від швидкодії якої залежить швидкодія асиметричних криптографічних програмно-апаратних комплексів. Наведено модифікацію алгоритму реалізації операції множення двох N-розрядних чисел на основі ШПФ та попереднім обчисленням коефіцієнтів ДПФ. У новому алгоритмі операції виконуються над сигналами розрядності N, у противагу стандартному алгоритму, який оперує сигналами розрядністю 2N. Даний алгоритм дозволяє зменшити у два рази кількість задіяних паралельних процесорів, зберігаючи обчислювальну складність для кожного з процесорів, у порівняні зі стандартним алгоритмом. Наведений алгоритм є ефективним також і в послідовній моделі обчислень.

Ключові слова: паралельна модель обчислень, асиметрична криптографія, багаторозрядна арифметика, багаторозрядне множення, ДПФ, ШПФ.

OPTIMIZATION OF MULTI-DIGIT MULTIPLICATION BASED ON FFT IN PARALLEL COMPUTATIONAL MODEL

It is considered the operation of multi-digit multiplication for parallel computational model, that has biggest influence on performance of asymmetric cryptographic computer systems. It is given modification of N-digit multiplication algorithm based on FFT and DTF`s coefficients previously computed. New algorithm operates with multi-digits of the length of N, contrary to standard algorithm that uses multi-digits of the length of 2N. Algorithm reduces in two times the number of used parallel processors keeping the same computational complexity of each processor in comparison with standard algorithm. Given algorithm is also efficient in sequential computational model.

Key words: parallel computational model, asymmetric cryptography, multidigit arithmetic, multidigit multiplication, DFT, FFT.

Терещенко Андрій Миколайович, кандидат фізико-математичних наук, старший інженер-програміст ТОВ «СімКорп – Україна».
E-mail: teramidi@ukr.net
Терещенко Андрей Николаевич, кандидат физико-математических наук, старший инженер-программист ООО «СимКорп – Украина».
Tereshchenko Andrii, Ph.D in physics and mathematics Senior software developer LLC «SimCorp – Ukraine».

УДК 511.512

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС ВРС АЛГОРИТМА ПОТОЧНОГО ШИФРОВАНИЯ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ ВИДЕОСИГНАЛОВ, ПЕРЕДАВАЕМЫХ С БОРТА БПЛА

Анатолий Белецкий, Артем Максименко, Денис Навроцкий, Анастасия Свердлова, Александр Семенюк

Поточный ВРС (Block Packet Cipher) алгоритм ориентирован на криптографическую защиту и помехоустойчивое кодирование дискретной видеоинформации, передаваемой с Борта подвижного летательного аппарата на Землю. Шифрование осуществляется поразрядным сложением по модулю 2 блоков исходного текста, размер которых составляет 128, 256, 512 или 1024 бит, с равными по длине блоками двоичных псевдослучайных чисел (ключами, или гаммами). Потоки гамм, синхронно генерируемых как на Борту, так и на Земле, вырабатываются совокупностью криптографических преобразований (примитивов) секретного базового общего ключа, загружаемого на этапе предполетного обслуживания в бортовую и наземную аппаратуру шифрования. Помехоустойчивое кодирование блоков зашифрованных видеосигналов осуществляется одним из трех алгоритмов: Хемминга, БЧХ или Рида-Соломона. Совокупность блоков данных, число которых пропорционально размеру гаммы, образует пакет зашифрованной информации. Переходу к формированию очередного пакета предшествует преобразование общего ключа шифрования, который в свою очередь управляет параметрами блочных ключей (функций гаммирования). Моделирующий комплекс допускает возможность исключения или модификации одного или нескольких примитивов, принимающих участие в образовании шифрующих гамм.

Ключевые слова: *криптографические примитивы, поточные шифры, программно-моделирующий комплекс.*

I. Введение и постановка задачи.

Беспилотные летательные аппараты (БПЛА) в настоящее время составляют основу авиации специального применения. БПЛА используются для патрулирования границ, аэрофотосъемки, разведки геофизическими методами, контроля радиационного фона, а также для сбора различной информации по заявкам гражданских и военных ведомств. Из приведенного краткого, но неуклонно расширяющегося списка областей применения БПЛА однозначно вытекает, как следствие, необходимость обеспечения надлежащей криптографической защиты каналов передачи данных между летательным аппаратом, именуемым также для краткости как «Борт», и наземным пунктом управления (НПУ), который иначе будем обозначать термином «Земля». Пренебрежение такой защитой чревато опасностью несанкционированного вмешательства противника в канал управления БПЛА, что может привести к захвату аппарата.

К важнейшим видам информации, которыми обмениваются Борт и Земля, относятся командная, телеметрическая и видеоинформация [1-3].