2. *Beaulieu R., Shors D., Smith J., et al.* The Simon and Speck Families Of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404, 2013.
3. *Abed F., List E., Lucks S., and Wenzel J.* Differential and Linear Cryptanalysis of Reduced-Round Simon. ePrint Archive, Report 2013/526, 2013.
4. *Vaudenay S.* On the Lai — Massey Scheme // ASIACRYPT'99. LNCS. 1999. V. 1716. P. 8–19.
5. *Biham E. and Shamir A.* Differential Cryptanalysis of the Data Encryption Standard. Berlin; Heidelberg: Springer, 1993.

УДК 004.056.55 DOI 10.17223/2226308X/13/36

КОДИРОВАНИЕ ИНФОРМАЦИИ МАТРИЦАМИ УОЛША

М. С. Беспалов, К. М. Малкова

Рассмотрено представление общей линейной группы $\mathrm{GL}(n,2)$ подгруппой автоморфизмов $\mathrm{GL}(N,2)$ при мультипликативной нотации в её действии в пространстве $\mathbb{R}^N$, где $N=2^n$. Каждая матрица как элемент группы $\mathrm{GL}(n,2)$ определяет упорядочения группы $\mathbb{Z}_2^n$ и её группы характеров, популярных при цифровой обработке информации в виде дискретных функций Уолша. На основе быстрого преобразования Уолша и данного соответствия создан программный прототип автоматической системы кодирования выходного сигнала в виде перестановки набора спектральных характеристик.

Ключевые слова: *дискретные функции Уолша, кодовая матрица, быстрое преобразование Уолша, кронекерово произведение.*

Для $\mathbb{Z}_2$ — аддитивной группы поля $\mathbb{F}_2$ — существуют разные представления, среди которых нас интересуют её мультипликативное представление $(\{1,-1\};\cdot)$ и векторное представление $(\{S,A\};\circ)$ с операцией умножения по Адамару векторов $S=(1\ 1)$, $A=(1\ -1)\in\mathbb{R}^2$. Для декартова произведения $\mathbb{Z}_2^n$ группы аддитивное представление рассматривается относительно операции $\oplus$ покоординатного сложения по модулю 2, а мультипликативное — относительно той же операции $\circ$ покоординатного умножения.

Популярные при цифровой обработке сигналов *дискретные функции Уолша* [1, 2] уровня n в работе [3] определены без привлечения нумерации как кронекерово произведение векторов S и A в количестве n сомножителей.

Теорема 1. Множество дискретных функций Уолша уровня n составляет подгруппу G мультипликативной группы $\mathbb{Z}_2^N$, где $N=2^n$, изоморфную группе $\mathbb{Z}_2^n$.

При декартовом произведении $\mathbb{Z}_2^n$ векторного представления $\mathbb{Z}_2=(\{S,A\};\circ)$ элементы будем записывать через разделительный знак $\otimes$, совпадающий с символом кронекерова произведения, что доказывает изоморфизм. Если перейдём к числам $S=(1\ 1)$ и $A=(1\ -1)$ и выполним кронекерово произведение, то получим элементы мультипликативной группы $\mathbb{Z}_2^N$. На основе свойства

$$(u\otimes v)\circ(w\otimes t)=(u\circ w)\otimes(v\circ t),$$

верного для $u,w\in\mathbb{R}^k$, $v,t\in\mathbb{R}^m$, устанавливается их групповое свойство.

Рассмотренная подгруппа $G\subseteq\mathbb{Z}_2^N$ составляет группу характеров конечной абелевой группы $\mathbb{Z}_2^n$, изоморфизм которых вытекает из теории двойственности Понтрягина [4].

Для решения задач цифровой обработки информации [2] эти группы нас интересуют в виде упорядоченных групп. В [5] подробно разбираются три известные нумерации

(Адамара, Пэли и Уолша) дискретных преобразований Уолша и высказывается сожаление об отсутствии других изученных «с точки зрения быстроты сходимости спектров при разложении сигналов и удобств практического применения». Рассматриваются перестановки на $N = 2^n$ элементах в виде двоичной инверсии и кода Грея, организующие переходы между нумерациями.

Определение 1 [3]. Назовём W-матрицей уровня n такую, что все её строки суть различные дискретные функции Уолша уровня n; все её столбцы — различные дискретные функции Уолша уровня n.

Таким образом, любая W-матрица V задаёт два линейных порядка на множестве всех дискретных функций Уолша выбранного уровня: по строкам и по столбцам для двух возможных способов кодирования $y = Vx$ и $y = xV$. Невырожденная матрица K как элемент общей линейной группы $\mathrm{GL}(n, 2)$ также задаёт два аналогичных линейных порядка элементов группы $\mathbb{Z}_2^n$. Так как матрица K, как показано далее, определяет порядок следования отсчётов выходного сигнала при цифровой обработке информации, то назовём её *кодовой матрицей* для данного набора спектральных характеристик.

Теорема 2 [3]. Множество невырожденных булевых матриц порядка n изоморфно множеству W-матриц уровня n.

Указана следующая процедура вычисления W-матрицы по кодовой. Зададим матрицы C_n размера $n \times 2^n$ рекуррентным соотношением

$$C_1 = (0\,1), \quad C_n = \begin{pmatrix} C_{n-1} & C_{n-1} \\ 0_{n-1} & 1_{n-1} \end{pmatrix}, \tag{1}$$

где блоки $0_{n-1} = (0\,0\ldots0)$, $1_{n-1} = (1\,1\ldots1)$ суть строки длины 2^{n-1}. В столбцах матрицы C_n вида (1) лексикографически упорядочены инверсии двоичных кодов чисел от 0 до $2^n - 1$. По формуле (над полем $\mathbb{F}_2$)

$$C_n^{\mathrm{T}} \cdot K \cdot C_n \tag{2}$$

вычислим булеву матрицу порядка $N = 2^n$, в которой произведём перекодировку элементов: $1 \Rightarrow -1$, $0 \Rightarrow 1$.

Обратная процедура выделения кодовой матрицы из W-матрицы: выборкой $(2^0, 2^1, \ldots, 2^{n-1})$ выделим главную подматрицу, в которой произведём обратную перекодировку элементов: $1 \Rightarrow 0$, $-1 \Rightarrow 1$.

Для сокращения записи кодовую матрицу заменяем на *кодовую метку* с записью строк в шестнадцатиричной системе счисления. Все шесть W-матриц уровня 2 явно записаны в [5, 6]. Четыре из них симметричные и соответствуют нумерациям Адамара, Пэли, Уолша и предложенной в [7]. Их кодовые метки 21, 12, 13 и 31 соответственно. Для уровня три их кодовые метки 421, 124, 136 и 652, а для уровня четыре — 8421, 1248, 136C и CA52 соответственно. Общее число W-матриц уровня n, совпадающее с порядком группы $\mathrm{GL}(n, 2)$, вычисляется по формуле $(2^n - 2^0)(2^n - 2^1)\ldots(2^n - 2^{n-1})$.

Известно, что j-я строка произведения матриц равна линейной комбинации строк второго сомножителя с коэффициентами из j-й строки первого сомножителя. По этому правилу реализация левого умножения в (2) организует упорядочение всех элементов векторного пространства $\mathbb{Z}_2^n$ относительно упорядоченного базиса, указанного в строках матрицы K. Правое умножение в (2) организует упорядочение базиса векторного подпространства $G \subset \mathbb{Z}_2^N$. В терминах блочного кодирования [8] произведение

$K \cdot C$ составляет порождающую матрицу для блочного линейного $(2^n, n)$-кода, который (в результате перекодировки $1 \Rightarrow -1$, $0 \Rightarrow 1$) превращается в упорядоченный ортогональный базис пространства $\mathbb{R}^N$ из дискретных функций Уолша уровня n.

Если умножения в формуле (2) рассматривать справа налево, а не стандартно слева направо, то получим аналогичные взаимосвязи для столбцов, а не строк. Известно, что j-й столбец произведения матриц равен линейной комбинации столбцов первого сомножителя с коэффициентами из j-го столбца второго сомножителя. Тогда правое умножение в (2) организует упорядочение всех элементов векторного пространства $\mathbb{Z}_2^n$ в порядке, заданном в столбцах K. Левое умножение в (2) организут упорядочение базиса векторного подпространства $G \subset \mathbb{Z}_2^N$ так, что произведение $C^{\mathrm{T}} \cdot K$ составляет транспонированную порождающую матрицу $(2^n, n)$-кода, переходящую в упорядоченный ортогональный базис пространства $\mathbb{R}^N$.

Авторами создан программный прототип (C#), который моделирует процессы кодирования и декодирования числовых данных с использованием кодовой матрицы. Тип исходных числовых данных, в поле которого будут происходить все программные расчёты, выбирает пользователь, что даёт возможность выделять минимальное необходимое количество байт памяти. В программе предусмотрено задание кодовой метки вручную и случайно. Перед кодированием происходит формирование кодовой матрицы из кодовой метки, её визуализация и проверка на невырожденность. Если матрица невырожденная, то над исходным числовым массивом совершается *быстрое преобразование Уолша* и перестановка элементов выходного массива в порядке, указанном формулой (2) в кодовой матрице. Для декодирования сообщения сначала происходит обратная перестановка элементов, затем *обратное быстрое преобразование Уолша.*

Например, для некоторого сообщения в виде даты выходной сигнал можно выдать в нумерации Пэли $y = (24, 7, 2, 1, 3, 3, 9, 18)$ для кодовой метки 124 или в переставленном виде $y = (24, 3, 9, 2, 1, 18, 3, 7)$ для кодовой метки 463. Предложим разные варианты кодирования. Так как сумма цифр даты меньше 64, для начального отсчёта отведём шесть бит. Так как для представления начального отсчета (числа 24) достаточно пяти, то на каждый из остальных отсчётов алгоритм отводит по пять бит. Получим в первом случае на выходе

$$011000001110001000001000110001101001100 10.$$

Для выходного сигнала с кодовой меткой 463 каждый отсчёт представим в фибоначчиевой системе счисления и получим

$$1000100011000110001011001101101000011000 1101001.$$

На базе дискретных функций Уолша традиционно обрабатывается видео- и аудиоинформация. С помощью системы кодовых меток можно организовать многоканальную систему перенастраивающихся декодеров при передаче скрытой информации по открытым каналам связи.

Характерной особенностью выходного слова служит его представление в алфавите из двух символов (а не трёх) за счёт отсутствия разделительных знаков между отсчётами, которые в данных примерах после простых манипуляций расставляются. Эта особенность важна для массивов с неизвестной заранее разрядностью отсчётов исходного сообщения.

Описанная конструкция допускает p-ичное обобщение, теория которого в виде аналогов приведённых определений, теорем и выносных формул разработана в [9].

ЛИТЕРАТУРА

1. *Малоземов В. Н., Машарский С. М.* Основы дискретного гармонического анализа. СПб.: Лань, 2012.
2. *Залманзон Л. А.* Преобразование Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. М.: Наука, 1989.
3. *Беспалов М. С.* Собственные подпространства дискретного преобразования Уолша // Проблемы передачи информации. 2010. Т. 46. № 3. С. 60–79.
4. *Моррис С.* Двойственность Понтрягина и строение локально компактных абелевых групп. М.: Мир, 1980.
5. *Трахман А. М., Трахман В. А.* Основы теории дискретных сигналов на конечных интервалах. М.: Сов. радио, 1975.
6. *Беспалов М. С., Скляренко В. А.* Дискретные функции Уолша и их приложения. Владимир: ВлГУ. 2014.
7. *Беспалов М. С.* Новая нумерация матриц Уолша // Проблемы передачи информации. 2009. Т. 45. № 4. С. 43–53.
8. *Питерсон У., Уэлдон Э.* Коды, исправляющие ошибки. М.: Мир, 1976.
9. *Беспалов М. С.* Дискретное преобразование Крестенсона // Проблемы передачи информации. 2010. Т. 46. № 4. С. 91–115.

УДК 519.7 DOI 10.17223/2226308X/13/37

ПРИМЕНЕНИЕ ИНВЕРСНЫХ ЛАЗЕЕК ДЛЯ ПОСТРОЕНИЯ АТАК ИЗ КЛАССА «УГАДЫВАЙ И ОПРЕДЕЛЯЙ» НА ХЕШ-ФУНКЦИИ СЕМЕЙСТВА MD4[1]

И. А. Грибанова, А. А. Семёнов

Приведены новые атаки из класса «угадывай и определяй» для хеш-функций вида MD4-k, $k > 39$. Описываемые атаки основаны на концепции инверсной лазейки. Для решения задач криптоанализа, ослабленных подстановками угадываемых бит, используются SAT-решатели. Задача поиска инверсной лазейки, обеспечивающей атаку с относительно малой трудоёмкостью, ставится в форме задачи минимизации специальной псевдобулевой функции. Для её решения используются три метаэвристических алгоритма: алгоритм поиска с запретами, (1+1)-FEA_β и специальный вариант генетического алгоритма. Перечисленные алгоритмы дают атаки на рассматриваемые функции с близкими оценками трудоемкости. Для функции сжатия полнораундового MD4 лучшие атаки строит генетический алгоритм.

Ключевые слова: *задача поиска прообразов криптографической хеш-функции, атаки из класса «угадывай и определяй», инверсные лазейки, SAT.*

1. О понятии инверсной лазейки

Понятие инверсной лазейки (Inverse Backdoor Set, IBS) введено в [1]. Кратко напомним его суть. Рассматривается задача обращения (поиска прообразов) произвольной функции вида

$$f : \{0,1\}^n \to \{0,1\}^m, \tag{1}$$

заданной программой (алгоритмом) M_f. Более точно, требуется по произвольному $\gamma \in$ $\in \operatorname{Range} f$ найти такой $\alpha \in \{0,1\}^n$, что $f(\alpha) = \gamma$. Подход к решению данной задачи,

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046. Грибанова И. А. поддержана стипендией Президента РФ СП-3545.2019.5.