Секция 3

МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

УДК 519.1 DOI 10.17223/2226308X/10/25

О ПРИМИТИВНОСТИ НЕКОТОРЫХ МНОЖЕСТВ ПЕРЕМЕШИВАЮЩИХ ОРГРАФОВ РЕГИСТРОВЫХ ПРЕОБРАЗОВАНИЙ

Я. Э. Авезова

Получены условия примитивности и оценки экспонентов для нескольких множеств орграфов $\hat{\Gamma} = \{\Gamma_0, \dots, \Gamma_{n-1}\}$ с вершинами $0, \dots, n-1$.
Критерий: если Γ_i имеет гамильтонов контур $(0, \dots, n-1)$ и дугу $(i, (i+l) \bmod n)$, $n \geqslant l > 1$, $i = 0, \dots, n-1$, то множество $\hat{\Gamma}$ примитивное, если и только если НОД$(n, l-1) = 1$, при этом $n - 1 \leqslant \exp \hat{\Gamma} \leqslant 2n - 2$; если Γ_i имеет также дугу $(i, (i+\lambda) \bmod n)$, $n \geqslant \lambda > l > 1$, $i = 0, \dots, n-1$, то множество $\hat{\Gamma}$ примитивное, если и только если НОД$(n, l-1, \lambda-1) = 1$, $\exp \hat{\Gamma} \geqslant (\sqrt{8n+1} - 3)/2$. При этом если НОД$(n, l-1) = 1$, то $\exp \hat{\Gamma} \leqslant n - 1 + \max\{b, n-b+1\}$, где $b = (\lambda - 1)(l-1)^{\varphi(n)-1} \bmod n$ и $\varphi(n)$ — функция Эйлера.
Пусть n чётное, орграф Γ_i при чётных i имеет контур $(0, \dots, n-1)$ и дугу $(i, (i+l) \bmod n)$ и при нечётных i имеет контур $(n-1, \dots, 0)$ и дугу $(i, (i+\lambda) \bmod n)$. Тогда если НОД$(n, l-1) = 1$ или НОД$(n, \lambda+1) = 1$, то множество $\hat{\Gamma}$ примитивное и $\exp \hat{\Gamma} \leqslant 2n - 2$.

Ключевые слова: *примитивность множества графов, экспонент орграфа, экспонент множества орграфов.*

Введение

Основные обозначения: $\mathbb{N}_p = \{1, \dots, p\}$, $p \in \mathbb{N}$; НОД$(a_1, \dots, a_n)$ — наибольший общий делитель натуральных чисел $a_1, \dots, a_n$; (i, j) — дуга в орграфе Γ, инцидентная вершинам i и j; $\langle X \rangle$ — подполугруппа, порождённая подмножеством X мультипликативной полугруппы.

Свойство примитивности перемешивающего графа криптографического преобразования, необходимое для перемешивания данных, важно для приложений в области анализа и синтеза итеративных блочных шифров и генераторов гаммы. Критерий примитивности и универсальные оценки экспонента орграфа известны [1, гл. 11]. Понятия примитивности и экспонента орграфа естественным образом распространены на множества орграфов [2, § 10.2].

Пусть $\hat{\Gamma} = \{\Gamma_1, \dots, \Gamma_p\}$ — множество орграфов. Слову $w = w_1 \dots w_s$ в алфавите $\mathbb{N}_p$ соответствует произведение орграфов $\Gamma(w) = \Gamma_{w_1} \cdot \ldots \cdot \Gamma_{w_s}$. Слово $\Gamma_{w_1} \dots \Gamma_{w_s}$ в алфавите $\hat{\Gamma}$ называется положительным (примитивным), если орграф $\Gamma(w)$ полный (примитивный). Множество $\hat{\Gamma}$ называется примитивным, если полугруппа $\langle \hat{\Gamma} \rangle$ содержит полный орграф, наименьшая длина положительного слова называется экспонентом множества $\hat{\Gamma}$, обозначается $\exp \hat{\Gamma}$.

Критерий примитивности множества орграфов получен автором [3], универсальная оценка экспонента примитивного множества неизвестна. Проблема распознавания

примитивности множества орграфов алгоритмически разрешима, но в общем задача трудоёмкая из-за необходимости проверять примитивность большого количества слов полугруппы $\langle\hat{\Gamma}\rangle$. В частных случаях (например, когда орграфы $\Gamma_1,\dots,\Gamma_p$ имеют общие части) получены и условия примитивности, и оценки экспонентов.

Работа посвящена исследованию примитивности множеств перемешивающих орграфов регистровых преобразований, особенностью орграфов является наличие общего гамильтонова контура. Выбор объекта исследования обоснован широким применением регистров сдвига в современных криптосистемах.

1. Множество перемешивающих орграфов регистров правого сдвига

Получены условия примитивности множества орграфов $\hat{\Gamma}=\{\Gamma_0,\dots,\Gamma_{n-1}\}$ с вершинами $0,\dots,n-1$ и оценка экспонента множества $\hat{\Gamma}$. Случай множества перемешивающих орграфов регистров левого сдвига рассматривается симметрично.

Теорема 1. Пусть орграф Γ_i из множества $\hat{\Gamma}$ имеет гамильтонов контур $(0,\dots,n-1)$ и дугу $(i,(i+l)\bmod n)$, $n\geqslant l>1$, $i=0,\dots,n-1$. Тогда множество $\hat{\Gamma}$ примитивное, если и только если $\text{НОД}(n,l-1)=1$, при этом $n-1\leqslant\exp\hat{\Gamma}\leqslant 2n-2$.

Пусть $d=\text{НОД}(n,l)$ и $\hat{\Gamma}(d)=\{\Gamma_i\in\hat{\Gamma}:i\equiv 0\bmod d\}$, тогда множество $\hat{\Gamma}(d)$ примитивное, если $\text{НОД}(n,l-1)=1$, и $\exp\hat{\Gamma}(d)\leqslant 2n-2$.

Заметим, что множество $\hat{\Gamma}$ теоремы 1 содержит орграфы Виландта.

Теорема 2. Пусть орграф Γ_i из множества $\hat{\Gamma}$ имеет гамильтонов контур $(0,\dots,n-1)$ и дуги $(i,(i+l)\bmod n)$ и $(i,(i+\lambda)\bmod n)$, $n\geqslant\lambda>l>1$, $i=0,\dots,n-1$. Тогда:

а) множество $\hat{\Gamma}$ примитивное, если и только если $\text{НОД}(n,l-1,\lambda-1)=1$, при этом $\exp\hat{\Gamma}\geqslant(\sqrt{8n+1}-3)/2$;

б) если $\text{НОД}(n,l-1)=1$, то

$$\exp\hat{\Gamma}\leqslant n-1+\max\{b,n-b+1\},\ \text{где } b=(\lambda-1)(l-1)^{\varphi(n)-1}\bmod n.$$

В табл. 1 и 2 даны оценки экспонентов множеств графов в условиях теорем 1 и 2 соответственно при некоторых значениях n, l и λ.

Таблица 1

Оценки экспонентов множеств графов (теорема 1)

n	l	Полный орграф	$\exp\Gamma_i$, $i=0,\dots,n-1$	$\exp\hat{\Gamma}$
5	2	$\Gamma_2\Gamma_4\Gamma_1\Gamma_3\Gamma_0\Gamma_2\Gamma_4\Gamma_1$	17	$4\leqslant\exp\hat{\Gamma}\leqslant 8$
6	2	$\Gamma_2\Gamma_4\Gamma_0\Gamma_2\Gamma_4\Gamma_0\Gamma_2\Gamma_4\Gamma_0\Gamma_2$	26	$5\leqslant\exp\hat{\Gamma}\leqslant 10$
7	2	$\Gamma_2\Gamma_4\Gamma_6\Gamma_1\Gamma_3\Gamma_5\Gamma_0\Gamma_2\Gamma_4\Gamma_6\Gamma_1\Gamma_3$	37	$6\leqslant\exp\hat{\Gamma}\leqslant 12$
8	4	$(\Gamma_4\Gamma_0)^7$	38	$7\leqslant\exp\hat{\Gamma}\leqslant 14$

Таблица 2

Оценки экспонентов множеств графов (теорема 2, б)

n	l	λ	b	$r=\max\{b,n-b+1\}$	Полный орграф	$\exp\Gamma_i$, $i=0,\dots,n-1$	$\exp\hat{\Gamma}$
5	2	4	3	$r=\max\{3,3\}=3$	$\Gamma_2\Gamma_4\Gamma_1\Gamma_3\Gamma_0\Gamma_2\Gamma_4$	9	$\exp\hat{\Gamma}\leqslant 7$
6	2	4	3	$r=\max\{3,4\}=4$	$\Gamma_2\Gamma_4\Gamma_0\Gamma_2\Gamma_4\Gamma_0\Gamma_2\Gamma_4\Gamma_0$	14	$\exp\hat{\Gamma}\leqslant 9$
7	2	5	4	$r=\max\{4,4\}=4$	$\Gamma_2\Gamma_4\Gamma_6\Gamma_1\Gamma_3\Gamma_5\Gamma_0\Gamma_2\Gamma_4\Gamma_6$	19	$\exp\hat{\Gamma}\leqslant 10$
8	4	5	4	$r=\max\{4,5\}=5$	$\Gamma_4\Gamma_0\Gamma_4\Gamma_0\Gamma_4\Gamma_0\Gamma_4\Gamma_0\Gamma_4\Gamma_0\Gamma_4\Gamma_0$	22	$\exp\hat{\Gamma}\leqslant 12$

2. Множество орграфов регистров с разнонаправленными сдвигами

Теорема 3. Пусть n чётное, орграф Γ_i при чётных i имеет контур $(0,\dots,n-1)$ и дугу $(i,(i{+}l) \bmod n)$, при нечётных i — контур $(n{-}1,\dots,0)$ и дугу $(i,(i{+}\lambda) \bmod n)$. Если НОД$(n,l{-}1){=}1$ или НОД$(n,\lambda{+}1){=}1$, то множество $\hat{\Gamma}$ примитивное и $\exp\hat{\Gamma} \leqslant 2n-2$.

Полученные оценки экспонентов множеств графов имеют порядок $\mathrm{O}(n)$. В то же время экспонент отдельного орграфа множества в ряде случаев имеет порядок $\mathrm{O}(n^2)$ и достигает максимального значения n^2-2n+2.

ЛИТЕРАТУРА

1. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Изд-во Юрайт, 2016. 209 с.
2. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
3. *Авезова Я. Э., Фомичев В. М.* Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикладная дискретная математика. 2017. №1(35). С. 89–101.

УДК 519.7 DOI 10.17223/2226308X/10/26

ПРИМЕНЕНИЕ АЛГОРИТМОВ РЕШЕНИЯ ПРОБЛЕМЫ БУЛЕВОЙ ВЫПОЛНИМОСТИ ФОРМУЛ ДЛЯ ОЦЕНКИ СТОЙКОСТИ БЛОЧНЫХ ШИФРОВ СЕМЕЙСТВА ГОСТ К АЛГЕБРАИЧЕСКОМУ КРИПТОАНАЛИЗУ[1]

Л. К. Бабенко, Е. А. Маро

Представлено применение методов алгебраического анализа к стандартам симметричного шифрования Магма и Present. В качестве способов решения систем булевых нелинейных уравнений выбраны: 1) сведение к задаче выполнимости булевых формул (SAT-задаче) и решение с помощью CryptoMiniSat; 2) применение метода расширенной линеаризации. Для данных методов рассмотрены методики проведения оценки защищённости информации методами алгебраического криптоанализа при использовании симметричных блочных шифров. Проведены эксперименты, показывающие применимость алгебраических методов криптоанализа для сокращённого числа раундов исследуемых шифров. Для шифра Магма выполнен алгебраический анализ при различных заполнениях блоков замены: заданном в стандарте, тождественной замене и замене, являющейся слабой к линейному анализу.

Ключевые слова: *криптография, алгебраический криптоанализ, блочные алгоритмы шифрования, Магма, PRESENT, SAT-решатель, SageMath.*

В современном криптографическом научном сообществе на протяжении последних 15 лет развиваются и совершенствуются методы алгебраического криптоанализа, основанные на использовании нелинейных примитивов алгоритмов шифрования с целью описания алгоритма шифрования в виде систем уравнений, связывающих искомый ключ и известные данные. Повышение производительности современных SAT-решателей привело к возникновению идеи о возможности их применения для вычислительно трудоёмких задач криптоанализа [1 – 3]. Применяются различные методики проведения алгебраического криптоанализа на основе SAT-решения и построения

[1]Работа выполнена при поддержке гранта РФФИ, проект №17-07-00654 А.