

**ИССЛЕДОВАНИЕ MDS ПРЕОБРАЗОВАНИЙ,
ЗАДАВАЕМЫХ УМНОЖЕНИЕМ НА ФИКСИРОВАННЫЙ
ЭЛЕМЕНТ В ПОЛЯХ ГАЛУА**

Осенникова Клавдия Владимировна

Студентка

Факультет ВМК МГУ имени М. В. Ломоносова, Москва, Россия

E-mail: osennikovaklava@gmail.com

Такой класс матриц, как MDS матрицы, широко используется для построения криптографических схем и протоколов. Так, в блочных шифрах, основанных на модели SP-сети, каждый раунд может состоять из нелинейного и линейного преобразований. Для того, чтобы шифр был стойким к атакам, раундовые преобразования должны обеспечивать лавинный эффект - свойство схемы, при котором изменение одного бита на входе (в открытом тексте) приводит к значительному изменению битов на выходе (битов шифротекста). Лавинный эффект осуществляется за счёт перемешивания (confusion) и рассеивания (diffusion), термины впервые были введены Клодом Шенноном в статье “Теория связи в секретных системах” в 1949 году. Перемешивание обеспечивает как можно более сложную зависимость ключа и шифрованных данных и используется для того, чтобы усложнить задачу получения информации о ключе. Рассеивание - свойство алгоритма, при котором влияние одного бита открытого текста распространяется на большое количество битов шифротекста, скрывая статистические характеристики текста. MDS матрицы, умножение на которые используется в качестве линейного преобразования в блочных шифрах, обеспечивают свойство рассеивания для противодействия соответствующим атакам. В связи с этим рассматривается такое понятие, как коэффициент ветвления (branch number), определяемый как $\theta_M = \min_{v \neq 0} \{wt(v) + wt(vM)\}$, где M - матрица размером $k \times k$, подсчёт ведётся по всем возможным векторам соответствующей размерности, элементы вектора и матрицы являются элементами некоторого конечного поля, $wt(v)$ - вес вектора (количество ненулевых компонент). Если коэффициент ветвления равен $k + 1$, то такая матрица является MDS матрицей. В работе были рассмотрены MDS преобразования, являющиеся элементами поля Галуа $GF(2^n)$. Умножение на элементы поля рассматривалось как умножение в поле $(GF(2^s))^k$. Были найдены MDS преобразования для полей размерности $n = 4, 6, 8, 9, 10, 12, 14, 16$, а также спектры количества коэффициентов ветвления вида $[N_2, \dots, N_{k+1}]$, где

$N_i = \#\{M | \theta_M = i\}$ – количество таких M для фиксированного поля. Кроме того, были рассмотрены так называемые нормальные базисы векторного пространства $\{\alpha, \alpha^q, \alpha^{q^2}, \dots, \alpha^{q^{n-1}}\}$ для α равного корню неприводимого многочлена, а также при произвольном значении α . Элементы поля $a \in GF(2^n)$ могут быть представлены в таком базисе точно так же, как и в стандартном степенном базисе, – в виде многочленов с коэффициентами из поля $GF(q)$. Найдены такие α , при которых преобразование сохраняет свои MDS-свойства после перехода между базисами. Также в нормальном базисе был реализован алгоритм быстрого умножения на основе предложенного в [2] при использовании суперкомпьютера “Ломоносов” [3]. Работа выполнена с использованием оборудования Центра коллективного пользования сверхвысокопроизводительными вычислительными ресурсами МГУ имени М.В. Ломоносова. В работе доказан ряд утверждений о существовании MDS-преобразований определённого типа в полях вида $GF(2^{2s})$

Литература

1. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
2. Болотов А. А., Гашков С. Б., Хохлов Р. А., Быстрые вычисления в конечных полях с использованием стандартных оптимальных базисов // Интеллектуальные системы. Теория и приложения (ранее: Интеллектуальные системы по 2014, 2, ISSN 2075-9460). 2002. Т. 7. С. 245-292
3. Воеводин Вл. В., Жуматий С. А., Соболев С. И., Антонов А. С., Брызгалов П. А., Никитенко Д. А., Стефанов К. С., Воеводин Вад. В. Практика суперкомпьютера "Ломоносов"// Открытые системы. - Москва: Издательский дом "Открытые системы" N 7, 2012. С. 36-39.