3.Geoffrion A,M. Elements of lorge-seecele mathematical programming. Parts – Management Scsence, 1970, 16, № 11, p 652-691.
4.Левин Г.М. Ганаев В,С, Декомпозиционные методы оптимизации проектных решений. Минск. Наука и техника, 1978, 240 с.
5.Изурков В.И. Декомпозиция в задачах большой размерности. М., Наука, 19981, 352 с.

УДК 519.6

Богданов А.М., Зинченко Я.В.

МОДИФИКАЦИЯ АЛГОРИТМА УМНОЖЕНИЯ СВЕРХБОЛЬШИХ ЧИСЕЛ НА ОСНОВЕ КОЭФФИЦИЕНТОВ УОЛША

В настоящее время при программной реализации асимметричных криптоалгоритмов существует необходимость в быстром выполнении операции умножения многоразрядных чисел, размерность которых реально составляет 512-4096 бит.

Известно, что число шагов (битовых операций), необходимых для умножения двух m-разрядных чисел "в столбик", равняется m^2. Однако, нашли широкое применение методы, позволяющие вычислить требуемое произведение быстрее, чем за m^2 шагов. Это метод Карацубы со сложностью $O\left(m^{1,59}\right)$, модулярный метод, имеющий сложность $O\left(m^{1,63}\right)$, и другие. Алгоритм Шенхаге-Штрассена является асимптотически самым быстрым из известных и позволяет умножить два m-разрядных числа за $m\,log\,m\,log\,log\,m$ шагов [1]. Этот алгоритм основан на идее использования теоремы о дискретной свертке двух функций, т. к. произведение многоразрядных чисел без учета переносов является дискретной циклической сверткой двух сомножителей. Поскольку дискретная циклическая свертка дает основной вклад в оценку сложности алгоритма, то для эффективного ее вычисления используется алгоритм быстрого преобразования Фурье.

В работе [2] описан и проанализирован эффективный алгоритм умножения многоразрядных чисел, в основу которого положен разработанный в [3] алгоритм вычисления циклической свертки, основанный на коэффициентах Уолша и отсутствии перехода в поле комплексных чисел.

В данной статье предлагается методика модификации алгоритма вычисления циклической свертки, предложенного в [3], путем уменьшения общего числа сложений, необходимых для его реализации. Сущность модификации заключается в замене операции вычисления коэффициентов Уолша с использованием быстрого преобразования Уолша (БПУ) на операцию вычисления этих коэффициентов с использованием быстрого преобразования Хаара (БПХ).

Из [3] известно, что общее количество сложений, необходимых для вычисления циклической свертки, равно:

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

где $Q_1^{+} = n \cdot 2^{n+1}$ – количество сложений, необходимых для выполнения шага 1 алгоритма (вычисление коэффициентов Уолша F^{x} и F^{y} исходных последовательностей x и y с использованием БПУ), $Q_2^{+} = 4\left(3^{n-1} - 2^{n-1}\right)$ – число сложений, необходимых для

выполнения шага 2 алгоритма (вычисление вектора линейных комбинаций из коэффициентов F^x и F^y), $Q_3^+ = \left(3^{n+1} - 3{,}5 \cdot 2^n\right)$ – количество сложений, необходимых для выполнения шага 3 алгоритма (вычисление коротких сверток).

Оптимизация алгоритма вычисления циклической свертки по числу сложений, возможна за счет минимизации количества сложений при выполнении шага 1.

Известно [4], что число сложений, которые необходимы для вычисления коэффициентов Уолша и Хаара векторов длины $N = 2^n$ с использованием быстрых алгоритмов, равняется $n \cdot 2^n$ и $2\left(2^n - 1\right)$ соответственно. Из приведенных ниже соотношений, связывающих преобразования Уолша и Хаара, следует, что преобразование Уолша можно заменить преобразованием Хаара, которое обеспечивает экономию числа сложений (при $N = 2^n = 256$ примерно в четыре раза) и, соответственно, более высокую скорость вычислений. Эти соотношения дают семейство ортогональных преобразований, включающее преобразования Уолша и Хаара, к которым относится один общий алгоритм быстрого вычисления.

Обозначим, в соответствии с [5], матрицы Хаара $\left[H_2^n\right]$ и Уолша-Адамара $\left[W_2^n\right]$ порядка 2^n, строки которых представляют собой 2^n функций Хаара и Уолша, нормированных на $1/\sqrt{2^n}$; разобьем матрицы $\left[H_2^n\right]$ и $\left[W_2^n\right]$ на $(n+1)$ прямоугольных подматриц $\left[MH_{2^n}^k\right]$ и $\left[MW_{2^n}^k\right]$ размером $\left(2^n \times 2^{k-1}\right)$, $k = 1, \ldots, n$. Матрица $\left[MH_{2^n}^0\right]$ представляет собой первую строку H^0, матрица $\left[MW_{2^n}^0\right]$ представляет собой первую строку W^0, а матрицы $\left[MH_{2^n}^k\right]$ и $\left[MW_{2^n}^k\right]$ формируются из функций Хаара и Уолша ранга r, причем $2^{k-1} \le r \pi 2^k$.

Матрицы $\left[H_2^n\right]$ и $\left[W_2^n\right]$, а также подматрицы $\left[MH_{2^n}^k\right]$ и $\left[MW_{2^n}^k\right]$ представлены на рис. 1.

$$\begin{matrix}
H_0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
H_1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
H_2 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} & 0 & 0 & 0 & 0 \\
H_3 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & -\sqrt{2} & -\sqrt{2} \\
H_4 & 2 & -2 & 0 & 0 & 0 & 0 & 0 & 0 \\
H_5 & 0 & 0 & 2 & -2 & 0 & 0 & 0 & 0 \\
H_6 & 0 & 0 & 0 & 0 & 2 & -2 & 0 & 0 \\
H_7 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & -2
\end{matrix}$$

$\left[MH_3^0\right]$, $\left[MH_3^1\right]$, $\left[MH_3^2\right]$, $\left[MH_3^3\right]$

Матрица Хаара порядка 2^n

$$\begin{matrix}
W_0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
W_1 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
W_2 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\
W_3 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\
W_4 & 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\
W_5 & 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\
W_6 & 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\
W_7 & 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1
\end{matrix}$$

$\left[MW_3^0\right]$, $\left[MW_3^1\right]$, $\left[MW_3^2\right]$, $\left[MW_3^3\right]$

Матрица Уолша-Адамара порядка 2^n

Рис. 1. Матрицы и подматрицы Хаара и Уолша-Адамара

Между подматрицами $\left[MH^{k}_{2^n} \right]$ и $\left[MW^{k}_{2^n} \right]$ существует связывающее их матричное соотношение [6]:

$$\left[MW^{k}_{2^n} \right] = \left[W_{2^{k-1}} \right] \cdot \left[S_{2^{k-1}} \right] \cdot \left[MH^{k}_{2^n} \right], \quad k = 1, \ldots, n, \tag{2}$$

где $\left[W_{2^{k-1}} \right]$ – упорядоченная матрица Уолша-Адамара порядка 2^{k-1}, а $\left[S_{2^{k-1}} \right]$ – матрица перестановок порядка 2^{k-1} вида

$$\left[S_{2^{k-1}} \right] = \begin{bmatrix} & & & 1 \\ & 0 & . & \\ & & . & \\ & & 1 & \\ & . & & 0 \\ 1 & & & \end{bmatrix}.$$

Поскольку $\left[W_{2^{k-1}} \right]$ и $\left[S_{2^{k-1}} \right]$ симметричны и ортогональны, то можно получить обратное соотношение:

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

В работе [7] доказывается справедливость выражений (2) и (3) и определяются соотношения, связывающие преобразованные векторы $V_W\left(V_{W_0}, V_{W_1}, \ldots, V_{W_{2^n-1}} \right)$ и $V_H\left(V_{H_0}, V_{H_1}, \ldots, V_{H_{2^n-1}} \right)$, соответствующие исходному вектору V.

Умножив правые части выражений (2) и (3) на вектор V, получим:

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

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

Наборы коэффициентов преобразованных векторов, появляющихся в выражениях (4) и (5), называются зонами. Из соотношений видно, что зона преобразованного вектора V_H определяет соответствующую зону преобразованного вектора V_W. Это свойство показывает, что если вектор V аппроксимируется некоторым подмножеством зон преобразованных векторов V_H и V_W или, в частности, если эти векторы усекаются в конце зоны, то после обратных преобразований получается исходный приближенный вектор V.

В соотношениях (4) и (5) соответствующие зоны связаны ортогональными преобразованиями. Из теоремы Парсеваля следует, что энергии соответствующих зон преобразованных векторов одинаковы.

На рис. 2 приведена схема алгоритма быстрого вычисления преобразования Хаара 8-го порядка. Согласно [7], повторное применение соотношения (4) позволяет получить из этой схемы схему алгоритма быстрого вычисления преобразования Уолша 8-го порядка, представленную на рис. 3. Пунктирными линиями обведены преобразования Уолша низших порядков, после которых производятся перестройки матриц $[S]$.

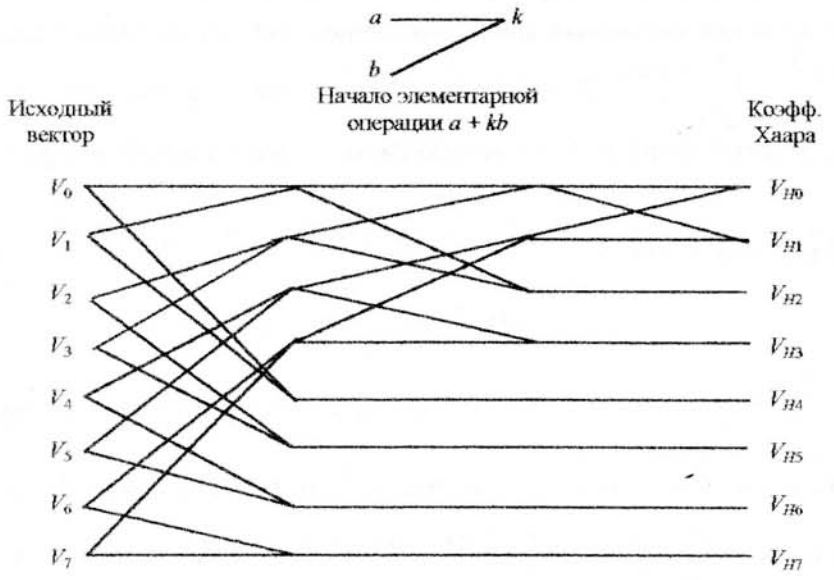

Рис. 2. Схема алгоритма быстрого вычисления преобразования Хаара

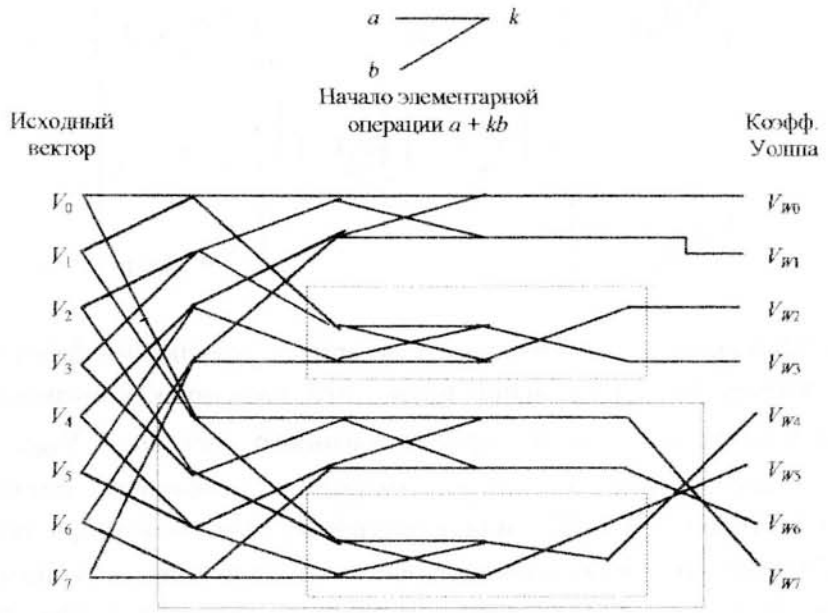

Рис. 3. Схема алгоритма быстрого вычисления преобразования Уолша

Таким образом, применение соотношений (2) и (3) приводит к тому, что преобразование Хаара действует так же, как и преобразование Уолша, а количество сложений, которые необходимы для вычисления коэффициентов Уолша последовательности длины $N = 2^n$, уменьшается на величину $n \cdot 2^n - 2\left(2^n - 1\right) = n \cdot 2^n - 2^{n+1} + 2$. С учетом того, что в алгоритме (1) обрабатываются две последовательности (x и y), и для каждой из них получается указанный выигрыш, общее уменьшение числа сложений составит $n \cdot 2^{n+1} - \left(2^{n+2} - 4\right) = 2^{n+1}(n-2) + 4$. Общее число сложений, необходимых для вычисления циклической свертки модифицированным алгоритмом будет равно:

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

где $Z_1^{+} = \left(2^{n+2} - 4\right)$ – количество сложений, необходимых для выполнения шага 1 алгоритма (вычисление коэффициентов Уолша F^x и F^y последовательностей x и y с использованием БПХ), $Z_2^{+} = Q_2^{+} = 4\left(3^{n-1} - 2^{n-1}\right)$ – число сложений, необходимых для выполнения шага 2 алгоритма (вычисление вектора линейных комбинаций из F^x и F^y), $Z_3^{+} = Q_3^{+} = \left(3^{n+1} - 3{,}5 \cdot 2^n\right)$ – количество сложений, необходимых для выполнения шага 3 алгоритма (вычисление коротких сверток).

Результаты сравнения исходного (1) и модифицированного (6) алгоритмов приведены в сводной табл. 1, содержащей число сложений, необходимых для вычисления циклической свертки каждым из них.

Таблица 1

Сложность алгоритмов вычисления циклической свертки

n	Q^+_1	Q^+_2	Q^+_3	Q^+_Σ	Z^+_1	Z^+_2	Z^+_3	Z^+_Σ	Эконом. числа сложен.
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
6	768	844	1963	3575	252	844	1963	3059	516
5	320	260	617	1197	124	260	617	1001	196
4	128	76	187	391	60	76	187	323	68
3	48	20	53	121	28	20	53	101	20
2	16	4	13	33	12	4	13	29	4
1	4	0	2	6	4	0	2	0	0

Эффективность модифицированного алгоритма определяется коэффициентом эффективности h по соотношению:

$$h = \frac{Q^+_\Sigma - Z^+_\Sigma}{Q^+_\Sigma} \cdot 100\%. \qquad (7)$$

На рис. 4 изображен график зависимости коэффициента эффективности модифицированного алгоритма, выраженного в процентах, от значений n. Из графика видно, что максимальная экономия по числу сложений достигается при малых значениях n ($h = 17{,}4\%$ при $n = 4$), поэтому данный алгоритм наиболее целесообразно использовать для вычисления сверток коротких временных последовательностей.

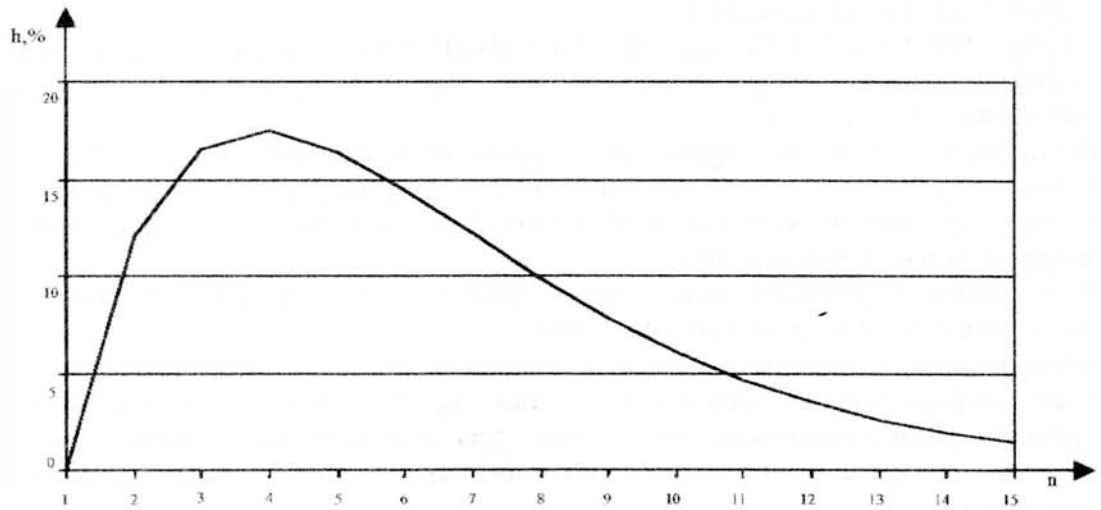

Рис. 4. Эффективность модифицированного алгоритма

Список литературы:

1. *Кнут Д.* Искусство программирования для ЭВМ. Т. 2. – М. : Мир, 2001. – 730 с.

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

3. *Pitassi D. A.* Fast convolution using the Walsh transform//Appl. of Walsh Funktions. – 1971. – P. 130-133.

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, pp. 73-90.

6. *Alexits G.* Convergence Problems of Orthogonal Series, New York: Pergamon, 1961, pp. 46-62.

7. *Файн Б.* Связь между преобразованиями Хаара и Уолша-Адамара//ТИИЭР, 1972. №5.

УДК 681.3

С.Р. Коженевский, Г.Т. Солдатенко

ЗАЩИТА ИНФОРМАЦИИ В ЦЕПЯХ ЭЛЕКТРОПИТАНИЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Что имеем – не храним,
Потерявши – плачем.
Народный ЭПОС

В современном мире большие объемы информации обрабатываются, хранятся и передаются электронными методами, и, следовательно, сопровождаются электромагнитными излучениями. Поэтому существует реальная возможность несанкционированного доступа к этой информации посредством радиоперехвата или контактного подключения к коммуникациям [2]. В подтверждение этому достаточно привести такие примеры.

В отчетах Агентства Национальной Безопасности США опубликованы сведения о том, что около 80% разведывательной информации поступает по техническим каналам утечки информации за счет радиоперехвата.

Фирма «ЕПОС» и ЦТЗИ «Барьер» ОАО «НИИЭМП» демонстрировали на выставке EnterEx-2001 перехват информации с монитора по радиоканалу с помощью радиолюбительских устройств.

Но информацию можно перехватить и путем подключения к цепям электропитания. Так, в частности, на рис. 1 показана установка, с помощью которой мы демонстрируем возможность перехвата информации, отображаемой на мониторе компьютера, путем анализа напряжения в линии электропитания.

В установке применены стандартные приборы: селективный вольтметр SMV-11, эквивалент сети NNB-111, осциллограф С1-65А.

Персональный компьютер является центральным звеном в информационных системах обработки информации и находится в зоне пристального внимания конкурентов, злоумышленников и разведывательных служб. Для получения информации используются все доступные средства, в том числе и различные анализаторы, подключаемые к линиям электропитания.

Прежде чем приступить к рассмотрению обозначенной проблемы необходимо дать некоторые пояснения используемой терминологии.