Индикаторные матрицы систем функций Уолша и их криптографические приложения

Белецкий А. Я.[1]

[1]Проф., д.т.н., кафедра электроники, Национальный авиационный университет,
пр. Космонавта Комарова,1, Киев, Украина, abelnau@ukr.net

Аннотация **— Рассматриваются вопросы формирования симметричных систем функций Уолша двоично степенного порядка на основе их индикаторных матриц, являющихся симметричными относительно вспомогательной диагонали (0,1)-матрицами, невырожденными в кольце вычетов по модулю 2. Порядок индикаторных матриц логарифмически связан с порядком систем Уолша. Обсуждается проблема разработки алгоритмов криптографической защиты пакетов дискретных сигналов, базирующихся на их быстром преобразовании Фурье в базисах систем функций Уолша. Устанавливается правило перестановки отсчетов сигналов на входе процессора БПФ, обеспечивающее вычисление спектра в заданном базисе функций Уолша.**

Ключевые слова: **индикаторные матрицы систем Уолша, обобщенные коды Грея, криптографическая защита пакетов видеосигнала.**

Indicator Matrix of Walsh Functions of Systems and Cryptographic Applications

Beletsky A. Ja.[1]

[1]Prof., Dr. Sc., Department of Electronics, National Aviation University,
pr. Kosmonavt Komarov, 1, Kiev, Ukraine, abelnau@ukr.net

Abstract **— The issues of formation of asymmetric systems, binary power Walsh functions of order on the basis of indicator matrices that are symmetric with respect to the auxiliary diagonal (0.1) matrix, non-degenerate in the ring of residues modulo 2. The procedure of test matrices is logarithmically related to the order of the Walsh system. The problem of the development of algorithms for cryptographic protection of packets of digital signals based on their fast Fourier transform in the bases of systems of Walsh functions. Establishes the right permutation signal samples at the input of the FFT processor provides the calculation of the spectrum in a given basis Walsh functions.**

Keywords: **matrix indicator Walsh systems, generalized Gray codes, cryptographic protection of video packets.**

Введение

Несмотря на более чем вековую историю своего зарождения и развития до настоящего времени из большого числа симметричных систем функций Уолша $\boldsymbol{W}_N$, где $N-$порядок системы, в приложениях нашли применение лишь три системы Уолша. Первая из них, система Уолша-Адамара $\boldsymbol{H}_N=\{h(k,t)\}$, где k и t – номер (порядок) и аргумент (дискретное время) базисной функции системы, разработана Адамаром (Hadamard) в 1893 году [1]. Упорядочивая функции $h(k,t)$ систем Адамара в порядке возрастания числа знакоперемен, Уолш (Walsh) пришел в 1923 году к системам функций $\boldsymbol{W}_N$, получивших впоследствии название систем Уолша, упорядоченных по Качмажу [2]. И, наконец, в 1932 году математиком Пэли (Paley) предложена третья (и, можно сказать, последняя структурированная) система Уолша-Пэли $\boldsymbol{P}_N$ [3].

В докладе рассматриваются системы Уолша (введем для них обозначение $\boldsymbol{W}_N$, совсем не обязательно относящееся к системам Уолша-Качмажа), порядки которых составляют величину $N=2^n$. Будем называть такие порядки *двоично степенными*. Степень $n-$ это натуральные числа, совпадающие с порядком *индикаторной матрицы* (ИМ) $\boldsymbol{J}_w$ системы $\boldsymbol{W}_N$ [4]. Определение ИМ дается ниже по тексту.

В работах [5,6] получены оценки $L(n)$ числа симметричных систем Уолша в зависимости от порядка n ИМ системы:

$$L(n)=\prod_{i=1}^{n}(2^i-(i)_2)\,, \qquad (1)$$

где $(a)_m-$вычет числа a по модулю m.

Номера (порядки) базисных функций k систем Уолша, упорядоченных по Адамару, Качмажу и Пэли, связаны (рис. 1), как впервые отмечено в [7], кодами Грея. Аббревиатурами на рис. 1 обозначены операторы: ДИП – двоично-инверсной перестановки, КГ – прямого кодирования Грея и ОКГ – обратного кодирования Грея.

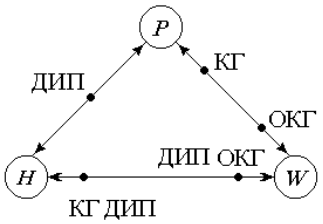

Рисунок 1 – Взаимосвязь номеров базисных функций в классических системах Уолша

Тремя *классическими системами* $\boldsymbol{H}$, $\boldsymbol{W}$ и $\boldsymbol{P}$ (рис.1), не исчерпывается множество систем Уолша. Согласно оценке (1) всего существует, например, 28 таких систем восьмого порядка.

Вызывает недоумение тот факт, что оказались вне поля зрения как математиков, так и разработчиков электронной аппаратуры, возможности построения кодов, инверсных по направлению формирования классическим кодам Грея. В известной (классической) схеме процесс формирования прямых и обратных кодов Грея развивается по направлению преобразования слева направо. При этом старший (левый) разряд преобразуемого числа сохраняется как при прямом, так и обратном преобразованиях. Вместе с тем, можно построить схему преобразования кодов, обратную по направлению классическому (*левостороннему*) преобразованию Грея. В таком классе кодов Грея, названном *правосторонним преобразованием* [8], при прямом и обратном преобразовании сохраняется неизменным значение младшего (правого) разряда преобразуемого кода.

Совокупность перечисленных выше простых кодов, именуемых также *преобразованиями Грея* (ПГ) или *операторами Грея*, сведена в табл. 1, а их матричные формы показаны в табл. 2.

Таблица 1. Полная группа простых операторов Грея

Обозначение оператора	**Выполняемая операция**
0(e)	Сохранение исходной комбинации
1	Инверсная перестановка
2	Прямое левостороннее ПГ
3	Обратное левостороннее ПГ
4	Прямое правостороннее ПГ
5	Обратное правостороннее ПГ
6	Циклический сдвиг вправо
7	Циклический сдвиг влево

Таблица 2. Матричные формы простых операторов Грея

$0=\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}$	$2=\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}$	$4=\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}$	$6=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$
$1=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$	$3=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}$	$5=\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix}$	$7=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$

Комбинация лево- и правосторонних кодов Грея, как прямых, так и обратных, совместно с операторами инверсной перестановки 1 и циклического сдвига 6,7 привела к возможности построения *составных кодов Грея* (СКГ) G, образуемых произведением $l>1$ простых кодов g_i

$$G=\prod_{i=1}^{l} g_i, \quad g_i \in \{0,1,\ldots,7\}. \qquad (2)$$

Например, в общем случае СКГ $G=242$ означает, что некоторый бинарный вектор $n-$го порядка $\boldsymbol{x}=x_{n-1},x_{n-2},\ldots x_1,x_0$, или (0,1)-матрица $\boldsymbol{M}$ того же порядка, подвергается преобразованию Грея сначала оператором 2, затем 4 и, наконец, снова оператором 2.

Произведение в кольце вычетов по модулю 2 матричных операторов, расположенных в столбцах табл. 2, за исключением матриц левого столбца, равно единичной матрице.

Множество простых КГ (табл. 1 и 2) и на их основе – СКГ (2) дают возможность установить взаимосвязь (рис. 2) всех 28 симметричных систем Уолша восьмого порядка, индикаторные матрицы которых $\boldsymbol{J}_w$ представлены в табл. 3.

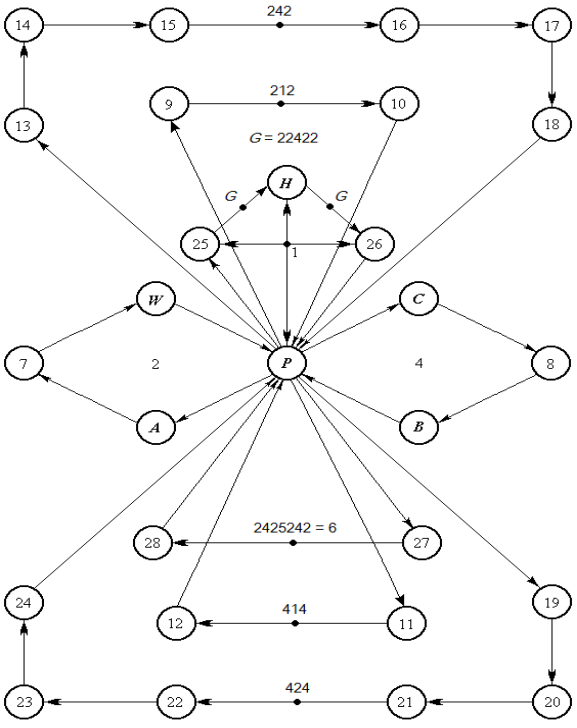

Рисунок 2. Полный граф Пэли-связанных систем функций Уолша восьмого порядка

Таблица 3. Индикаторные матрицы систем функций Уолша восьмого порядка

$\boldsymbol{E}=\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}$	$\boldsymbol{H}=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$	$\boldsymbol{W}=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}$	$\boldsymbol{A}=\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}$	$\boldsymbol{B}=\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix}$	$\boldsymbol{C}=\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}$	$7=\begin{bmatrix}1&0&1\\0&1&0\\0&0&1\end{bmatrix}$
$8=\begin{bmatrix}1&0&0\\0&1&0\\1&0&1\end{bmatrix}$	$9=\begin{bmatrix}0&1&0\\1&0&1\\1&1&0\end{bmatrix}$	$10=\begin{bmatrix}1&0&1\\1&0&0\\1&1&1\end{bmatrix}$	$11=\begin{bmatrix}0&1&1\\1&0&1\\0&1&0\end{bmatrix}$	$12=\begin{bmatrix}1&1&1\\0&0&1\\1&0&1\end{bmatrix}$	$13=\begin{bmatrix}0&1&1\\1&1&1\\0&1&0\end{bmatrix}$	$14=\begin{bmatrix}1&0&1\\1&1&0\\1&1&1\end{bmatrix}$
$15=\begin{bmatrix}0&0&1\\1&0&0\\1&1&0\end{bmatrix}$	$16=\begin{bmatrix}0&1&0\\0&1&1\\1&0&0\end{bmatrix}$	$17=\begin{bmatrix}1&1&1\\1&0&1\\0&1&1\end{bmatrix}$	$18=\begin{bmatrix}1&1&0\\0&0&1\\1&0&1\end{bmatrix}$	$19=\begin{bmatrix}0&1&0\\1&1&1\\1&1&0\end{bmatrix}$	$20=\begin{bmatrix}1&1&1\\0&1&1\\1&0&1\end{bmatrix}$	$21=\begin{bmatrix}0&1&1\\0&0&1\\1&0&0\end{bmatrix}$
$22=\begin{bmatrix}0&0&1\\1&1&0\\0&1&0\end{bmatrix}$	$23=\begin{bmatrix}1&1&0\\1&0&1\\1&1&1\end{bmatrix}$	$24=\begin{bmatrix}1&0&1\\1&0&0\\0&1&1\end{bmatrix}$	$25=\begin{bmatrix}1&1&0\\1&1&1\\0&1&1\end{bmatrix}$	$26=\begin{bmatrix}0&1&1\\1&1&1\\1&1&0\end{bmatrix}$	$27=\begin{bmatrix}0&1&0\\0&0&1\\1&0&0\end{bmatrix}$	$28=\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$

На основании анализа данных табл. 1 и 2 сформулируем определение ИМ систем Уолша:

Индикаторными матрицами $\boldsymbol{J}_w$ *систем функций Уолша* $\boldsymbol{W}_N$ *двоично степенного порядка* $N=2^n$, *где* $n-$ *натуральное число, являются правосторонне симметрические (0,1)-матрицы* $n-$*го порядка, то есть матрицы, симметричные относительно вспомогательной диагонали* (необходимые условия)*, невырожденные в кольце вычетов по модулю 2* (достаточные условия).

Основная цель данного исследования состоит в разработке алгоритма криптографической защиты информации (КЗИ), передаваемой с борта беспилотного летательного аппарата (БПЛА) на наземный пункт управления (НПУ). В качестве метода КЗИ предлагается использовать быстрое преобразование Фурье (БПФ) дискретных сигналов в базисах систем функций Уолша высокого порядка ($N \geq 256$), стохастически выбираемых из большого числа этих систем, что затрудняет противнику несанкционированный доступ к закрытым данным. Для достижения поставленной цели необходимо решить такие задачи:

- предложить способы компактного описания систем функций Уолша большого порядка и их быстрого стохастического синтеза;
- разработать алгоритм перестановки отсчетов дискретных сигналов на входах процессора БПФ (реализующий схему Кули-Тьюки), который обеспечивает формирование спектра сигнала в требуемом базисе систем функций Уолша, исключая необходимость факторизации матриц Уолша.

Прямая и обратная задачи Уолша.

Между матрицами систем функций Уолша $\boldsymbol{W}$ и их индикаторными матрицами $\boldsymbol{J}_w$ существует взаимно однозначное соответствие (*биекция*) $\boldsymbol{W} \leftrightarrow \boldsymbol{J}_w$, которое устанавливается далее так называемыми «прямой» и «обратной» задачами Уолша.

Прямая задача Уолша состоит в том, чтобы по заданной индикаторной матрице $\boldsymbol{J}_w$ $n-$го порядка вычислить матрицу Уолша $\boldsymbol{W}_N$ двоично степенного порядка $N=2^n$.

Обратная задача Уолша предполагает вычисление индикаторной матрицы $\boldsymbol{J}_w$ для заданной матрицы Уолша $\boldsymbol{W}_N$.

Обратимся сначала к более простой обратной задаче на примере системы Уолша-Кули восьмого порядка из пространства изображений [6]

$$\boldsymbol{C}_8=\begin{array}{c} \\ 0\\1\\2\\3\\4\\5\\6\\7\\ k\end{array}\begin{array}{c}\begin{array}{cccccccc}0&1&2&3&4&5&6&7&\quad t\end{array}\\ \begin{bmatrix}0&0&0&0&0&0&0&0\\0&0&1&1&1&1&0&0\\0&1&1&0&0&1&1&0\\0&1&0&1&1&0&1&0\\0&1&0&1&0&1&0&1\\0&1&1&0&1&0&0&1\\0&0&1&1&0&0&1&1\\0&0&0&0&1&1&1&1\end{bmatrix}\end{array}, \qquad (3)$$

которая образуется заменой знака + на 0, а – на 1 соответствующей матрицы, принадлежащей пространству оригиналов.

Бинарные системы Уолша $\boldsymbol{W}_N$, подобные (3), можно представить $(n,N)-$*сокращенными матрицами* $\boldsymbol{Q}_N$, число строк (*базисных функций*) которых n совпадает со степенью двойки в порядке N системы $\boldsymbol{W}_N$. Для матрицы (3) имеем

$$\boldsymbol{Q}_c=\begin{array}{c} \\ 1\\2\\4\\ \downarrow k\end{array}\begin{array}{c}\begin{array}{cccccccc}0&1&2&3&4&5&6&7&\rightarrow t\end{array}\\ \begin{bmatrix}0&0&1&1&1&1&0&0\\0&1&1&0&0&1&1&0\\0&1&0&1&0&1&0&1\end{bmatrix}\end{array}. \qquad (4)$$

От сокращенных форм систем Уолша, например, (4), легко переходим к их полным формам (3). В самом деле, базисные функции нулевого порядка восстанавливаются тривиально, а оставшиеся функции однозначно составляются из функций, уже имеющихся в сокращенных матрицах систем Уолша. В частности, например, базисная функция третьего порядка вычисляется преобразованием

$$c(3,t) = F\left\{c(2,t), c(1,t)\right\},$$

где $F-$ преобразование, которое сводится к поразрядному перемножению знаков базисных функций $c(2,t)$ и $c(1,t)$ систем Уолша в пространстве оригиналов, или поразрядному сложению элементов базисных функций по модулю 2 для систем в пространстве изображений.

Число столбцов сокращенной матрицы может быть сведено к числу её строк, если произвести отбор тех и только тех столбцов матрицы, номера которых t, как и номера строк k, являются степенью двойки. В результате редуцирования столбцов сокращенной матрицы (4) приходим к квадратной матрице

$$\hat{\boldsymbol{J}} = \begin{array}{c} \\ 1 \\ 2 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 4 \end{array} \rightarrow t \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{array},$$

которую назовем *первородной матрицей* систем функций Уолша.

Инверсией строк первородных матриц приводим их к правосторонне симметрическим индикаторным матрицам систем Уолша.

Решение прямой задачи Уолша предполагает последовательность вычислений, инверсную последовательности в обратной задаче Уолша.

Спектр сигналов в базисах Уолша

Утверждение. *Индикаторные матрицы систем функций Уолша $N-$го порядка однозначно определяют правило перестановки номеров отсчетов t, дискретного сигнала $x(t)$ на входе процессора БПФ, формирующего дискретный спектр сигнала $\boldsymbol{X}(k)$, $k = \overline{0,N-1}$, в базисе $\boldsymbol{W}_N$. Правило перестановки номеров отсчетов входного сигнала задается соотношением*

$$l = t \cdot (\mathbf{1} \cdot \bar{\boldsymbol{J}}), \quad t = \overline{0,N-1}, \qquad (5)$$

в котором $\bar{\boldsymbol{J}}$ – матрица, обратная ИМ $\boldsymbol{J}$, а $\mathbf{1}$ – матрица инверсной перестановки.

Дерево БПФ, составленное по схеме Кули-Тьюки из операторов «бабочка» для ряда систем Уолша, будет иметь вид, показанный на рис. 3.

Колонки $\boldsymbol{H}$, $\boldsymbol{P}$ и $\boldsymbol{C}$ дерева отвечают номерам t отсчетов сигнала при формировании спектра в базисах Уолша-Адамара, Уолша-Пэли и Уолша-Кули соответственно.

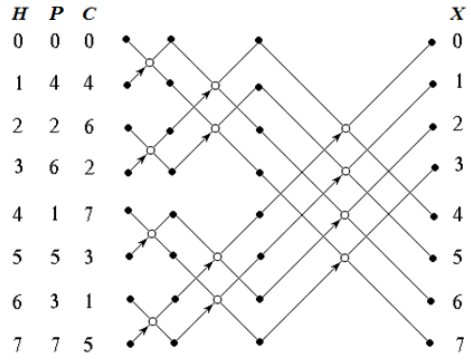

Рисунок 3. Дерево восьмиточечного БПФ с прореживанием по времени

ВЫВОДЫ

Таким образом, установлено, что индикаторные матрицы систем функций Уолша обладают рядом замечательных свойств. Во-первых, они могут быть не только легко программно рассчитаны на компьютерах, но и, во-вторых, однозначно определяют как структуру системы Уолша $\boldsymbol{W}$, так и порядок расположения номеров t отсчетов дискретного сигнала $x(t)$ на входе процессора БПФ, формирующего спектр сигнала в произвольном базисе $\boldsymbol{W}$. Тем самым проблема рандомизации матриц Уолша $\boldsymbol{W}$, ранее решавшаяся с целью построения алгоритмов БПФ, теряет свою актуальность.

И, наконец, ИМ функций Уолша большого порядка имеют хорошую перспективу применения в системах КЗИ. В самом деле, в условиях априорной неопределенности относительно базиса $\boldsymbol{W}$ противнику потребуются значительные дорогостоящие ресурсы для взлома ключа шифрования (базиса $\boldsymbol{W}$) и за время, потраченное на вычисление базиса, зашифрованные данные, скорее всего, потеряют свою актуальность.

ЛИТЕРАТУРА REFERENCES

[1] Hadamard M. J., Buii. Sci. Math, 1898, A17, 240.

[2] Walsh I. L. Amer. J. Math., 1923, 45, 5.

[3] Paley B. E. Proc. London Math. Soc. (2), 1932, 34, 241.

[4] Белецкий А. Я. Индикаторные матрицы систем функций Уолша. / А. Я. Белецкий. // Вісник СумДУ. Серія Технічни науки, № 4, 2009. – С. 85-93.

[5] Артемьев М. Ю. О формировании симметрических систем функций Виленкина-Крестенсона. / М. Ю. Артемьев, Г. П. Гаев, Т. Э. Кренкель, А. П. Скотников // Радиотехника и электроника, 1978, № 7, с. 1432-1440.

[6] Белецкий А. Я. Комбинаторика кодов Грея. — Научное издание. / А. Я. Белецкий. — К.: Изд. компания «Квіц», 2003. – 506 с.

[7] Ен. Функции Уолша и код Грея. // Зарубежная радиоэлектроника, № 7, 1972. – С. 27-35.

[8] Белецкий А. Я. Коды Грея. — Научное издание. / А. Я. Белецкий. — К.: Изд. компания «Квіц», 2002. – 150 с.