УДК 519.711/.22(02)

КРИПТОГРАФИЧЕСКИЕ ПРИЛОЖЕНИЯ ИНДИКАТОРНЫХ МАТРИЦ СИСТЕМ ФУНКЦИЙ УОЛША

Анатолий Белецкий

В статье рассматриваются вопросы формирования и криптографических приложений симметричных систем функций Уолша двоично степенного порядка. Синтез систем осуществляется на основе их индикаторных матриц. Индикаторными являются правосторонне симметрические (0,1)-матрицы, т.е. матрицы, симметричные относительно вспомогательной диагонали, невырожденные в кольце вычетов по модулю 2. Порядок индикаторных матриц логарифмически связан с порядком систем Уолша. Решение отмеченной проблемы синтеза составляет так называемую прямую задачу Уолша. Обратная задача состоит в том, чтобы по заданной матрице системы Уолша вычислить её индикаторную матрицу. Обсуждается проблема разработки алгоритмов криптографической защиты пакетов видеосигналов, передаваемых по радиоканалу с борта беспилотного летательного аппарата на Землю. Криптопреобразование сводится к двумерному быстрому преобразованию Фурье видеосигнала в базисе систем функций Уолша, защищенных от несанкционированного доступа. Устанавливается правило перестановки отсчетов дискретного сигнала на входе процессора БПФ, обеспечивающее вычисление спектра сигнала в заданном базисе функций Уолша.

Ключевые слова: *системы функций Уолша, индикаторные матрицы систем Уолша, обобщенные коды Грея, дискретное двумерное преобразование Фурье, криптографическая защита пакетов видеосигнала.*

1. Введение и постановка задачи.

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 $\boldsymbol{H}_N$, разработана Адамаром (Hadamard) в 1893 году [1]. Матрица Адамара восьмого порядка имеет вид

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

где k и t – номер (порядок) и аргумент (дискретное время) базисной функции $h(k,n)$ системы $\boldsymbol{H}_N$.

Упорядочивая функции $h(k,n)$ систем Адамара $\boldsymbol{H}_N$ 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].

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

И, наконец, в 1932 году математиком Пэли (Paley) предложена третья (и, можно сказать, последняя структурированная) система Уолша-Пэли [3].

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

В статье 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*. Аналогично можно говорить об $m-$ ично степенном порядке $N = m^n$ дискретных Виленкина-Крестенсона функций [4-6], частным случаем которых, $m = 2$, являются системы функций Уолша. Степень n это натуральные числа, совпадающие с порядком *индикаторной матрицы* (ИМ) $\boldsymbol{J}_w$ системы $\boldsymbol{W}_N$ [7]. Определение ИМ дается ниже по тексту.

В работах [8, 9] получена оценка $L(n)$ числа симметричных систем функций Уолша в зависимости от порядка n ИМ систем:

$$L(n) = \prod_{i=1}^{n} (2^i - (i)_2), \qquad (4)$$

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

Номера (порядки) базисных функций k_w систем Уолша, упорядоченных по Адамару (1), Качмажу (2) и Пэли (3), связаны (рис. 1), как впервые отмечено в [10], кодами Грея [11].

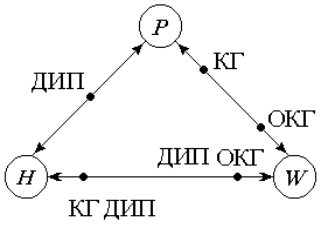

Рис. 1. Взаимосвязь номеров базисных функций в системах Уолша (1)-(3)

Аббревиатурами на рис. 1 обозначены операторы: ДИП – двоично-инверсной перестановки, КГ – прямого кодирования Грея и ОКГ – обратного кодирования Грея.

Согласно рис. 1, номера базисных функций систем Адамара k_h и Пэли k_p биективно связаны оператором ДИП, что соответствует таким преобразованиям:

$$k_p = k_h \cdot \boldsymbol{I}; \quad k_h = k_p \cdot \boldsymbol{I}, \qquad (5)$$

где $\boldsymbol{I} -$ матрица инверсной перестановки (МИП), известная также как *обменная* матрица [12], т.е. матрица, на элементах вспомогательной диагонали которой располагаются единицы, а в оставшихся элементах – нули. Матрицу $\boldsymbol{I}$ будем также обозначать как $\mathbf{1}$ (см. табл. 1).

Матрица инверсной перестановки $\boldsymbol{I}$ (или $\mathbf{1}$), например, для систем Уолша восьмого порядка, $n = 3$, выглядит следующим образом

$$\boldsymbol{I} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \qquad (6)$$

Далее, пару преобразований $\boldsymbol{P} \leftrightarrow \boldsymbol{W}$ можно отобразить формулами

$$k_w = k_p \cdot \bar{\boldsymbol{G}}; \quad k_p = k_w \cdot \boldsymbol{G},$$

где

$$\boldsymbol{G} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}; \quad \bar{\boldsymbol{G}} = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}, \qquad (7)$$

есть матрицы прямого $\boldsymbol{G}$ и обратного $\bar{\boldsymbol{G}}$ преобразований Грея соответственно.

И, наконец, согласно рис. 1, имеем

$$k_w = k_h \cdot \boldsymbol{I} \cdot \bar{\boldsymbol{G}}; \quad k_h = k_w \cdot \boldsymbol{G} \cdot \boldsymbol{I}. \qquad (8)$$

Подставив матрицы (6) и (7) в равенства (8), получим

$$k_w = k_h \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}; \qquad (9)$$

$$k_h = k_w \cdot \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \qquad (10)$$

Из соотношений (7)-(10) следует, что умножение квадратной матрицы на МИП слева эквивалентно инверсии строк, а справа – инверсии столбцов этой матрицы.

Тремя *классическими системами* $\boldsymbol{H}$, $\boldsymbol{W}$ и $\boldsymbol{P}$ (рис. 1), не исчерпывается все множество симметричных систем Уолша. Согласно оценке (4) всего существует 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 преобразовании.

Вместе с тем, можно построить схему преобразования кодов, обратную по направлению классическому (*левостороннему*) преобразованию Грея. В таком классе кодов Грея, названном *правосторонним преобразованием* [13], при прямом и обратном преобразовании сохраняется неизменным значение младшего (правого) разряда преобразуемого кода.

Совокупность перечисленных выше *простых кодов Грея* (ПКГ), именуемые также как операторы Грея, сведена в табл. 1.

Таблица 1

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

Матричные формы ПКГ третьего порядка показаны в табл. 2.

Таблица 2

Матричные формы простых операторов Грея

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

Комбинация лево- и правостороннего преобразований (кодов) Грея (ПГ) как прямого, так и обратного, совместно с оператором инверсной перестановки и операторами циклического сдвига (лево- и правостороннего) привела к возможности построения комбинированных или *составных кодов Грея* [14].

Составными кодами Грея (СКГ) G $k-$го порядка являются коды, образованные произведением k простых кодов, т.е.

$$G=\prod_{i=1}^{k} g_i, \quad g_i \in \{0,1,\ldots,7\}. \qquad (11)$$

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 матричных операторов, расположенных в строках табл. 2, за исключением матриц верхней строки, равно единичной матрице 0 (или e).

Множество ПКГ (табл. 1 и 2) и на их основе – СКГ (11) дают возможность установить [6, 9, 14] взаимосвязь (рис. 2) всех 28 симметричных систем Уолша восьмого порядка.

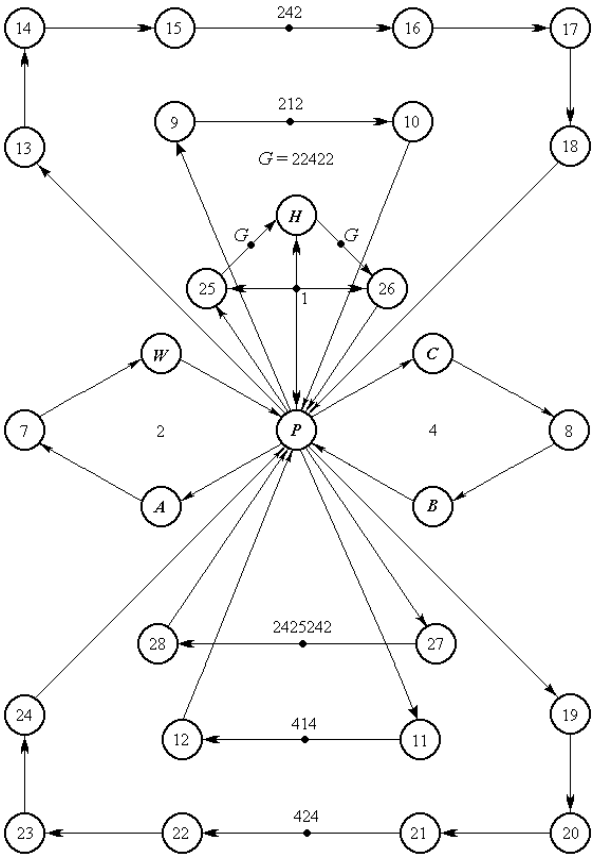

Рис. 2. Полный граф Пэли-связанных систем Уолша восьмого порядка

Индикаторные матрицы $\boldsymbol{J}_w$ симметричных систем Уолша $\boldsymbol{W}$ восьмого порядка, за исключением ИМ системы Уолша-Пэли $\boldsymbol{J}_p$ (единичной матрицы $\boldsymbol{E}$), сведены в табл. 3.

Таблица 3

Индикаторные матрицы систем функций Уолша восьмого порядка

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

Как показали результаты машинного анализа числа $L(n)$ индикаторных матриц систем Уолша, программно вычисленные на компьютерах для ряда значений n, совпадают с аналитической оценкой (4) этих чисел.

На основании данных табл. 3 сформулируем определение ИМ $\boldsymbol{J}_w$ систем Уолша $\boldsymbol{W}$.

Определение. *Индикаторными матрицами* $\boldsymbol{J}_w$ *систем функций Уолша* $\boldsymbol{W}$ *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, невырожденные в кольце вычетов по модулю 2.*

Согласно рис. 2 для определения полного множества систем Уолша восьмого порядка оказалось достаточным воспользоваться лишь шестью первыми (из восьми) простыми операторами Грея (табл. 2). Как показали результаты анализа такими же простыми, но уже четвертого порядка, и на их основе – составными кодами Грея, удалось связать (и, тем самым, определить структуру) только 126 из 448 систем Уолша 16-го порядка. Если же задействовать все простые операторы Грея $g\in\{0,1,\ldots,7\}$, то Пэли-связанными становятся все системы Уолша 16-го порядка.

Из табл. 3 следует, что ИМ $\boldsymbol{J}_{27}$ является оператором циклического сдвига на один разряд вправо (оператор 6 в табл. 2), а ИМ $\boldsymbol{J}_{28}-$ на один разряд влево (простой оператор 7). Поэтому, как следует из рис. 2, операторы 6 и 7 могут быть выражены произведениями простых кодов Грея $g_i\in\{2,3,4,5\}$ в виде

$$6=2425242;\quad 7=3534353.$$

Обратимся к графу, представленному на рис. 2. В этом графе, например, кружок, содержащий число 19, означает, что 19-я симметричная система Уолша $\boldsymbol{W}$ образуется в результате перестановки номеров базисных функций системы Уолша-Качмажа $\boldsymbol{P}$ составным кодом Грея $G=424$.

Выбирая из табл. 2 матричные формы простых операторов 2 и 4, приходим к такому выражению для СКГ

$$\boldsymbol{J}_{19}=\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}\cdot\begin{bmatrix}1&1&0\\0&1&1\\0&0&1\end{bmatrix}\cdot\begin{bmatrix}1&0&0\\1&1&0\\0&1&1\end{bmatrix}. \qquad (12)$$

Примем во внимание, что матричные преобразования в (12) выполняются в кольце вычетов по модулю 2. Следовательно

$$\boldsymbol{J}_{19}=\begin{bmatrix}0&1&0\\1&1&1\\1&1&0\end{bmatrix}. \qquad (13)$$

Матрица (13) однозначно определяет 19-ю систему функций Уолша $\boldsymbol{W}$ и является ИМ этой системы. Соответствие между номерами k_p базисных функций Уолша-Пэли и номерами k_{19} базисных функций 19-й системы Уолша, вычисляется соотношением

$$k_{19}=k_p\cdot\boldsymbol{J}_{19}. \qquad (14)$$

Переставляя базисные функции системы $\boldsymbol{P}$, заданной равенством (3), по правилу (14), получим

матрицу $\boldsymbol{W}_{19}$ 19-й системы функций Уолша восьмого порядка

$$\boldsymbol{W}_{19} = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ k \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \quad t \\ \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & - & - & - & - & + & + \\ + & - & + & - & + & - & + & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & - & + & - & + \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & - & - & + & - & + & + & - \end{bmatrix} \end{array} .$$

Основная цель данной статьи состоит в разработке алгоритма криптографической защиты пакетов видеоинформации (КЗИ), передаваемых по радиоканалу с борта беспилотного летательного аппарата (БПЛА) на наземный пункт управления (НПУ). В качестве метода КЗИ предлагается использовать двумерное быстрое преобразование Фурье (БПФ) дискретных видеосигналов в базисах систем функций Уолша высокого порядка ($N \geq 256$), стохастически выбираемых из большого числа этих систем, что затрудняет противнику несанкционированный доступ к базисам БПФ.

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 Уолша, исключая необходимость факторизации матриц Уолша.

2. Прямая и обратная задачи Уолша [15]. 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 $\boldsymbol{W}_N$.

Первой рассмотрим более простую задачу, которой является обратная задача Уолша.

Обратная задача Уолша

Последовательность вычислений при решении обратной задачи рассмотрим на примере системы функций Уолша восьмого порядка.

1) Пусть задана симметричная система Уолша в пространстве оригиналов. Обозначим её $\boldsymbol{C}_8^*$,

$$\boldsymbol{C}_8^* = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ k \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \quad t \\ \begin{bmatrix} + & + & + & + & + & + & + & + \\ + & + & - & - & - & - & + & + \\ + & - & - & + & + & - & - & + \\ + & - & + & - & - & + & - & + \\ + & - & + & - & + & - & + & - \\ + & - & - & + & - & + & + & - \\ + & + & - & - & + & + & - & - \\ + & + & + & + & - & - & - & - \end{bmatrix} \end{array} . \quad (15)$$

2) Произведя замену знака + на цифру 0, а – на 1, перейдем от *знакопеременной формы* представления системы функций Уолша (15) к ее *бинарной форме* $\boldsymbol{C}_8$ (в пространстве изображений)

$$\boldsymbol{C}_8 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ k \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \quad t \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \end{array} . \quad (16)$$

Знакопеременные (из пространства оригиналов) и бинарные системы Уолша можно представить в сокращенных формах $\boldsymbol{Q}_N$, включив в них базисные функции, порядок которых k равен степени числа 2. Для систем (15) и (16) имеем

$$\boldsymbol{Q}_8^* = \begin{array}{c} \\ 1 \\ 2 \\ 4 \\ \downarrow k \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \quad \rightarrow t \\ \begin{bmatrix} + & + & - & - & - & - & + & + \\ + & - & - & + & + & - & - & + \\ + & - & + & - & + & - & + & - \end{bmatrix} \end{array} , \quad (17)$$

$$\boldsymbol{Q}_8 = \begin{array}{c} \\ 1 \\ 2 \\ 4 \\ \downarrow k \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \rightarrow t \\ \begin{bmatrix} 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array} . \quad (18)$$

Прямоугольные $(n, N)-$матрицы $\boldsymbol{Q}$ (17) и (18), где $n-$ число строк и $N-$ число столбцов, назовем *сокращенными матрицами систем Уолша.*

От сокращенных форм систем Уолша, например, (17) и (18), легко переходим к их полным формам (15) и (16). В самом деле, базисные функции нулевого порядка $c(0,t)$ восстанавливаются тривиально, а функции порядка $k \neq 2^j$ однозначно определяются набором функций, порядок которых является степенью двойки, т.е. недостающие функции составляются из функций, уже имеющихся в сокращенных матрицах систем Уолша. В частности, базисная функция третьего порядка $c(3,t)$ вычисляется преобразованием функций $c(1,t)$ и $c(2,t)$, что отобразим выражением

$$c(3,t) = F\{c(2,t), c(1,t)\}, \quad (19)$$

где $F-$ преобразование, которое сводится к поразрядному перемножению знаков базисных функций для знакопеременных форм систем Уолша (15) и поразрядному сложению элементов базисных функций по модулю 2 в том случае, когда система Уолша представлена в бинарной форме (16).

Подобно преобразованию (19) для оставшихся систем функций Уолша восьмого порядка получим

$$\begin{aligned} c(5,t) &= F\{c(4,t), c(1,t)\}, \\ c(6,t) &= F\{c(4,t), c(2,t)\}, \\ c(7,t) &= F\{c(4,t), c(2,t), c(1,t)\}. \end{aligned} \quad (20)$$

Преобразования (19) и (20) подобны способу составления произвольных $n-$битных чисел из набора n ортонормированных векторов:

$$\begin{aligned} 2^0 &= 0 \ \cdots \ 0 \ 1; \\ 2^1 &= 0 \ \cdots \ 1 \ 0; \\ \cdots &\ \cdots \ \cdots \ \cdots \ \cdots; \\ 2^n &= 1 \ \cdots \ 0 \ 0; \end{aligned}$$

3) 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, т.е. $t = 2^i$, $i = \overline{0, n-1}$. В результате описанного редуцирования столбцов сокращенных матриц (17) и (18) приходим к квадратным матрицам $\hat{\boldsymbol{J}}$, которые назовем *первородными матрицами систем функций Уолша.*

$$\hat{\boldsymbol{J}}^* = \begin{array}{c} \\ 1 \\ 2 \\ 4 \\ \downarrow k \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 4 \end{array} \rightarrow t \\ \begin{bmatrix} + & - & - \\ - & - & + \\ - & + & + \end{bmatrix} \end{array} , \quad (21)$$

$$\hat{\boldsymbol{J}} = \begin{array}{c} \\ 1 \\ 2 \\ 4 \\ \downarrow k \end{array} \begin{array}{c} \begin{array}{ccc} 1 & 2 & 4 \end{array} \rightarrow t \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \end{array} . \quad (22)$$

Обратим внимание на то, что матрицы (21) и (22) обладают *левосторонней симметрией*, тогда как индикаторные матрицы $\boldsymbol{J}$ систем Уолша $\boldsymbol{W}$ являются *правосторонне симметрическими.*

4) Инверсией строк бинарных первородных-матрицы $\hat{\boldsymbol{J}}$ приводим их к правосторонне симметрическим индикаторным матрицам $\boldsymbol{J}$ систем функций Уолша $\boldsymbol{W}$.

Инверсия строк первородной матрицы реализуется посредством МИП по формуле

$$\boldsymbol{J} = \mathbf{1} \cdot \hat{\boldsymbol{J}}. \quad (23)$$

Из соотношений (6), (22) и (23) получим

$$\boldsymbol{J} = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}. \quad (24)$$

Матрица (24) как раз и является ИМ $\boldsymbol{J}_c$ системы Уолша $\boldsymbol{C}$, названой системой Уолша-Кули, поскольку впервые была получена на основе дерева БПФ по схеме Кули-Тьюки [16]. Отличительная особенность системы $\boldsymbol{C}$ состоит в том, что она, будучи используемой в качестве базиса ДПФ (или БПФ), является единственной симметричной системой функций Уолша двоично степенного порядка, доставляющей линейную связанность частотным шкалам процессора БПФ [6, 9].

Прямая задача Уолша

Естественно, что решение прямой задачи Уолша предполагает выполнение вычислений в последовательности, инверсной последовательности вычислений для обратной задачи Уолша, т.е. первым выполняется п. 5, затем 4 и т.д.

Пройдемся по этой цепочке вычислений. Предположим, что индикаторная матрица $\boldsymbol{J}$ системы функций Уолша задана соотношением (24). Искомая система Уолша $\boldsymbol{W}$ может быть определена в результате таких последовательных шагов преобразований индикаторной матрицы.

1) Инвертируя строки индикаторной матрицы $\boldsymbol{J}$ (24), получим первородную матрицу $\hat{\boldsymbol{J}}$ системы Уолша (22).

2) От первородной матрицы (22) преобразованиями (20) приходим к образующей матрице $\boldsymbol{Q}$ (18).

3) На основании образующей матрицы $\boldsymbol{Q}$ (18) восстанавливаем бинарную форму системы функций Уолша (16).

4) Заменой в (16) цифр 0 знаком +, а 1 знаком –, получим системы Уолша восьмого порядка (15) из пространства оригиналов.

3. Синтез индикаторных матриц систем функций Уолша. Напомним, что ИМ систем Уолша должны удовлетворять следующим двум требованиям. Во-первых, индикаторные матрицы должны быть правосторонне симметрическими. И, во-вторых, определитель ИМ по модулю 2 должен быть равен 1.

Алгоритм формирования ИМ поясним на примере матриц четвертого порядка. В качестве одного из вариантов можно предложить такую последовательность циклического заполнения элементов матрицы 4x4 бинарными числами.

$$\boldsymbol{M} = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & \\ 8 & 9 & & \\ 10 & & & \end{bmatrix}.$$

Оставшиеся пустыми элементы тестируемой матрицы $\boldsymbol{M}$ определяются, согласно принципу правосторонней симметрии, значениями:

$$b_{24} = b_{13}; \quad b_{33} = b_{22}; \quad b_{34} = b_{12};$$
$$b_{42} = b_{31}; \quad b_{43} = b_{21}; \quad b_{44} = b_{11},$$

где $b_{ij} \in \{0,1\}$ – содержимое $ij-$й ячейки матрицы $\boldsymbol{M}$.

Циклы переопределения элементов матрицы $\boldsymbol{M}$ организуются таким образом, что элемент 1 соответствует внешнему, а 10 – внутреннему циклу. Матрица $\boldsymbol{M}$ отбраковывается, если ее определитель по модулю 2 равен 0 и включается в состав ИМ, если определитель равен 1.

Первые восемь ИМ четвертого порядка, взятые из Приложения 1 [6], показаны в табл. 4.

Таблица 4

Пример индикаторных матриц четвертого порядка

ИМ 1				ИМ 2			
0	0	0	1	0	0	0	1
0	0	1	0	0	1	0	0
0	1	0	0	0	0	1	0
1	0	0	0	1	0	0	0
ИМ 3				ИМ 4			
0	0	0	1	0	0	0	1
0	1	1	0	0	1	0	0
0	0	1	0	0	1	1	0
1	0	0	0	1	0	0	0
ИМ 5				ИМ 6			
0	0	1	0	0	0	1	1
0	0	0	1	0	0	0	1
0	1	0	0	0	1	0	0
1	0	0	0	1	0	0	0
ИМ 7				ИМ 8			
0	0	1	0	0	0	1	1
0	0	1	1	0	1	0	1
0	1	0	0	0	0	1	0
1	0	0	0	1	0	0	0

4. Вычисление спектра дискретных сигналов в заданном базисе функций Уолша. Обратим внимание на важнейшее свойство индикаторных матриц систем Уолша, которое сформулируем в виде следующего утверждения.

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

$$l = t \cdot (\mathbf{1} \cdot \bar{\boldsymbol{J}}),\ t = \overline{0, N-1}, \qquad (25)$$

где $\bar{\boldsymbol{J}}$ – матрица, обратная ИМ $\boldsymbol{J}$; $\mathbf{1}$ – перестановочная матрица.

Известно [17], что если на вход процессора БПФ, реализующего схему Кули-Тьюки, подведены отсчеты входных сигналов $x(l)$, номера которых l расставлены в естественной последовательности $l = \overline{0, N-1}$, то на выходе процессора образуется спектр сигнала $\boldsymbol{X}(k)$, $k = \overline{0, N-1}$, в базисе функций Уолша-Адамара.

Если же номера l отсчетов сигнала $x(l)$ подвергнуть двоично инверсной перестановке, то формируемый на выходе процессора БПФ спектр будет соответствовать спектру сигнала в базисе функций Уолша-Пели $\boldsymbol{P}$.

Оба приведенные выше факта подтверждают достоверность соотношения (25) Утверждения. В самом деле, ИМ системы функций Уолша-Адамара $\boldsymbol{H}$ является матрица инверсной перестановки (МИП), т.е. $\boldsymbol{J}=\mathbf{1}$, пример которой приведен выражением (6). Матрица $\overline{\mathbf{1}}$ совпадает с МИП, а произведение $\mathbf{1}\cdot\overline{\boldsymbol{J}}=\mathbf{1}\cdot\overline{\mathbf{1}}$ равняется единичной матрице $\boldsymbol{E}$. Последнее, согласно (25), означает, что для формирования спектра в базисе Уолша-Адамара $\boldsymbol{H}$ отсчеты l сигнала на входе процессора должны быть расставлены в естественном порядке 0,1,…, N-1, как и отсчеты t.

Далее, ИМ системы Уолша-Пели $\boldsymbol{P}$ является единичная матрица $\boldsymbol{E}$, для которой $\overline{\boldsymbol{E}}=\boldsymbol{E}$ и $\mathbf{1}\cdot\boldsymbol{E}=\mathbf{1}$. Следовательно, для формирования спектра в базисе Уолша-Пэли номера отсчетов сигнала на входе процессора БПФ должны образовывать двоично инверсную последовательность.

Для получения спектра $\boldsymbol{X}(k)$ в любом другом базисе $\boldsymbol{H}$, отличном от базиса Уолша-Адамара $\boldsymbol{H}$ или Уолша-Пэли $\boldsymbol{P}$, достаточно переопределить номера l отсчетов входного сигнала $x(l)$ преобразованием (25). Подтвердим это правило на конкретном примере.

Выберем в качестве базиса восьмиточечного процессора БПФ систему функций Уолша-Кули $\boldsymbol{C}_8$ (16). Базису $\boldsymbol{C}_8$ соответствует ИМ (24). Следовательно

$$\overline{\boldsymbol{J}}_C=\begin{bmatrix}1&0&0\\1&1&0\\1&1&1\end{bmatrix}$$

и

$$\mathbf{1}\cdot\overline{\boldsymbol{J}}_c=\begin{bmatrix}1&1&1\\1&1&0\\1&0&0\end{bmatrix}. \qquad (26)$$

На основании соотношений (25) и (26) составим табл. 5 перестановок номеров t отсчетов дискретного сигнала $x(t)$, подводимых к входу процессора БПФ.

Таблица 5

К вычислению номеров l отсчетов сигнала на входе процессора БПФ в базисе $\boldsymbol{C}_8$

t	0	1	2	3	4	5	6	7
l	0	4	6	2	7	3	1	5

С учетом строки l табл. 5 дерево БПФ по схеме Кули-Тьюки, составленной из операторов «бабочка» (рис. 3), будет иметь вид, показанный на рис. 4.

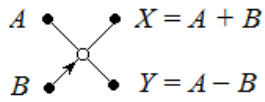

Рис. 3. Преобразования, реализуемые оператором «бабочка»

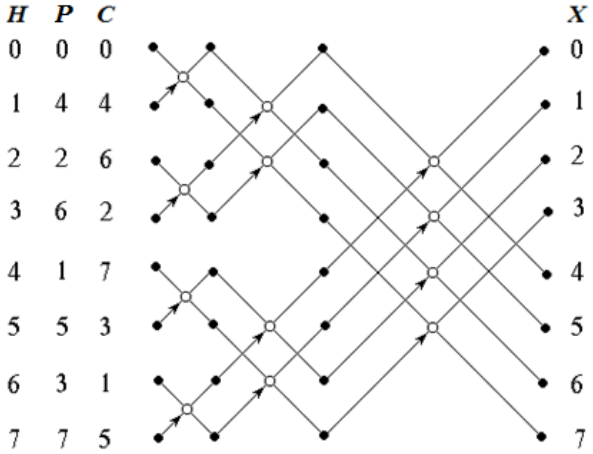

Рис. 4. Дерево восьмиточечного БПФ с прореживанием по времени

Колонки $\boldsymbol{H}$, $\boldsymbol{P}$ и $\boldsymbol{C}$ (рис. 4) соответствуют последовательностям номеров отсчетов сигнала при формировании спектра в базисах Уолша-Адамара, Уолша-Пэли и Уолша-Кули соответственно, а колонка содержит последовательность гармоник спектра (точнее – коэффициентов ряда Фурье). Результаты вычисления спектральных компонент сигнала в базисе функций Уолша-Кули в первых двух ступенях преобразования восьмиточечного процессора БПФ размещены в прямоугольных окнах на рис. 5.

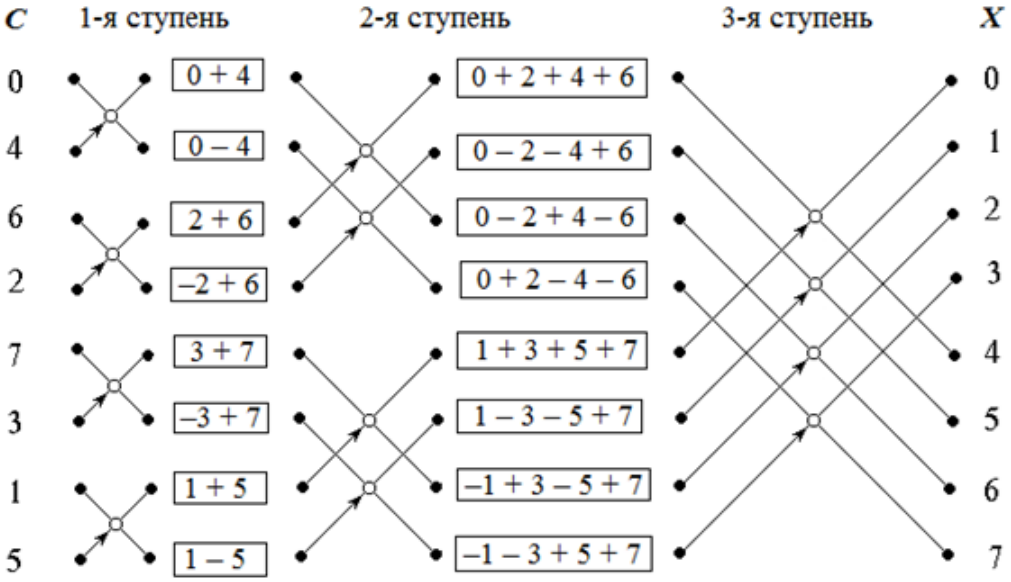

Рис. 5. К вычислению спектра сигнала в базисе функций Уолша-Кули

Сведем в табл. 6 результаты вычисления коэффициентов спектра $\boldsymbol{X} = \{X(k,l)\}$ третьей ступенью процессор БПФ (рис. 5), сохраняя в ячейках таблицы лишь знаки отсчетов сигнала, с которыми отсчеты входят в компоненты спектра.

Таблица 6

Составляющие спектральных компонент

	0	1	2	3	4	5	6	7	$\rightarrow t$
0	+	+	+	+	+	+	+	+	
1	+	+	−	−	−	−	+	+	
2	+	−	−	+	+	−	−	+	
3	+	−	+	−	−	+	−	+	
4	+	−	+	−	+	−	+	−	
5	+	−	−	+	−	+	+	−	
6	+	+	−	−	+	+	−	−	
7	+	+	+	+	−	−	−	−	

$\downarrow k$

Сопоставляя данные табл. 6 и матрицы (16), приходим к заключению, что расстановка $\boldsymbol{C}$ отсчетов сигналов (рис. 4) на входе процессора БПФ по схеме Кули-Тьюки приводит к формированию спектра в базисе Уолша-Кули (выделенному в табл. 5 жирными линиями). А это является дополнительным подтверждением правоты Утверждения 1, что приводит к такому важнейшему следствию.

Следствие 1. *Проблема рандомизации матриц систем функций Уолша* $\boldsymbol{W}$, *ранее решавшаяся с целью построения алгоритмов БПФ в базисах* $\boldsymbol{W}$, *теряет свою актуальность, поскольку формирование спектра дискретного сигнала* $x(t)$, $t = 0,1,\ldots,N-1$, $N = 2^n$, $n \geq 2$, *в том или ином базисе* $\boldsymbol{W}$ *двоично степенного порядка* N *достигается простой перестановкой номеров* t *отчетов сигнала* $x(t)$ *на входе процессора БПФ по формуле* (25), *т.е. однозначно определяется индикаторной матрицей* $\boldsymbol{J}$ *системы функций* $\boldsymbol{W}$.

5. Обсуждение результатов. И так, мы убедились в том, ИМ 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 самой системы Уолша, так и порядок расположения номеров t отсчетов дискретного сигнала $x(t)$ на входе процессора БПФ, формирующего спектр сигнала в произвольном базисе $\boldsymbol{W}$.

Согласно выражению (4) всего существует $L(8) = 28'897'705'984$ индикаторных матриц систем Уолша восьмого порядка, т.е.

$$2^{34} < L(8) < 2^{35},$$

а это уже достаточно большое число. Системы функций $\boldsymbol{W}$, вычисленные на основании этих ИМ, могут быть использованы, например, для организации криптографической защиты пакетов видеосигналов, передаваемых с борта беспилотного летательного аппарата (БПЛА) на наземный пункт управления (НПУ).

Пусть случайным образом выбрана одна из $L(8)$ индикаторных матриц $\boldsymbol{J}$ восьмого порядка, доступная легализованным абонентам A и B сети связи и априори неизвестная противнику. Этой ИМ однозначно соответствует матрица $\boldsymbol{W}$ сис-

темы функций Уолша 256 порядка. Используя матрицу $\boldsymbol{W}$ в качестве базиса БПФ, абонент A, в качестве которого будем предполагать микроконтроллер (МК) бортовой аппаратуры БПЛА, формирует двумерный спектр $\boldsymbol{X}$ пакета, состоящего из 256 отсчетов видеосигналов $\boldsymbol{x}(t)$, $t = \overline{0,255}$, соответствующих некоторому первичному двумерному изображению Ξ.

Абонент B (МК НПУ) на основании пакета $\boldsymbol{X}$, переданного по радиоканалу, процессором БПФ в базисе функций $\boldsymbol{W}$ восстанавливает исходный пакет видеосигналов $\boldsymbol{x}(t)$ – первичное изображение Ξ.

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 $\boldsymbol{W}$, зашифрованные данные, скорее всего, потеряют свою актуальность.

Выводы. На основе правосторонне симметричных индикаторных матриц систем функций Уолша $\boldsymbol{J}$ $n-$ го порядка, где $n-$ натуральное число, разработаны достаточные простые алгоритмы синтеза биективно связанных с матрицами $\boldsymbol{J}$ левосторонне симметричных (классических) систем функций Уолша $\boldsymbol{W}_N$ двоично степенного порядка $N = 2^n$.

Системы Уолша находят в настоящее время разнообразное применение в различных областях науки и техники. Перспективным является использование систем Уолша в криптографии для защиты пакетов видеосигналов, передаваемых по радиоканалу с борта БПЛА на НПУ.

Отмеченная проблема (защита видео изображений) лишь частично затронута в настоящей статье, и для её детализации необходимы дополнительные исследования.

ЛИТЕРАТУРА

[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]. Виленкин Н. Я. Об одном классе полных ортогональных систем. // Известия АН СССР. Сер. мат., 1949, № 3.
[5]. Chrestenson H. E. A class of generalired Walsh functions. // Pacific J. Math., 1955, v. 5.
[6]. Белецкий А. Я. Дискретные ортогональные базисы Виленкина-Крестенсона функций. — Научная монография. — Palmarium Academic Publishing, Germany, 2015. – 232 с. ISBN 978-3-659-60300-6.
[7]. Белецкий А. Я. Индикаторные матрицы систем функций Уолша. / А. Я. Белецкий. // Вісник СумДУ. Серія Технічни науки, № 4, 2009. – С. 85-93
[8]. 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.
[9]. Белецкий А. Я. Комбинаторика кодов Грея. — Научное издание. / А. Я. Белецкий. — К.: Изд. компания «Квіц», 2003. – 506 с.
[10]. Ен. Функции Уолша и код Грея. // Зарубежная радиоэлектроника, № 7, 1972. – С. 27-35.
[11]. Grey F. Pulse code communication. – Pat. USA, # 2632058, 1953.
[12]. Блейхут Р. Теория и практика кодов, контролирующих ошибки. / Р. Блейхут. – М.: Мир, 1986. – 576 с.
[13]. Белецкий А. Я. Коды Грея. — Научное издание. / А. Я. Белецкий. — К.: Изд. компания «Квіц», 2002. – 150 с.
[14]. Белецкий А. Я. Обобщенные коды Грея. — Научная монография. — Palmarium Academic Publishing, Germany, 2014. – 208 с. ISBN 978-3-639-68389-9.
[15]. Белецкий А.Я. Прямая и обратная задача Уолша. /А. Я. Белецкий, Е. А. Белецкий. — Тезисы МНК «АВИА-2013», Киев, НАУ, Том 4. – С. 24.36-24.39 [Электронный ресурс] avia.nau.edu.ua/doc/2013/AVIA2013_v4.pdf
[16]. Beletsky A. Ya. Syntesis and analysis of system of Wolsh-Cooly basis functions. Proceedings of XIII International Conference NIKON-2000. – Wroclaw, 2000.
[17]. Трахтман А. М. Основы теории дискретных сигналов на конечных интервалах. / А. М. Трахтман, В. А. Трахтман — М.: Сов. радио, 1975. – 208 с.

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]. Vilenkin N. Y. On a class of complete orthogonal systems. // Proceedings of the Academy of Sciences of the USSR. Ser. mat., 1949, № 3.
[5]. Chrestenson H. E. A class of generalired Walsh functions. // Pacific J. Math., 1955, v. 5/
[6]. Beletsky A. Ya. Discrete orthogonal bases Vilenkin-Christenson functions. — Scientific monograph. — Palmarium Academic Publishing, Germany, 2015. – 232 c. ISBN 978-3-659-60300-6.

[7]. Beletsky A. Ya. Indicator matrix system of Walsh functions. // Bulletin of Sum State University. A series of technical sciences, № 4, 2009. – P. 85-93
[8]. Artemyev, M. Yu., Baev G. P., Ernst T. E., Skotnikov A. P. On the formation of symmetric systems of functions Vilenkin-Christenson. // Radio Engineering and Electronics, 1978, № 7, pp. 1432-1440.
[9]. Beletsky A. Ya. Combinatorics Gray codes. — Scientific publication. — K.: Publishing House. Comp. "Kvits", 2003. – 506 p.
[10]. En. Walsh functions and the Gray code. // Foreign radioelectronics, № 7, 1972. – P. 27-35.
[11]. Grey F. Pulse code communication. — Pat. USA, # 2632058, 1953.
[12]. Blahut R. Theory and practice of error control codes. — M.: Mir, 1986. – 576 p.
[13]. Beletsky A. Ya. Gray codes. — Scientific publication. — K.: Publishing House. Comp. "Kvits", 2002. – 150 p.
[14]. Beletsky A. Ya. Generalized Gray codes. — Scientific publication. — Palmarium Academic Publishing, Germany, 2014. – 208 c. ISBN 978-3-639-68389-9.
[15]. Beletsky A. Ya., Beletsky E. A. The direct and inverse problem of Walsh. — Proc. of XI IRTC "AVIA-2013", Kiev, NAU, Vol 4. – P. 24.36-24.39 http:avia.nau.edu.ua/doc/2013/AVIA2013_v4.pdf
[16]. Beletsky A. Ya. Syntesis and analysis of system of Wolsh-Cooly basis functions. Proc. of XIII Int. Conference NIKON-2000. – Wroclaw, 2000.
[17]. Trakhtman A. M., Trakhtman V. A. Fundamentals of the theory of discrete signals on finite intervals. — M.: Sov. Radio, 1975. – 208 p.

КРИПТОГРАФІЧНІ ЗАСТОСУВАННЯ ІНДИКАТОРНИХ МАТРИЦЬ СИСТЕМ ФУНКЦІЙ УОЛША

У статті розглядаються питання формування та криптографічного застосування симетричних систем функцій Уолша двійково ступеневого порядку. Синтез систем здійснюється на основі їх індикаторних матриць. Індикаторними є правосторонні симетричні (0,1)-матриці, тобто матриці, симетричні щодо допоміжної діагоналі, невироджені в кільці відрахувань по модулю 2. Порядок індикаторних матриць знаходиться в логарифмічній залежності від порядку систем Уолша. Рішення зазначеної проблеми синтезу становить так звану пряму задачу Уолша. Зворотнє завдання полягає в тому, щоб по заданій матриці системи Уолша обчислити її індикаторну матрицю. Обговорюється проблема розробки алгоритмів криптографічного захисту пакетів відеосигналів, переданих по радіоканалу з борту безпілотного літального апарату. Криптоперетворення зводиться до двовимірного швидкого перетворення Фур'є відеосигналу в базисі систем функцій Уолша, захищених від несанкціонованого доступу. Встановлюється правило перестановки відкликів дискретного сигналу на вході процесора ШПФ, що забезпечує обчислення спектру сигналу в заданому базисі функцій Уолша.

Ключові слова: системи функцій Уолша, індикаторні матриці систем Уолша, узагальнені коди Грея, дискретне двовимірне перетворення Фур'є, криптографічний захист пакетів відеосигналу.

A CRYPTOGRAPHIC USE INDICATOR MATRICES SYSTEMS WALSH FUNCTIONS

The article deals with the formation and application of cryptographic systems, symmetric Walsh functions binary power order. A synthesis system is based on their indicator matrices. The indicator is right-sided symmetric (0,1)-matrix, i.e. matrix, symmetric with respect to the auxiliary diagonal, non-degenerate in the ring of residues modulo 2. The order of test matrices is a logarithmic dependence on the order of the Walsh system. The decision marked the problem of the synthesis of the so-called direct problem Walsh. The inverse problem is that for a given matrix of Walsh matrix to calculate its tally. The problem of the development of algorithms for cryptographic protection of video packets transmitted over the air on board unmanned aircraft. Kripto transform reduced to a two-dimensional fast Fourier transform in the basis of the video systems Walsh functions are protected from unauthorized access. Establishes the right permutation counts discrete input signal processor FFT calculates the spectrum of the signal in a given basis Walsh functions.

Keywords: system of Walsh functions, display matrix systems Walsh generalized Gray codes, two-dimensional discrete Fourier transform, cryptographic protection of video packets.

Білецький Анатолій Якович, доктор технічних наук, професор, заслужений діяч науки і техніки України, лауреат Державної премії України в галузі науки і техніки, професор кафедри електроніки Національного авіаційного університету.
E-mail: abelnau@ukr.net

Белецкий Анатолий Яковлевич, доктор технических наук, профессор, заслуженный деятель науки и техники Украины, лауреат Гос. премии Украины в области науки и техники, профессор кафедры электроники Нац. авиац. ун-та.

Beletsky Anatoly, Doctor of Science, Professor, Honored Scientist of Ukraine, Laureate of the State Prize of Ukraine in Science and Technology, Professor of Department Electronics of National Aviation University.