Код безопасности
ГК «Информзащита»

Развитие матрично-графового подхода к оценке перемешивающих свойств композиций криптографических функций

д.ф.-м.н., проф. Фомичёв В.М.

РусКрипто 2015

Актуальность

Итеративные функции векторных пространств, где каждый бит выхода зависит от всех битов входа, используются:

- в системах аутентификации для выработки кодов аутентификации;

- в симметричных криптосистемах для противодействия криптоаналитическим атакам типа последовательного опробования частей ключа.

Матрично-графовый подход

Для преобразования $g=\{g_1(x_1,\ldots,x_n),\ldots,g_n(x_1,\ldots,x_n)\}$ n-мерного векторного пространства требуется определить свойства g^t, степени преобразования.

Точные методы определения существенных переменных функций трудоемки, так как требуют просмотра таблиц функций. Поэтому для g^t применяется оценочный матрично-графовый подход.

Функции g соответствует **перемешивающий** n-вершинный **орграф** $\Gamma(g)$ (**перемешивающая 0,1-матрица** $M(g)=(m_{ij})$ смежности его вершин), где g_j существенно зависит от $x_i \Leftrightarrow (i,j)$ дуга в $\Gamma(g)$ ($m_{ij}=1$), $i,j\in\{1,\ldots,n\}$.

Задача: определить **экспонент** графа $\Gamma(g)$ (матрицы $M(g)$) – наименьшее натуральное число t: граф $\Gamma^t(g)$ полный ($M^t(g)>0$).

Матрица $M^t=(m_{ij}^{(t)})$ описывается числом путей длины t из i в j в графе Γ.

Примитивность графов

Граф Г (матрица M) **примитивный,** если существует t: граф $\Gamma^t(g)$ полный ($M^t(g)>0$).

Для примитивности Г необходима его сильная связность.

[*Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц*]:

Универсальный критерий примитивности: если $C_1,\ldots,C_k$ суть все простые контуры длин $l_1,\ldots,l_k$ соответственно сильно связного орграфа Г, то Г примитивный $\Leftrightarrow \gcd(l_1,\ldots,l_k)=1$.

Код Безопасности
ГК «Информзащита»

Экспоненты n-вершинных графов (1)

[*Wielandt H. Unzerlegbare nicht negative Matrizen*]:

Абсолютная достижимая оценка:

$$\exp\Gamma \le n^2-2n+2,\ n>2.$$

[*Фомичев В. М. Оценки экспонентов примитивных графов*]:

Описаны орграфы, где достигается абсолютная оценка. Для остальных примитивных орграфов $\exp\Gamma \le n^2-3n+4$ при нечетном $n>3$.

[*Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц*]:

Если l – длина кратчайшего простого контура в Г:

$$\exp\Gamma \le n+l(n-2).$$

В частности, для орграфа Г с петлей

$$\exp\Gamma \le 2n-2. \qquad (1)$$

[*Фомичев В. М. Свойства путей в графах и мультиграфах*]

Оценка (1) уточнена. Пусть в вершине r имеется петля. Обозначим $d_{i,r,j}$ длину кратчайшего пути из i в j, проходящего через r, $d_r=\max\{d_{i,r,j},\ i,j=1,\dots,n\}$. Тогда $\exp\Gamma \le d_r$.

Экспоненты n-вершинных графов (2)

Частные классы: [*Фомичев В. М. Оценки экспонентов примитивных графов*]:

Граница понижается при известных длинах l и λ двух простых контуров C и C', где $(l,\lambda)=1$. Пусть h – число общих вершин контуров C и C', $n>2$, тогда

если $h=0$, то $\exp\Gamma \le l\lambda-2l-3\lambda+3n$;

если $h>0$, то $\exp\Gamma \le l\lambda-l-3\lambda+h+2n$.

[*Фомичев В.М. Оценка экспонента некоторых графов с помощью чисел Фробениуса для трех аргументов*]:

Оценки понижены для орграфов с известными длинами l, λ и μ трех простых контуров, где $(l,\lambda,\mu)=1$. Оценки выражены в ряде случаев через числа Фробениуса от 3-х аргументов.

[*Сачков В.Н., Тараканов В.Е. Комбинаторика неотрицательных матриц*]:

При $n\ge4$ дан критерий примитивности турнира (графа T без петель, где каждая пара вершин соединена ровно одной дугой) и при $n\ge5$ (d – диаметр):

$$d\le\exp T_n\le d+3.$$

Экспоненты *n*-вершинных графов (3)

[*Князев А. В. Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов*]:

Для примитивного графа с одинаковыми полустепенями захода и исхода вершин получены оценки экспонентов, в том числе, с ограничением на обхват графа.

[*Дорохова А. М., Фомичев В. М. Уточненные оценки экспонентов перемешивающих графов биективных регистров сдвига над множеством двоичных векторов*]:

Для обобщения блочных шифров Фейстеля (регистр длины n над V_r) получены условия примитивности и оценки экспонента перемешивающего графа $\Gamma(\varphi)$ с nr вершинами. Оценка для частного класса существенно меньше nr.

Код Безопасности
ГК «Информзащита»

Локальная примитивность матрицы

Для поточных систем условие примитивности графа (матрицы) можно ослабить до **локальной примитивности**.

[*Кяжин С.Н., Фомичев В.М. Локальная примитивность графов и неотрицательных матриц*]:

Пусть A – квадратная 0,1-матрица порядка n, $\varnothing \neq J \subseteq \{1,\ldots,n\}$, $A(J^2)$ ($A(J)$) – подматрица размера $r \times r$ ($n \times r$), полученная из A вычеркиванием строк и столбцов с номерами $j \notin J$ (столбцов с номерами $j \notin J$).

Матрица A называется ***J^2-примитивной*** (***J-примитивной***), если $A^t(J^2)>0$ ($A^t(J)>0$) при любом $t \geq \gamma$; наименьшее γ называется **J^2-экспонентом (J-экспонентом)** матрицы.

Даны критерии J^2- и J-примитивности, оценки локальных экспонентов.

1. Граф Г J^2-примитивный $\Leftrightarrow$ в Г имеется компонента сильной связности, содержащая J (ксс(J)).

2. Связный граф Г J-примитивный, если в Г имеется ксс(J), достижимая из любой вершины графа Г.

Системы матриц (1)

Система $\Omega=\{M_1,\ldots,M_p\}$ квадратных 0,1-матриц ($\Omega=\{\Gamma_1,\ldots,\Gamma_p\}$ орграфов) **примитивная**, если мультипликативная полугруппа $\langle\Omega\rangle$ содержит положительную матрицу (полный граф).

Экспонент примитивной системы Ω – наименьшая длина l слова в алфавите Ω, представляющего положительную матрицу (определение распространено и на системы разноразмерных матриц).

Множественным экспонентом системы Ω (setexp) называется наименьшее l: положительны все слова длины l в алфавите Ω.

[*Князев А. В.*]: Для любой множ. примит. системы Ω:

$$\text{setexp}\Omega\le 2^n-2.$$

[*Сачков В.Н.*]: Уточнены оценки $\text{setexp}\Omega$ в частных случаях.

Системы матриц (2)

[*Авезова Я.Э., Фомичев В.М. Комбинаторные свойства систем разноразмерных 0,1-матриц*]:

Если матрица $M=M_1+\ldots+M_p$ примитивная, то $\exp\Omega \geq \exp M$. Эта оценка верна и для СРМ, где M – сумма матриц $M_1,\ldots,M_p$, приведенных к единому размеру приписыванием нулей.

Для Ω введены понятия субпримитивности и субэкспонента, равного наименьшей длине t слова $M_{i_1} \ldots M_{i_t}$ в алфавите Ω, для которого положительна матрица $M_{i_1}+M_{i_1}M_{i_2}+\ldots+M_{i_1}\cdot\ldots\cdot M_{i_t}$.

[*Фомичев В. М. Свойства путей в графах и мультиграфах*]:

Если $\Omega=\{\Gamma_1,\ldots,\Gamma_p\}$ и граф $\Gamma_1\cup\ldots\cup\Gamma_p$ сильно связный, то при $n\geq 4$ система Ω субпримитивна и субэкспонент не больше $(n^2-2)(n-1)/2$.

Минимальные примитивные графы

Граф называется **минимальным примитивным**, если он становится непримитивным при удалении любой дуги.

Минимальность важна с точки зрения экономной реализации.

[*Фомичев В.М. Свойства минимальных примитивных орграфов*]*:*

При $n \geq 4$ все примитивные орграфы с числом дуг $n+1$ являются минимальными и имеются минимальные примитивные орграфы с числом дуг от $n+2$ до $2n-3$.

Дано описание всех минимальных примитивных орграфов с числом дуг $n+1$ и $n+2$.

Зарубежные статьи

по исследованию других обобщений экспонента:

- Y. Huang, B. Liu. Generalized *r*-exponents of primitive digraphs // Taiwanese Journal of Mathematics, 2011. – Vol. 15, No. 5. – pp. 1999–2012.
- Z. Miao, K. Zhang. The local exponent sets of primitive digraphs // Linear Algebra and its Applications, 2000. – No. 307. – pp. 15–33.
- R. A. Brualdi, B. Liu. Generalized exponents of primitive directed graphs // Journal of Graph Theory, 1990. – No. 14. – pp. 483–499.
- B. Liu. Generalized exponents of Boolean matrices // Linear Algebra and its Applications, 2003. – No. 373. – pp. 169–182.
- J. Shen, S. Neufeld. Local exponents of primitive digraphs // Linear Algebra and its Applications, 1998. – No. 268. – pp. 117–129.
- J. Shao, J. Wang, G. Li. Generalized primitive exponents with the complete characterization of the extremal digraphs // Chinese Journal of Contemporary Mathematics, 1994. – No. 15(4). – pp. 317–324.

.

Спасибо за внимание!