УДК 519.6:519.712.3:510.52

О. М. Богданов, Я. В. Зінченко
Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України «КПІ»
вул. Московська, 45/1, 01011 Київ, Україна

Методи зменшення часу реалізації операції множення надвеликих чисел для системи захисту інформації

Для підвищення швидкодії асиметричних криптографічних систем розроблено методи зменшення часу реалізації операції множення надвеликих чисел. Указані методи базуються на застосуванні математичного апарату вейвлет-перетворень і, в порівнянні з відомими методами, дозволяють суттєво зменшити обчислювальну складність операції множення багаторозрядних чисел.

Ключові слова: *асиметричні криптографічні системи, надвеликі числа, вейвлет-перетворення.*

У більшості асиметричних криптографічних систем захисту інформації при шифруванні, дешифруванні і генерації ключів основною є операція модулярного зведення в ступінь, яка являє собою багаторазове виконання операції множення за модулем простого числа чи добутку простих чисел. З метою забезпечення необхідної практичної криптостійкості зазначених систем, розмірності модулів для них вибираються рівними 512…2048 бітам і більше. Оскільки ж процесори сучасних універсальних ПЕОМ не спеціалізовані на багаторозрядну арифметику, то обчислення ними добутків надвеликих чисел «стовпчиком» (складність цього традиційного методу порядку m^2, де m — довжина числа в бітах) вимагає істотних часових витрат, що обумовлює низьку швидкість роботи програмних реалізацій асиметричних криптосистем.

Одним із основних рішень проблеми підвищення швидкодії програмних реалізацій асиметричних криптосистем є застосування спеціальних методів множення надвеликих чисел [1]. На сьогоднішній день розроблена досить велика кількість таких методів, кожен з яких має свою область ефективного застосування в залежності від області значень m, моделі обчислень, програмної чи апаратної реалізації. Усі ці методи є рекурсивними і засновані на зведенні множення m-розрядних чисел до послідовності множень чисел з меншою кількістю розрядів. При їх практичній реалізації m-розрядні двійкові числа, що перемножуються, на-

приклад u і v, представляються як масиви l-бітних слів $(u_1, u_2, u_3, \ldots, u_K)$ та $(v_1, v_2, v_3, \ldots, v_K)$, де K — кількість l-бітних блоків у числах. Довжина блоку дорівнює розрядності процесора використовуваної ЕОМ.

Асимптотично найшвидшим з відомих методів є метод Шенхаге-Штрассена [1, 2]. Він заснований на ідеї використання теореми про дискретну згортку двох функцій і дозволяє помножити два m-розрядних двійкових числа за $m \log m \log\log m$ кроків (бітових операцій). Оскільки дискретна згортка дає основний внесок в оцінку складності методу, то для ефективного її обчислення використовується алгоритм швидкого перетворення Фур'є (ШПФ). Однак, використання для обчислення добутків надвеликих чисел алгоритму ШПФ пов'язане з деякими обчислювальними труднощами, оскільки цей алгоритм розроблений для поля комплексних чисел, а перемножуються цілі багаторозрядні числа. До таких труднощів варто віднести витрати машинного часу на обчислення тригонометричних функцій, а також боротьбу з помилками заокруглення при обчисленні тригонометричних функцій виду $W_N = e^{-i2\pi/N}$.

Авторами пропонуються два методи зменшення часу реалізації операції множення надвеликих чисел. Перший — це модифікація методу, який був запропонований у роботі [3]. Сутність модифікації полягає в заміні операції обчислення коефіцієнтів Уолша з використанням швидкого перетворення Уолша (ШПУ) на операцію обчислення цих коефіцієнтів із використанням швидкого перетворення Хаара (ШПХ). У порівнянні з запропонованим у [3] модифікований метод дозволяє зменшити час виконання операції множення надвеликих чисел за рахунок скорочення кількості додавань, необхідних для її реалізації. Другий метод є самостійним методом авторів і заснований на використанні вейвлетів Хаара для ефективного обчислення дискретної згортки без переходу в поле комплексних чисел. На відміну від відомих, розроблений метод дозволяє зменшити час виконання операції множення надвеликих чисел за рахунок скорочення кількості множень, необхідних для її реалізації. Розглянемо запропоновані методи по-порядку.

З [3] відомо, що загальна кількість додавань, які необхідні для обчислення циклічної згортки двох послідовностей x та y довжиною $N = 2^n$ (згортка дає основний внесок в оцінку складності методу множення великих чисел), дорівнює:

$$\begin{aligned} Q_{\Sigma}^{+} &= Q_1^{+} + Q_2^{+} + Q_3^{+} = \\ &= n \cdot 2^{n+1} + 4\left(3^{n-1} - 2^{n-1}\right) + 3^{n+1} - 3{,}5 \cdot 2^n = 13 \cdot 3^{n-1} + 2^{n+1}\left(n - 2{,}75\right), \end{aligned} \tag{1}$$

де $Q_1^{+} = n \cdot 2^{n+1}$ — кількість додавань, необхідних для виконання кроку 1 алгоритму (обчислення коефіцієнтів Уолша F^x та F^y вихідних послідовностей x та y з використанням ШПУ); $Q_2^{+} = 4\left(3^{n-1} - 2^{n-1}\right)$ — кількість додавань, необхідних для виконання кроку 2 алгоритму (обчислення вектора лінійних комбінацій з коефіцієнтів F^x та F^y); $Q_3^{+} = \left(3^{n+1} - 3{,}5 \cdot 2^n\right)$ — кількість додавань, необхідних для виконання кроку 3 алгоритму (обчислення коротких згорток).

Оптимізація алгоритму обчислення циклічної згортки за кількістю додавань можлива за рахунок мінімізації кількості додавань при виконанні кроку 1.

Відомо [4], що кількість додавань, необхідних для обчислення коефіцієнтів Уолша та Хаара векторів довжиною $N = 2^n$ з використанням швидких алгоритмів, дорівнює $n \cdot 2^n$ та $2\left(2^n - 1\right)$ відповідно. З приведених нижче співвідношень, які пов'язують перетворення Уолша та Хаара, випливає, що перетворення Уолша можна замінити перетворенням Хаара. Останнє забезпечує економію кількості додавань (при $N = 2^n = 256$ приблизно в чотири рази) і, відповідно, більш високу швидкість обчислень. Ці співвідношення дають сімейство ортогональних перетворень, яке включає перетворення Уолша та Хаара. До цих перетворень відноситься один загальний алгоритм швидкого обчислення.

Відповідно до [5] позначимо матриці Хаара $\left[H_2^n\right]$ й Уолша-Адамара $\left[W_2^n\right]$ порядку 2^n, рядки яких являють собою 2^n функцій Хаара й Уолша, нормованих на $1/\sqrt{2^n}$; розіб'ємо матриці $\left[H_2^n\right]$ і $\left[W_2^n\right]$ на $(n+1)$ прямокутних підматриць $\left[MH_{2^n}^k\right]$ і $\left[MW_{2^n}^k\right]$ розміром $\left(2^n \times 2^{k-1}\right)$, $k = 1, ..., n$. Матриця $\left[MH_{2^n}^0\right]$ являє собою перший рядок H^0, матриця $\left[MW_{2^n}^0\right]$ являє собою перший рядок W^0, а матриці $\left[MH_{2^n}^k\right]$ і $\left[MW_{2^n}^k\right]$ формуються з функцій Хаара й Уолша рангу r, причому $2^{k-1} \le r < 2^k$. Матриці $\left[H_2^n\right]$ і $\left[W_2^n\right]$, а також підматриці $\left[MH_{2^n}^k\right]$ і $\left[MW_{2^n}^k\right]$ представлені на рис. 1.

$$\left\{\begin{array}{rcccccccc}
H_0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
H_1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
H_2 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\
H_3 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\
H_4 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\
H_5 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\
H_6 & 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\
H_7 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2
\end{array}\right.
\begin{array}{l}
\left.\begin{array}{l} \\ \end{array}\right\}\left[MH_3^0\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MH_3^1\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MH_3^2\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MH_3^3\right]
\end{array}$$

Матриця Хаара порядку 2^n

$$\left\{\begin{array}{rcccccccc}
W_0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
W_1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
W_2 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
W_3 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
W_4 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
W_5 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
W_6 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
W_7 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1
\end{array}\right.
\begin{array}{l}
\left.\begin{array}{l} \\ \end{array}\right\}\left[MW_3^0\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MW_3^1\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MW_3^2\right] \\
\left.\begin{array}{l} \\ \end{array}\right\}\left[MW_3^3\right]
\end{array}$$

Матриця Уолша-Адамара порядку 2^n

Рис. 1. Матриці і підматриці Хаара й Уолша-Адамара

Між підматрицями $\left[MH_{2^n}^k\right]$ й $\left[MW_{2^n}^k\right]$ існує матричне співвідношення, яке їх зв'язує [6]:

$$\left[MW_{2^n}^k\right] = \left[W_{2^{k-1}}\right] \cdot \left[S_{2^{k-1}}\right] \cdot \left[MH_{2^n}^k\right], \quad k = 1, ..., n, \tag{2}$$

де $\left[W_{2^{k-1}}\right]$ — упорядкована матриця Уолша-Адамара порядку 2^{k-1}, а $\left[S_{2^{k-1}}\right]$ — матриця перестановок порядку 2^{k-1}.

Оскільки $\left[W_{2^{k-1}}\right]$ і $\left[S_{2^{k-1}}\right]$ симетричні й ортогональні, то є можливість одержати зворотне співвідношення:

$$\left[MH_{2^n}^{k}\right] = \left[W_{2^{k-1}}\right] \cdot \left[S_{2^{k-1}}\right] \cdot \left[MW_{2^n}^{k}\right], \quad k = 1, \ldots, n. \tag{3}$$

У роботі [7] доводиться справедливість виразів (2) і (3) та визначаються співвідношення, що зв'язують перетворені вектори $V_w\left(V_{w_0}, V_{w_1}, \ldots, V_{w_{2^{n-1}}}\right)$ й $V_H\left(V_{H_0}, V_{H_1}, \ldots, V_{H_{2^{n-1}}}\right)$, які відповідають вихідному вектору V.

Помноживши праві частини виразів (2) і (3) на вектор V, одержимо:

$$\begin{pmatrix} V_{w_{2^{k-1}}} \\ . \\ V_{w_{2^{k-1}}} \end{pmatrix} = \left[W_{2^{k-1}}\right] \cdot \left[S_{2^{k-1}}\right] \cdot \begin{pmatrix} V_{H_{2^{k-1}}} \\ . \\ V_{H_{2^{k-1}}} \end{pmatrix}, \tag{4}$$

$$\begin{pmatrix} V_{H_{2^{k-1}}} \\ . \\ V_{H_{2^{k-1}}} \end{pmatrix} = \left[W_{2^{k-1}}\right] \cdot \left[S_{2^{k-1}}\right] \cdot \begin{pmatrix} V_{w_{2^{k-1}}} \\ . \\ V_{w_{2^{k-1}}} \end{pmatrix}. \tag{5}$$

Набори коефіцієнтів перетворених векторів, що з'являються у виразах (4) і (5), називаються зонами. Із співвідношень видно, що зона перетвореного вектора V_H визначає відповідну зону перетвореного вектора V_w. Ця властивість показує, що якщо вектор V апроксимується деякою підмножиною зон перетворених векторів V_H і V_w чи, зокрема, якщо ці вектори усікаються наприкінці зони, то після зворотних перетворень виходить вихідний наближений вектор V.

У співвідношеннях (4) і (5) відповідні зони зв'язані ортогональними перетвореннями. З теореми Парсеваля випливає, що енергії відповідних зон перетворених векторів однакові.

На рис. 2 наведено схему алгоритму швидкого обчислення перетворення Хаара 8-го порядку. Згідно [7], повторне застосування співвідношення (4) дозволяє одержати з цієї схеми схему алгоритму швидкого обчислення перетворення Уолша 8-го порядку, представлену на рис. 3. Пунктирними лініями обведені перетворення Уолша нижчих порядків, після яких здійснюються перебудови матриць $[S]$.

Таким чином, застосування співвідношень (2) і (3) призводить до того, що перетворення Хаара діє так само, як і перетворення Уолша, а кількість додавань, необхідних для обчислення коефіцієнтів Уолша послідовності довжини $N = 2^n$, зменшується на величину $n \cdot 2^n - 2\left(2^n - 1\right) = n \cdot 2^n - 2^{n+1} + 2$. З урахуванням того, що в алгоритмі (1) обробляються дві послідовності (x і y), і для кожної з них виходить зазначений виграш, загальне зменшення кількості додавань складе

$n \cdot 2^{n+1} - \left(2^{n+2} - 4\right) = 2^{n+1}(n-2) + 4$. Загальна кількість додавань, необхідних для обчислення циклічної згортки модифікованим алгоритмом, буде дорівнювати:

$$\begin{aligned} Z_{\Sigma}^{+} &= Z_1^{+} + Z_2^{+} + Z_3^{+} = \\ &= 2^{n+2} - 4 + 4\left(3^{n-1} - 2^{n-1}\right) + 3^{n+1} - 3{,}5 \cdot 2^{n} = 13 \cdot 3^{n-1} - 1{,}5 \cdot 2^{n} - 4, \end{aligned} \tag{6}$$

де $Z_1^{+} = \left(2^{n+2} - 4\right)$ — кількість додавань, необхідних для виконання кроку 1 алгоритму (обчислення коефіцієнтів Уолша F^x та F^y вихідних послідовностей x і y з використанням ШПХ); $Z_2^{+} = Q_2^{+} = 4\left(3^{n-1} - 2^{n-1}\right)$ — кількість додавань, необхідних для виконання кроку 2 алгоритму (обчислення вектора лінійних комбінацій з коефіцієнтів F^x та F^y); $Z_3^{+} = Q_3^{+} = \left(3^{n+1} - 3{,}5 \cdot 2^{n}\right)$ — кількість додавань, необхідних для виконання кроку 3 алгоритму (обчислення коротких згорток).

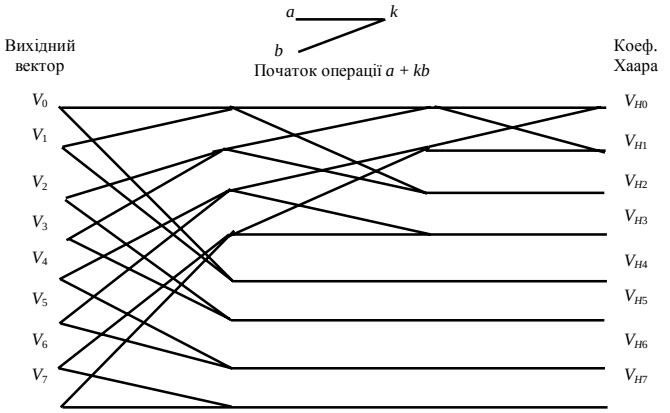

Рис. 2. Схема алгоритму швидкого обчислення перетворення Хаара

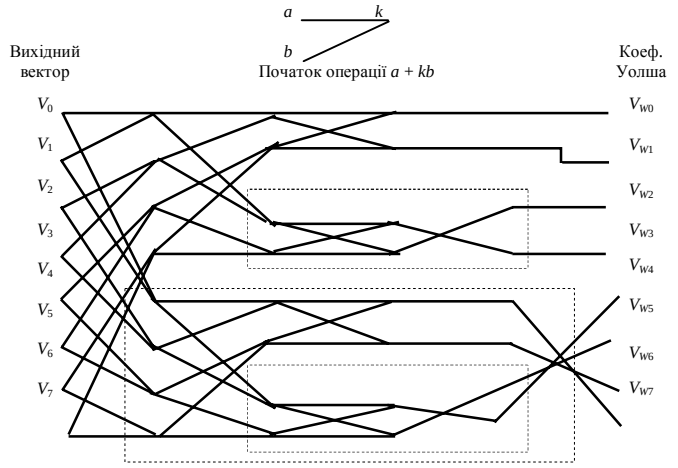

Рис. 3. Схема алгоритму швидкого обчислення перетворення Уолша

Результати порівняння вихідного (1) і модифікованого (6) алгоритмів приведені в зведеній табл. 1, яка містить кількість додавань, необхідних для обчислення циклічної згортки кожним з них. Аналіз таблиці показує, що для обчислення циклічної згортки по вихідному алгоритму (1) необхідне виконання більшої кількості операцій додавання, ніж по модифікованому алгоритму (6).

Таблиця 1. Складність алгоритмів обчислення циклічної згортки

n	Q_1^+	Q_2^+	Q_3^+	Q_Σ^+	Z_1^+	Z_2^+	Z_3^+	Z_Σ^+	Економія кількості додавань
10	20480	76684	173563	270727	4092	76684	173563	254339	16388
9	9216	25220	57257	91693	2044	25220	57257	84521	7172
8	4096	8236	18787	31119	1020	8236	18787	28043	3076
7	1792	2660	6113	10565	508	2660	6113	9281	1284

Ефективність модифікованого алгоритму визначимо коефіцієнтом ефективності h за співвідношенням:

$$h = \frac{Q_\Sigma^+ - Z_\Sigma^+}{Q_\Sigma^+} \cdot 100\%. \qquad (7)$$

На рис. 4 зображений графік залежності коефіцієнта ефективності модифікованого алгоритму, вираженого у відсотках, від значень n. З графіка видно, що максимальна економія за кількістю додавань досягається при невеликих значеннях n.

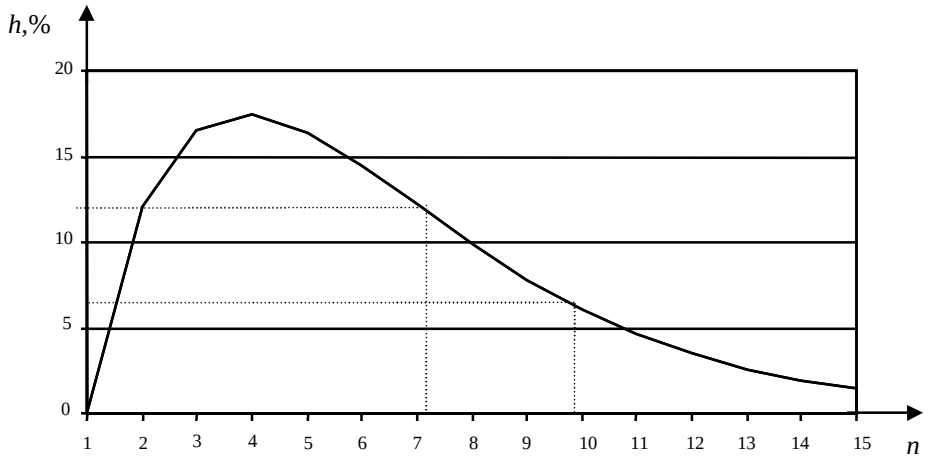

Рис. 4. Ефективність модифікованого алгоритму

На основі модифікованого алгоритму згортки будується метод зменшення часу реалізації операції множення надвеликих чисел [8]. Приведемо його короткий покроковий опис.

Крок 1. Обчислити згортку з використанням алгоритму (6).

Крок 2. Обчислити добуток u на v, виконуючи зсуви і додавання l-розрядних чисел.

При програмній реалізації розробленого методу на сучасних 32-бітних процесорах значення параметрів l і K вибираються в такий спосіб. Багаторозрядні числа u і v розбиваються на блоки довжиною, рівною 16-ти бітам ($l = 16$), і до кожного з блоків зліва додається така ж кількість нулів. З отриманих 32-бітних блоків (16 нулів плюс 16 значущих біт) формуються два часові ряди. Їхні довжини рівні $K = 2^a$. Довжина кожного часового ряду подвоюється шляхом додавання до нього такої ж кількості нульових 32-бітних блоків (у цьому випадку результатом обчислення циклічної згортки буде лінійна згортка, яка, з урахуванням зсувів і додавань l-розрядних чисел, і є добутком u і v). Загальна кількість 32-бітних блоків в одному часовому ряді $N = 2^n = 2 \cdot K$ дорівнює розмірності дискретного перетворення Уолша і, як правило, не перевищує 1024. У результаті справедливе співвідношення: $m = 2^b = 16 \cdot K = 8 \cdot N = 2^{n+3}$.

Порівняння розробленого методу зменшення часу реалізації операції множення надвеликих чисел з методом, запропонованим у роботі [3], показує, що при реалізації розробленого методу на ЕОМ необхідно виконання меншої кількості операцій додавання. У випадку, якщо $7 < n < 10$ (довжини багаторозрядних чисел-співмножників варіюються від 1024 до 8192 біт), економія кількості додавань складає від 7 % до 12 %. Зазначений діапазон довжин чисел-співмножників є найбільш придатним для сучасної класичної асиметричної криптографії.

Тепер розглянемо другий метод зменшення часу реалізації операції множення надвеликих чисел.

Відповідно до роботи [9], введемо деякі позначення.

Позначимо циклічну згортку $r_{xy}(x \circ y)$ двох векторів x і y довжини $N = 2^n$:

$$r_{xy}(k) = r_\tau = \sum_{m=0}^{N-1} x_m y_{k \underset{N}{\oplus} m}, \quad k = \overline{0,\ N-1}, \tag{8}$$

де $\underset{N}{\oplus}$ — додавання за модулем N, а також їхню лінійну згортку $S_{xy}(x \lozenge y)$:

$$S_{xy}(k) = \sum_{m=0}^{N-k-1} x_m y_{m+k}. \tag{9}$$

Оскільки згортки (8) і (9) можна легко виразити одну через іншу за допомогою співвідношень:

$$r_{xy}(m) = S_{xy}(m) + S_{xy}(N - m - 1), \tag{10}$$

$$S_{xy}(m) = r_{\tilde{x}\tilde{y}}(m), \qquad m = \overline{0,\ N-1}, \tag{11}$$

де $\hat{x}_r = \begin{cases} x_r, & r < N, \\ 0, & r \geq N, \end{cases}$ $\hat{y}_r = \begin{cases} y_r, & r < N, \\ 0, & r \geq N, \end{cases}$ $r = \overline{0,\ 2N-1}$, то алгоритми, отримані для циклічної згортки, легко перетворюються в алгоритми лінійної згортки і навпаки.

Визначимо знакову згортку $P_{xy}(x \nabla y)$ векторів x і y довжини $N = 2^n$ в такий спосіб:

$$P_{xy}(k) = \sum_{m=0}^{N-1} x_k y_{k \underset{N}{\oplus} m} \operatorname{Sign}\left[\left(m \underset{N}{\oplus} k\right) - m\right], \tag{12}$$

де $\operatorname{Sign}(x) = \begin{cases} 1, & x \geq 0, \\ -1, & x < 0. \end{cases}$

Запишемо циклічну згортку (8) в матричній формі:

$$r_{xy} = r_\tau = x_c y, \tag{13}$$

де x_c — циркулянтна матриця; представимо її у виді:

$$x_c = \sum_{m=0}^{N-1} x_m D^m, \tag{14}$$

де D — матриця циклічного зсуву на одну позицію.

Характеристичний поліном $d(\lambda)$ матриці D, рівний $(\lambda^N - 1)$, при $N = 2^N$ розкладається над $\Re$ на множники:

$$d(\lambda) = (\lambda - 1)(\lambda + 1)(\lambda^2 + 1), ..., (\lambda^{N/2} + 1), \tag{15}$$

внаслідок чого справедливе твердження про те, що матриця D приводиться над $\Re$.

Для розуміння суті наступних міркувань, приведемо доведену в [9] теорему про перетворення циркулянтної матриці до блочно-діагонального виду за допомогою перетворення Хаара.

Теорема. Матриця циклічного зсуву на один розряд перетворенням Хаара приводиться до блочно-діагонального виду, тобто:

$$HDH^{-1} = A = diag\{S_0 - S_0 S_1 S_2 S_{4...} S_{N/2}\}, \tag{16}$$

де S_i — матриця, розмірністю $2^i \times 2^i$, з елементами

$$[S_i]_{lk} = \begin{cases} 1, l = k+1, \\ -1, l = 2^i - 1, \ k = 0, \ S_0 = 1, \\ 0, \end{cases}$$

H — матриця перетворення Хаара.

З (16) випливає, що:

$$D = H^{-1} A H. \tag{17}$$

Підставимо (17) в (14):

$$x_c = \sum_{m=0}^{N-1`} x_m \left(H^{-1} A H\right)^m = \sum_{m=0}^{N-1} x_m H^{-1} A^m H. \tag{18}$$

Помноживши (18) зліва на H і справа на H^{-1}, одержимо:

$$H x_c H^{-1} = \sum_{m=0}^{N-1} x_m A^m. \tag{19}$$

Таким чином, з (19) випливає, що перетворення Хаара приводить циркулянтну матрицю до блочно-діагонального виду, що і потрібно було довести.

Співвідношення (19) також може бути записане в такий спосіб:

$$H x_c H^{-1} = h_0 \times \prod_{i=0}^{N/4} \sum_{k=0}^{2^i-1} h_{2^i+k} s_i^k, \tag{20}$$

де h_i — коефіцієнти розкладання вектора x по функціям Хаара; знак $(\times)$ означає прямий добуток матриць.

Перейдемо безпосередньо до алгоритму обчислення згортки.

Кінцеві часові ряди $x_0,...,x_{N-1}$ та $y_0,...,y_{N-1}$ представимо векторами-стовпцями:

$$x = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix}, \qquad y = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix}. \tag{21}$$

Позначимо вектори циклічного зсуву у виді:

$$x' = \begin{bmatrix} -x_{N-1} \\ x_0 \\ \vdots \\ x_{N-2} \end{bmatrix}, \qquad x'' = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_0 \end{bmatrix}, \qquad x''' = \begin{bmatrix} x_0 \\ x_{N-1} \\ \vdots \\ x_1 \end{bmatrix}. \tag{22}$$

Набір матриць $E, O, P, S,$ які перетворюють вектор довжини N у вектори довжини $N/2$, визначимо як:

$$Ex = \begin{bmatrix} x_0 \\ x_2 \\ \vdots \\ x_{N-2} \end{bmatrix}, \quad Ox = \begin{bmatrix} x_1 \\ x_3 \\ \vdots \\ x_{N-1} \end{bmatrix}, \quad Px = \begin{bmatrix} x_0 + x_1 \\ x_2 + x_3 \\ \vdots \\ x_{N-2} + x_{N-1} \end{bmatrix}, \quad Sx = \begin{bmatrix} x_0 - x_1 \\ x_2 - x_3 \\ \vdots \\ x_{N-2} - x_{N-1} \end{bmatrix}. \tag{23}$$

Відзначимо, що:

$$\begin{aligned} Px &= Ex + Ox, \;\; Sx = Ex - Ox, \\ Py &= Ey + Oy, \;\; Sy = Ey - Oy. \end{aligned} \tag{24}$$

Оскільки довжина вектора після перетворення будь-яким із приведених вище операторів стає в два рази менше, то перетворення припиняються, коли x стає одномірним вектором (числом).

Справедливі співвідношення:

$$EP_{xy} = Ex\nabla Ey + Ox\nabla Oy, \quad OP_{xy} = Ex\nabla Oy + (Ox)'\nabla Ey. \tag{25}$$

Розглянемо допоміжні згортки $a,\ b$ і c виду:

$$a = Ex\nabla Py = Ex\nabla(E+O)y, \;\; b = Sx\nabla Oy = (E-O)x\nabla Oy, \;\; c = \left[(Ox)' - Ex\right]\nabla Ey. \tag{26}$$

Тоді:

$$EP_{xy} = a - b, \quad OP_{xy} = a + c. \tag{27}$$

Співвідношення (26) і (27) зводять обчислення знакової згортки векторів довжиною N до обчислення трьох знакових згорток довжиною $N/2$. Оскільки згортка (12) векторів $x = [x_0]$ і $y = [y_0]$ є $P_{xy} = [x_0 y_0]$, то для обчислення згортки (12) векторів довжиною N буде потрібно 3^n операцій множення.

Порівнявши співвідношення (20) з алгоритмом (26), (27), який представляє собою кінцевий ітераційний процес, бачимо, що використання перетворення Хаа-

ра дає можливість звести обчислення циклічної згортки r_τ до визначення ряду знакових згорток коефіцієнтів розкладання векторів x і y по системі Хаара.

Розглянемо більш ефективний алгоритм обчислення дискретної циклічної згортки r_τ припускаючи, що $x = y$.

Представимо згортку (8) з використанням співвідношень (13) і (20) в операторному виді. Для цього визначимо матриці L, V, M, K і G, які перетворюють вектор довжиною N у вектори довжиною $N/2$:

$$Lx = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N/2-1} \end{bmatrix}, \qquad Vx = \begin{bmatrix} x_{N/2} \\ x_{N/2+1} \\ \vdots \\ x_{N-1} \end{bmatrix}, \qquad Mx = \begin{bmatrix} x_0 + x_{N/2} \\ x_1 + x_{N/2+1} \\ \vdots \\ x_{N/2-1} + x_{N-1} \end{bmatrix},$$

$$Kx = \begin{bmatrix} x_0 - x_{N/2} \\ x_1 - x_{N/2+1} \\ \vdots \\ x_{N/2-1} - x_{N-1} \end{bmatrix}, \qquad Gx = \begin{bmatrix} x_0 \cdot x_{N/2} \\ x_1 \cdot x_{N/2+1} \\ \vdots \\ x_{N/2-1} \cdot x_{N-1} \end{bmatrix}. \tag{28}$$

Відзначимо, що:

$$\begin{aligned} &Mx = Lx + Vx, \quad Kx = Lx - Vx, \quad Gx = Lx \cdot Vx, \\ &My = Ly + Vy, \quad Ky = Ly - Vy, \quad Gy = Ly \cdot Vy. \end{aligned} \tag{29}$$

Справедливі співвідношення:

$$\begin{aligned} &Er_{xx} = Ex \circ Ex + Ox \circ Ox, \\ &Or_{xx} = Ex \circ Ox + \left(Ox \circ Ex\right)''. \end{aligned} \tag{30}$$

Із співвідношень (30) випливає, що для обчислення циклічної згортки $r_{xy} = r_\tau$ векторів довжиною N необхідне визначення циклічної згортки векторів довжиною $N/2$.

Розглянемо допоміжні згортки a і b виду:

$$a = Px \circ Px = \left(E + O\right)x \circ \left(E + O\right)x, \qquad b = Ox \circ Ex. \tag{31}$$

Тоді:

$$Er_{xx} = a - b - b''', \qquad Or_{xx} = b'' + b'''. \tag{32}$$

Таким чином, необхідна згортка виходить за допомогою лінійної комбінації допоміжних згорток: a, b, b'' і b'''.

Для обчислення циклічної згортки r_τ по представленому алгоритму необхідне виконання $\left(3^{\log_2 N} + 3 + 2^{\log_2 N}\right)/4 = \left(3^n + 3 + 2^n\right)/4$ операцій множення.

На основі розглянутого швидкого алгоритму обчислення дискретної циклічної згортки будується метод зменшення часу реалізації операції множення надвеликих чисел [10]. Приведемо його короткий покроковий опис.

Крок 1. Обчислити згортку з використанням алгоритму (32).

Крок 2. Обчислити добуток u на v, виконуючи зсуви і додавання l-розрядних чисел.

При програмній реалізації розробленого методу на сучасних 32-бітних процесорах значення параметрів l і K вибираються за тим же принципом, що і для методу, заснованому на ШПУ.

Порівняємо розроблений метод з методом, описаним в [11], в якому для обчислення дискретної циклічної згортки r_τ використовується модифікований алгоритм ШПФ з попередньою заготовкою елементів матриці перетворення. Складність методу [11] дорівнює:

$$\begin{aligned} T^{\times} &= 3K\left(\log_2 K - 1\right) - 16 = \\ &= 1{,}5N\left(\log_2 \frac{N}{2} - 1\right) - 16 = 1{,}5 \cdot 2^n\left(\log_2 2^{n-1} - 1\right) - 16, \end{aligned} \tag{33}$$

де $K = 2^a$ — кількість блоків, на які розбиваються багаторозрядні числа-співмножники.

Результати порівняння методів приведені в зведеній табл. 2, яка містить кількість «малих» множень, необхідних для обчислення добутку багаторозрядних чисел кожним з них.

Таблиця 2. Складність методів множення багаторозрядних чисел

n	5	6	7	8	9	10	11	12	13
$T^{\times}$	368	944	2288	5360	12272	27632	61424	135152	294896
$W^{\times}$	70	199	580	1705	5050	15019	44800	133885	400630

Аналіз таблиці показує, що ефективність розробленого методу при $n \le 12$ вище ефективності методу, запропонованого в [11]. Для вказаних значень n при обчисленні добутку багаторозрядних чисел розробленому методу потрібна менша кількість «малих» множень, ніж методу, який використовує ШПФ.

1. *Кнут Д.* Искусство программирования. Т. 2: Получисленные алгоритмы. — М.: Издательский дом «Вильямс», 2001. — 832 с.

2. *Шенхаге А., Штрассен В.* Быстрое умножение больших чисел // Кибернетический сборник. — 1973. — Вып. 2. — С. 87–98.

3. *Задирака В.К., Мельникова С.С.* Анализ сложности алгоритма умножения сверхбольших чисел на основе коэффициентов Уолша // Кибернетика и систем. анализ. — 2001. — № 6. — С. 99–110.

4. *Толстых Г.Д.* Сверхбыстрое спектральное преобразование по функциям Хаара // Изв. вузов – радиоэлектроника. — 1979. — № 7. — С. 86–89.

5. *Andrews H.C.* Computer Techniques in Image Processing. — New York: Academic Press, 1970. — P. 73–90.

6. *Alexits G.* Convergence Problems of Orthogonal Series. — New York: Pergamon, 1961. — P. 46–62.

7. *Файн Б.* Связь между преобразованиями Хаара и Уолша-Адамара // ТИИЭР. — 1972. — № 5. — С. 100–113.

8. *Богданов А.М., Зинченко Я.В.* Модификация алгоритма умножения сверхбольших чисел на основе коэффициентов Уолша // Захист інформації. — 2002. — № 3. — С. 46–52.

9. *Садыхов Р., Шаренков А.* Алгоритмы ускоренной свертки // Автоматика. — 1986. — № 3. — С. 71–75.

10. *Богданов А.М., Зинченко Я.В.* Умножение сверхбольших чисел и быстрое преобразование Хаара // Захист інформації. — 2002. — № 4. — С. 58–67.

11. *Задирака В.К., Мельникова С.С.* Быстрое умножение многоразрядных чисел с использованием БПФ // Кибернетика и систем. анализ. — 1996. — № 3. — С. 63–67.

Надійшла до редакції 26.11.2004