имеет быстродействие в среднем в 1,34 раза меньше, чем ПЛИС-реализация на Virtex-5 XCVLX330T, а Perl-реализация в 2,6 раза медленнее RНР-реализации.

В целом, проведённые исследования показывают, что шифр FАРКС-4, как и базовый FАРКС, имеет коэффициент эффективности ПЛИС-реализации намного больше, чем RSA, но FАРКС-4 существенно медленнее FАРКС. Кроме того, реализация FАРКС-4 на ПЛИС имеет более высокое быстродействие по сравнению с программными реализациями этой шифрсистемы.

ЛИТЕРАТУРА

1. *Tao R. J.* Finite Automata and Application to Cryptography. Tsinghua University Press and Springer, 2008.
2. *Ковалев Д. С., Тренькаев В. Н.* Реализация на ПЛИС шифра FАРКС // Прикладная дискретная математика. Приложение. 2011. №4. С. 33–34.
3. *Bao F. and Igarashi Y.* Break Finite Automata Public Key Cryptosystem // LNCS. 1995. V. 944. P. 147–158.
4. *Wollinger T., Guajardo J., and Paar C.* Cryptography on FPGAs: State of the art implementations and attacks // ACM Transactions on Embedded Computing Systems. 2004. V. 3. Iss. 3. P. 534–574.

УДК 519.6

КРИПТОГРАФИЧЕСКИЕ СВОЙСТВА РАЗВЕТВЛЕНИЙ ФУНКЦИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ

К. Г. Когос, В. М. Фомичев

К основным задачам алгебраического анализа криптографических систем относятся разработка методов решения систем алгебраических уравнений (САУ) и оценка вычислительной сложности их решения. Один из приёмов решения состоит в том, что от нелинейной САУ можно перейти к решению нескольких линейных систем (СЛАУ) путем фиксации константами нескольких переменных. Этот подход достаточно детально рассмотрен в [1] на примере для разветвлений функций, реализуемых генератором « δ - τ шагов» и генератором с перемежающимся шагом. Вместе с тем не только линеаризация систем уравнений представляет интерес для анализа криптографических свойств. Более общий подход заключается в сведении САУ к системам уравнений определённого вида, левая часть которых задает преобразования, имеющие заданный признак [2, гл. 9].

Представим некоторые результаты исследования разветвлений криптографических функций векторных пространств над полем $GF(2)$ на преобразования, имеющие заданный признак.

При натуральных n, m рассмотрим множество $\Phi_{n,m}$ всех отображений $V^n \rightarrow V^m$, $n > m$, $V = \{0, 1\}$. Требуется решить нелинейную систему булевых уравнений

$$g(x_1, \dots, x_n) = a, \quad (1)$$

где $g \in \Phi_{n,m}$ и $a \in V^m$. Пусть функция $g(x_1, \dots, x_n)$ 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. Возможность разветвления функции на подфункции определённого вида вытекает из обобщения теоремы о разложении булевой функции по переменным.

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, функция $g : V^n \rightarrow V^m$ однозначно задана при любом k и всевозможных наборах фиксаций переменных $x_1, \dots, x_k$ множеством подфункций $\{g(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n) : (\sigma_1, \dots, \sigma_k) \in V^k\}$, реализующих отображения $V^{n-k} \rightarrow V^m$. При таком представлении говорят, что отображение $g \in \Phi_{n,m}$ разветвляется на отображения $g_{x_1, \dots, x_k}^{\alpha_1, \dots, \alpha_k}(x_{k+1}, \dots, x_n)$. Множество решений системы (1) содержится в объединении множеств решений систем уравнений

$$g(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n) = a. \quad (2)$$

Если $g(\sigma_1, \dots, \sigma_k, x_{k+1}, \dots, x_n)$ есть линейные преобразования множества V^{n-k} ранга $n - k$, то каждая из последних систем может быть решена с полиномиальной от $n - k$ сложностью. Принципиальная сложность реализации такого подхода состоит в построении соответствующего разветвления функции $g(x_1, \dots, x_n)$. Вместе с тем имеются случаи, когда такое построение практически возможно.

Пусть фиксируется $k = n - m$ переменных, без потери для общности считаем, что фиксируются переменные $x_1, \dots, x_{n-m}$, тогда функция g разветвляется на преобразования множества V^m .

Определение 1. Степенью 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 $x_1, \dots, x_{n-m}$; обозначается как $\aleph(g)$.

Определение 2. Пусть при всех фиксациях набора переменных $x_1, \dots, x_{n-m}$ функция g разветвляется только на преобразования, имеющие признак H (линейный признак). Тогда набор $(x_1, \dots, x_{n-m})$ назовем вполне H -сводящим (вполне линейаризующим) функцию g , а число различных преобразований $V^m \rightarrow V^m$, имеющих признак H , полученных при различных фиксациях переменных, назовем степенью H -разветвления (линейного разветвления) функции g . Эти величины, обозначаемые $\aleph(g, H)$ и $\lambda(g)$, определяют число различных систем уравнений вида (2), к которым сводится решение системы (1).

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

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

Отметим, что нижние и верхние границы достижимы:

- 1) $\aleph(g, H) = 1$, если функция g при любом опробовании сводится к единственному преобразованию из множества H ;
- 2) $\aleph(g, H) = 2^{n-m}$, если $2^{n-m} \leq |H|$ и различны все преобразования из множества H , на которые разветвляется функция g ;
- 3) $\aleph(g) = |H|$, если $2^{n-m} \geq |H|$ и каждое преобразование из множества H соответствует хотя бы одному опробованию набора переменных $x_1, \dots, x_{n-m}$.

Для криптографических приложений представляет интерес описание класса функций из $\Phi_{n,m}$, для которых оценка степени H -разветвления существенно ниже данных оценок. В частности, в [1] показано, что при фиксации l переменных, соответствующих знакам управляющей последовательности, преобразование генерирующих регистров генератора « δ - τ шагов» [2, с. 316] и преобразование генератора с перемежающимся шагом [2, с. 318] имеют степени линейного разветвления, не превышающие $l + 1$.

Представим также другой важный для приложений подход к построению разветвлений преобразований множества X^n , где X — конечное множество.

Будем говорить, что преобразование φ имеет признак H на множестве Y , где $Y \subseteq X^n$, если найдётся преобразование ψ с признаком H , такое, что $\varphi(x) = \psi(x)$ при любом $x \in Y$. Разбиение множества X^n с системой блоков $(Y_1, \dots, Y_r)$ назовём вполне H -сводящим преобразование φ , если φ имеет признак H на каждом из множеств $Y_1, \dots, Y_r$, то есть φ совпадает на множестве Y_i с преобразованием ψ_i , имеющим признак H , $i = 1, \dots, r$. В этом случае будем говорить, что φ разветвляется на преобразования $\psi_1, \dots, \psi_r$ с признаком H в соответствии с разбиением $(Y_1, \dots, Y_r)$.

Порядком H -сводимости преобразования φ назовём наименьший из порядков разбиений множества X^n , которые являются вполне H -сводящими преобразование φ .

Приведём пример. Пусть $H = T_\Delta \cup T_\nabla$, где T_Δ — множество треугольных преобразований пространства V^n , задаваемых системами координатных булевых функций вида $\{f_1(x_1), f_2(x_1, x_2), \dots, f_n(x_1, \dots, x_n)\}$ и T_∇ — двойственное множество треугольных преобразований пространства V^n , задаваемых системами координатных булевых функций вида $\{f_1(x_1, \dots, x_n), f_2(x_2, \dots, x_n), \dots, f_n(x_n)\}$. Обозначим через $\psi(x_1, \dots, x_n)$ булеву функцию, отличную от константы, и построим преобразование $\varphi(x_1, \dots, x_n)$ пространства V^n :

$$\varphi(x_1, \dots, x_n) = \psi(x_1, \dots, x_n)g(x_1, \dots, x_n) \oplus \bar{\psi}(x_1, \dots, x_n)g'(x_1, \dots, x_n),$$

где $g \in T_\Delta$, $g' \in T_\nabla$. Для заданного признака H функция $\psi(x_1, \dots, x_n)$ может быть выбрана так, что $\varphi \notin H$, при этом порядок H -сводимости преобразования φ равен 2. Для преобразования φ блоками вполне H -сводящего разбиения пространства V^n являются множества истинности и ложности функции $\psi(x_1, \dots, x_n)$.

Этот пример интересен тем, что нелинейная система уравнений $\varphi(x_1, \dots, x_n) = a$, где $a \in V^n$, может быть решена с полиномиальной от n сложностью. Заметим, что множество решений этой системы уравнений содержится в объединении множеств решений треугольных систем уравнений $g(x_1, \dots, x_n) = a$ и $g'(x_1, \dots, x_n) = a$. Как известно, при естественных вероятностных предположениях средняя трудоёмкость решения треугольных систем уравнений оценивается величиной порядка n [2, с. 356].

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 не только линейный признак.

ЛИТЕРАТУРА

1. Когос К. Г., Фомичев В. М. О разветвлениях криптографических функций на преобразования с заданным признаком // Прикладная дискретная математика. 2012. № 1(15). С. 50–54.
2. Фомичёв В. М. Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010.