

О РАЗВЕТВЛЕНИЯХ КРИПТОГРАФИЧЕСКИХ ФУНКЦИЙ НА ПРЕОБРАЗОВАНИЯ С ЗАДАНЫМ ПРИЗНАКОМ

К. Г. Когос, В. М. Фомичев

Национальный исследовательский ядерный университет (МИФИ), г. Москва, Россия

E-mail: fomichev@nm.ru

Понятийный аппарат, связанный с разветвлением функций на линейные подфункции, обобщен для разветвлений функций специального вида на преобразования, имеющие заданный признак. Получены оценки характеристик для разветвлений функций, реализуемых генераторами « δ - τ шагов» и с перемежающимся шагом.

Ключевые слова: степень разветвления, признак в полугруппе, генераторы гаммы с неравномерным движением, генератор с перемежающимся шагом.

Анализ криптографических систем алгебраическими методами состоит в разработке методов решения систем алгебраических уравнений (САУ) и оценке вычислительной сложности их решения. Известно, что от решения нелинейной САУ можно перейти к решению нескольких линейных систем (СЛАУ) путем фиксации константами нескольких переменных. Вместе с тем не только линеаризация систем уравнений представляет интерес для анализа криптографических свойств, важно свести САУ к системам уравнений определенного вида, левая часть которых задает преобразования, имеющие заданный признак [1, гл. 9].

Целью работы является обобщение понятийного аппарата, связанного с разветвлением функций на линейные подфункции [2], для разветвлений функций специального вида на преобразования, имеющие заданный признак, и исследование криптографических характеристик функций, реализуемых в некоторых генераторах гаммы с неравномерным шагом.

При натуральных n, m рассмотрим множество $\Phi_{n,m}$ всех отображений $V^n \rightarrow V^m$, $n > m$, $V = \{0, 1\}$. Пусть функция $g \in \Phi_{n,m}$ задается системой координатных функций $\{g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)\}$. Определим умножение булева монома $\mu = x_{i_1} \cdot \dots \cdot x_{i_p}$ степени p на отображение $g \in \Phi_{n,m}$:

$$\mu \cdot g(x_1, \dots, x_n) = \{\mu \cdot g_1(x_1, \dots, x_n), \dots, \mu \cdot g_m(x_1, \dots, x_n)\}.$$

Обозначим через $g_{x_1, \dots, x_k}^{\alpha_1, \dots, \alpha_k}(x_{k+1}, \dots, x_n)$ ограничение функции g на множество $(\alpha_1, \dots, \alpha_k, x_{k+1}, \dots, x_n)$. Здесь $\alpha_1, \dots, \alpha_k$ — фиксированные значения; $x_{k+1}, \dots, x_n$ — булевы переменные. Сформулируем обобщение теоремы о разложении булевой функции по переменным на отображения из множества $\Phi_{n,m}$.

Теорема 1. Для любой функции $g \in \Phi_{n,m}$ выполнено равенство

$$g(x_1, \dots, x_n) = \bigoplus_{(\sigma_1, \dots, \sigma_k) \in V^k} x_1^{\sigma_1} \cdot \dots \cdot x_k^{\sigma_k} \cdot g_{x_1, \dots, x_k}^{\sigma_1, \dots, \sigma_k}(x_{k+1}, \dots, x_n).$$

Итак, множество подфункций $\{g(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n) : (\sigma_1, \dots, \sigma_k) \in V^k\}$ однозначно задает отображение $g : V^n \rightarrow V^m$ при любом k и любом наборе фиксируемых

координат. Будем говорить, что отображение $g \in \Phi_{n,m}$ разветвляется на отображения $g_{x_1, \dots, x_k}^{\alpha_1, \dots, \alpha_k}(x_{k+1}, \dots, x_n)$.

Рассмотрим случай, когда фиксируется $k = n - m$ переменных. Тогда отображение g разветвляется на преобразования множества V^m . Набор номеров фиксируемых переменных обозначим I , то есть $I = \{i_1, \dots, i_{n-m}\}$, где $\{i_1, \dots, i_{n-m}\} \subseteq \{1, \dots, n\}$, а набор фиксируемых переменных обозначим $x(I)$, то есть $x(I) = \{x_{i_1}, \dots, x_{i_{n-m}}\}$.

Определение 1. *Степенью I -разветвления отображения $g \in \Phi_{n,m}$ называется число различных преобразований $V^m \rightarrow V^m$, полученных при фиксации всевозможными наборами двоичных констант набора переменных $x(I)$; обозначается $\mathfrak{a}_I(g)$.*

Напомним основные определения теории признаков в полугруппах [1, гл. 9].

Пусть G — конечная полугруппа, ее систему образующих обозначим через $S = \{s_1, \dots, s_p\} \subset G$, $p \in \mathbb{N}$, $G = \langle S \rangle$. Известно, что произвольный элемент g полугруппы G представляется словом в алфавите S . Признаком H (H -признаком) в полугруппе G называется подмножество H полугруппы G , состоящее из всех элементов G , обладающих определенным свойством. Элемент g полугруппы G имеет признак H , если $g \in H$. Непустое множество $R \subseteq G$ имеет H -признак, если $R \cap H \neq \emptyset$; R не имеет H -признака или имеет пустой H -признак, если $R \cap H = \emptyset$. Признак H в R называется тривиальным, если $|R \cap H| = 1$ (нетривиальным, если $|R \cap H| > 1$).

Определение 2. Пусть при всех фиксациях набора переменных $x(I)$ функция $g \in \Phi_{n,m}$ разветвляется только на преобразования, имеющие признак H . Тогда набор $x(I)$ назовем *вполне H -сводящим функцию g* , а число различных преобразований $V^m \rightarrow V^m$, полученных при фиксации всевозможными наборами двоичных констант набора переменных $x(I)$ и имеющих признак H , назовем *степенью (I, H) -разветвления функции g* и обозначим $\mathfrak{a}_{I(g,H)}$.

Определение 3. Пусть при всех фиксациях набора переменных $x(I)$ функция $g \in \Phi_{n,m}$ разветвляется только на линейные преобразования. Тогда набор $x(I)$ назовем *вполне линейризующим функцию g* , а число различных линейных преобразований $V^m \rightarrow V^m$, полученных при фиксации всевозможными наборами двоичных констант набора переменных $x(I)$, назовем *степенью линейного I -разветвления функции g* и обозначим $\lambda_I(g)$.

Пусть $N_n = \{1, \dots, n\}$, где n — натуральное число.

Определение 4. *Степенью разветвления функции g называется $\min_{I \subseteq N_n} \{\mathfrak{a}_I(g)\}$, где минимум берется по всем наборам $x(I)$ порядка $n - m$, эта величина обозначается $\mathfrak{a}(g)$.*

Определение 5. *Степенью H -разветвления функции g называется $\min_{I \subseteq N_n} \{\mathfrak{a}_I(g, H)\}$, где минимум берется по всем вполне H -сводящим наборам $x(I)$ порядка $n - m$, эта величина обозначается $\mathfrak{a}(g, H)$.*

Определение 6. *Степенью линейного разветвления функции g называется $\min_{I \subseteq N_n} \{\lambda_I(g)\}$, где минимум берется по всем наборам $x(I)$ порядка $n - m$, вполне линейризующим функцию g , эта величина обозначается $\lambda(g)$.*

Заметим, что если H есть моноид всех преобразований множества V^m , то $\mathfrak{a}_I(g, H) = \mathfrak{a}_I(g)$, $\mathfrak{a}(g, H) = \mathfrak{a}(g)$. Если H есть полугруппа всех линейных преобразований множества V^m , то $\mathfrak{a}_I(g, H) = \lambda_I(g)$, $\mathfrak{a}(g, H) = \lambda(g)$.

Далее без потери общности считаем, что фиксируются первые $n - m$ переменных, то есть $x_1, \dots, x_{n-m}$.

Для любой функции $g \in \Phi_{n,m}$, которая разветвляется только на преобразования, имеющие признак H , справедлива универсальная оценка степени (I, H) -разветвления:

$$1 \leq \mathfrak{a}_I(g, H) \leq \min(2^{n-m}, |H|).$$

Отметим, что нижние и верхние границы достижимы:

- 1) $\mathfrak{a}_I(g, H) = 1$, если функция g при любом опробовании сводится к единственному преобразованию из множества H ;
- 2) $\mathfrak{a}_I(g, H) = 2^{n-m}$, если $2^{n-m} \leq |H|$ и различны все преобразования из множества H , на которые разветвляется функция g ;
- 3) $\mathfrak{a}_H(g) = |H|$, если $2^{n-m} \geq |H|$ и каждое преобразование из множества H соответствует хотя бы одному опробованию набора переменных $x(I)$.

В частности, справедливы тривиальные оценки степени I -разветвления и степени линейного I -разветвления:

$$1 \leq \mathfrak{a}_I(g) \leq \min(2^{n-m}, 2^{m \cdot 2^m}), \quad (1)$$

$$1 \leq \lambda_I(g) \leq \min(2^{n-m}, 2^{m^2}).$$

Для криптографических приложений представляет интерес описание класса функций из $\Phi_{n,m}$, для которых оценка степени (I, H) -разветвления существенно ниже, чем в (1).

Введенное понятие степени разветвления функций может быть использовано для анализа некоторых генераторов гаммы с неравномерным движением. Неравномерное движение информации в регистрах генератора используется для введения нелинейной зависимости знаков выходной гаммы от ключевых элементов генератора, в качестве которого фигурирует начальное заполнение регистров. В этом случае степень линейного разветвления характеризует сложность определения начального заполнения генератора с помощью линеаризации уравнений.

Рассмотрим генератор « δ - τ шагов» [1, с. 316], представляющий собой двухблочную схему, где управляющий автомат есть фильтрующий генератор на базе ЛРС-1 (линейного регистра сдвига) длины n с фильтрующей булевой функцией $f(x)$, а генерирующий автомат есть ЛРС-2 длины m (с одной из ячеек которого снимается гамма), продвижение информации в котором зависит от управляющего знака, поступающего от ЛРС-1.

Обозначим $x_i = (x_{i,n}, \dots, x_{i,1})$, $y_i = (y_{i,m}, \dots, y_{i,1})$ состояния ЛРС-1 и ЛРС-2 соответственно в i -м такте, $i = 1, 2, \dots$; $x_1 = x$, $y_1 = y$ — их начальные состояния. Уравнения гаммообразования генератора имеют вид

$$\gamma_i = y_{\sigma(i,x),1},$$

где $\sigma(i, x)$ — суммарная «глубина продвижения» ЛРС-2 после первых i тактов функционирования:

$$\sigma(i, x) = \sum_{j=1}^i (\delta(f(x_j) \oplus 1) + \tau \cdot f(x_j)). \quad (2)$$

Ключом генератора являются начальные состояния ЛРС-1, ЛРС-2, а также функция усложнения f . Заметим, что состояние ЛРС-2 после l тактов функционирования зависит от поступившей от ЛРС-1 управляющей последовательности длины l и начального состояния ЛРС-2.

Зададим отображение ψ следующим образом: $\psi \in \Phi_{m+l,m}$, а именно ψ отображает множество управляющих последовательностей длины l и множество начальных состояний ЛРС-2 во множество состояний ЛРС-2 после l тактов функционирования генератора. Зафиксируем множество управляющих последовательностей и рассмотрим преобразования, на которые разветвляется отображение ψ . Таким образом, $I = \{1, \dots, l\}$, далее индекс I опускаем.

Теорема 2. Справедлива оценка степени линейного разветвления отображения ψ :

$$\lambda(\psi) \leq l + 1. \quad (3)$$

Доказательство. Пусть g — линейная подстановка, реализуемая за один такт генерирующим ЛРС-2. При фиксации начального состояния x ЛРС-1 соответствующая управляющая последовательность длины l определяется однозначно и функция ψ совпадает с линейным преобразованием $g^{\sigma(l,x)}$ множества V^m . Следовательно, степень линейного разветвления функции ψ не превосходит числа различных значений, которые принимает величина $\sigma(l, x)$. В соответствии с (2) значение $\sigma(l, x)$ зависит только от веса управляющей последовательности длины l . Таким образом, $\lambda(\psi) \leq l + 1$. ■

Данный результат в общем случае допускает уточнение, так как в теореме не учитываются структурные свойства управляющей последовательности, а именно то, что она может быть, например, линейной рекуррентной последовательностью. С целью уточнения полученных результатов реализован вычислительный эксперимент. На языке C++ написана программа, реализующая фильтрующий генератор (управляющий блок генератора « δ - τ шагов») на базе ЛРС-1 длины 17 с функцией обратной связи, соответствующей примитивному многочлену $1 \oplus x^3 \oplus x^{17}$, что обеспечивает максимальную длину периода ЛРС-1. Фильтрующая функция генератора $f(x) = x_1 x_2 \oplus x_{17}$ сбалансирована в силу линейности по x_{17} . В результате выполнения программы для ЛРС-1 получено, что функция «число единиц в выходной последовательности длины 2^{10} » при различных ненулевых начальных состояниях принимает всего 157 значений. Заметим, что данное значение существенно ниже верхней границы неравенства (3).

Усложнением генератора « δ - τ шагов» является генератор с перемежающимся шагом [1, с. 318]. Его гамма образуется как сумма гамм двух генераторов «стоп — вперед» с генерирующими ЛРС-2 и ЛРС-3 длин m и r соответственно. Оба генерирующих регистра имеют общий управляющий блок — фильтрующий генератор с фильтрующей булевой функцией $f(x)$ на базе ЛРС-1 длины n .

Обозначим $x_i = (x_{i,n}, \dots, x_{i,1})$, $y_i = (y_{i,m}, \dots, y_{i,1})$, $z_i = (z_{i,r}, \dots, z_{i,1})$ — состояния ЛРС-1, ЛРС-2 и ЛРС-3 соответственно в i -м такте, $i = 1, 2, \dots$; $x_1 = x$, $y_1 = y$, $z_1 = z$ — начальные состояния регистров. Уравнения гаммообразования генератора имеют вид

$$\gamma_i = y_{\sigma(i,x),1} \oplus z_{i-\sigma(i,x),1},$$

где $\sigma(i, x)$ — суммарная «глубина продвижения» ЛРС-2 после первых i тактов функционирования:

$$\sigma(i, x) = \sum_{j=1}^i f(x_j).$$

Ключом генератора являются начальные состояния ЛРС-1, ЛРС-2, ЛРС-3, а также функция усложнения f . Состояния ЛРС-2, ЛРС-3 после l тактов функционирования зависят от поступившей от ЛРС-1 управляющей последовательности длины l и начальных состояний ЛРС-2, ЛРС-3.

Зададим отображение $\pi \in \Phi_{m+r+l, m+r}$ следующим образом: π отображает множество начальных состояний ЛРС-2, ЛРС-3 и множество управляющих последовательностей длины l во множество состояний ЛРС-2, ЛРС-3 после l тактов функционирования генератора. Зафиксируем множество управляющих последовательностей и рассмотрим преобразования, на которые разветвляется отображение π . Аналогично теореме 2 доказывается следующая теорема.

Теорема 3. Справедлива оценка степени линейного разветвления отображения π :

$$\lambda(\pi) \leq l + 1.$$

Полученные результаты могут быть использованы для криптографического анализа криптосистем, построенных на основе некоторых генераторов гаммы с неравномерным движением. Перспективным направлением представляется исследование разветвлений криптографических функций на преобразования, имеющие признак H не только линейный.

ЛИТЕРАТУРА

1. Фомичёв В. М. Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.
2. Логачёв О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004. 470 с.