ИССЛЕДОВАНИЕ В НИЯУ МИФИ ПРИМИТИВНОСТИ НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

Когос Константин Григорьевич
НИЯУ МИФИ, Москва, аспирант
k.kogos@mail.ru

Кяжин Сергей Николаевич
НИЯУ МИФИ, Москва, студент
s.kyazhin@kaf42.ru

Фомичев Владимир Михайлович
Финансовый университет при Правительстве РФ, Москва, профессор
fomichev@nm.ru

Введение

В системах шифрования и идентификации к криптографическим функциям векторных пространств предъявляется требование совершенности, то есть зависимости каждой координатной функции от всех переменных [1]. Обобщениями свойства совершенности являются строгий лавинный критерий, критерии распространения, свойство «бент». Изучение совершенности криптографических функций — актуальная задача, так как в криптосистемах функции выбираются не случайно, а из отображений с рядом заданных свойств.

Из соображений простоты реализации совершенная функция строится в виде композиции нескольких функций с относительно слабыми перемешивающими свойствами, при этом важно, чтобы совершенная композиции содержала небольшое число перемножаемых функций. Например, так строятся подстановки итеративных блочных шифров, где важной характеристикой простоты реализации является число раундов шифрования.

1. Примитивность графов и неотрицательных матриц

Для оценки свойства совершенности используется математический аппарат матриц и графов.

Матрицу M над полем действительных чисел называют положительной (неотрицательной), если положительны (неотрицательны) все её элементы, обозначают: $M>0$ ($M\geq 0$). Квадратную 0,1-матрицу M называют примитивной, если $M^t>0$ при некотором натуральном t. Наименьшее натуральное γ, при котором $M^\gamma>0$, называется экспонентом (показателем примитивности) матрицы M, обозначается exp$M$.

Равносильным образом рассматривают n-вершинный орграф Г, матрица смежности вершин которого равна M. Орграф Г и матрица M одновременно примитивны или не примитивны, в случае примитивности их экспоненты равны. Связь между графами и неотрицательными матрицами основана на теореме [2]: пусть $M^t=(m_{ij}^{(t)})$, тогда число путей длины t из i в j в графе Г равно $m_{ij}^{(t)}$, $i,j\in\{1,\ldots,n\}$.

Известен универсальный критерий примитивности орграфа Г [3, с.226]. Если $C_1,\ldots,C_k$ есть все простые контуры орграфа Г длин $l_1,\ldots,l_k$ соответственно, то сильно связный орграф Г примитивен $\Leftrightarrow \gcd(l_1,\ldots,l_k)=1$. При использовании критерия могут быть полезны таблицы примитивных наборов натуральных чисел, свойства которых описаны в [4].

Абсолютная оценка экспонента примитивной матрицы M порядка n (орграфа Г) дана Виландтом [5]: $\exp M\leq n^2-2n+2$.

При $n>2$ описаны примитивные орграфы [6], на которых (и только на них) достигается абсолютная оценка Виландта. Они представляют собойгамильтонов контур, к которому добавлена дуга (i,j), где вершины i,j расположены на контуре на расстоянии 2, $i,j\in\{1,\ldots,n\}$. Множество этих изоморфных орграфов, названных графами Виландта, состоит из $n!$ изоморфных графов. Для орграфов Г, отличных от графов Виландта, при нечетном $n>3$ верна достижимая оценка: $\exp\Gamma\leq n^2-3n+4$.

Оценки экспонентов для других классов матриц и графов даны в обзорной статье [7].

2. Исследования в НИЯУ МИФИ

Исследования примитивности графов и неотрицательных матриц активно проводятся, в основном начиная с 2011 года, под руководством профессора Фомичева В.М. студентами 4-го и 5-го курсов (Когос К.Г., Коренева А.М., Кяжин С.Н.). Результаты исследований докладывались на конференциях, в том числе, на международных (научная сессия в НИЯУ МИФИ, EUROCRYPT'12, SIBECRYPT в 2011-12 гг.), составили основу нескольких УИРов, 3 дипломных проектов и

более 10 публикаций в материалах конференций и в ведущих математических журналах России.

Исследования проводятся по следующим направлениям:

- систематизация результатов, подготовка обобщающих обзоров [7];
- уточнение диаметров и экспонентов частных классов графов [6,9];
- исследование алгебраических и теоретико-числовых свойств множеств, связанных со свойством примитивности графов и матриц, построение алгоритмов распознавания указанных свойств, оценка вычислительной сложности алгоритмов [4,8];
- разработка приложений к решению криптографических задач [9].

Развиваются некоторые перспективные направления исследований:

- примитивность в частичной полугруппе разноразмерных матриц;
- локальная примитивность графов и матриц.

3. О приложениях теории примитивности графов и матриц

Приложения возможны к широкому классу коммуникаций, построенных с помощью бинарного отношения на множестве объектов.

Пример 1. Транспортная система коммуникаций. Вершинами орграфа являются n городов, ребра графа соответствуют непосредственным путям между городами. Пусть из i-го города стартует автоколонна машин i-го цвета, $i=1,\ldots,n$, (в колонне достаточно много машин), разделяясь на части по путям, выходящим из каждого города, и путь по любому одному ребру машины преодолевают за 1 день. С помощью свойств примитивности можно оценить количество дней, после которых во всех городах одновременно окажутся машины всех цветов.

Пример 2. Коммуникации преступного мира. Расследуется дело группы n преступников, в целом разобщенной, но между некоторыми членами группы (соседями) имеются связи (дуги графа). В начале i-й преступник располагает i-м аргументом для создания ложного, но правдоподобного алиби, $i=1,\ldots,n$. В первый час он передает всем соседям этот аргумент и ежечасно каждый преступник передает соседям весь набор аргументов, который он получил в предыдущий час. Набор менее чем из n аргументов считается ненадежным и преступником не запоминается. Считается, что дело станет нераскрываемым, когда одновременно все преступники получат все n аргументов. Оценив экспонент графа, можно оценить время, которое имеется у правоохранительных органов на раскрытие преступления.

Список источников

1. Фомичев В.М. Методы дискретной математики в криптологии. // В. М. Фомичев. — М.: Диалог-МИФИ, 2010 — 424 с.

2. Берж К. Теория графов и её применение. М.: ИЛ, 1962г. — 320с.

3. Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц. — М.: ТВП, 2000. — 448 с.

4. Кяжин С.Н., Фомичев В.М. О примитивных наборах натуральных чисел // Прикладная дискретная математика, №2(16), 2012.

5. Wielandt H. Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. No. 52. P. 642-648.

6. Фомичев В.М. Оценки экспонентов примитивных графов // Прикладная дискретная математика, №2(12), 2011.

7. Когос К.Г., Фомичев В.М. Положительные свойства неотрицательных матриц // Прикладная дискретная математика, №4(18), 2012.

8. Кяжин С.Н., Фомичев В.М. Алгоритмы анализа примитивности ориентированных графов // Безопасность информационных технологий, №1, 2012.

9. Коренева А.М., Фомичев В.М. Об одном обобщении блочных шифров Фейстеля // Прикладная дискретная математика, №3(17), 2012.