УДК 519.7
DOI: 10.25559/SITITO.15.201901.52-58

Вычисление минимальной степени многочлена над конечным полем для векторного булевого отображения, заданного полиномами Жегалкина

С. А. Белов
Московский государственный университет имени М.В. Ломоносова, г. Москва, Россия
serbel.sci@gmail.com

Аннотация

Рассматриваются векторные отображения над множеством из нуля и единицы, заданные множеством булевых функций. Булевы функции, входящие в отображение, в свою очередь, задаются полиномами Жегалкина. Зафиксировав правило, по которому двоичным векторам ставятся в соответствие элементы конечного поля характеристики два, получаем взаимно-однозначное соответствие между отображениями векторного пространства в себя и функциями над конечным полем. Конечное поле рассматривается как кольцо многочленов с операциями сложения и умножения по модулю выбранного неприводимого многочлена. Известно, что любую функцию над конечным полем можно записать в виде полинома. При этом для различных неприводимых многочленов полиномы над конечным полем, соответствующие заданному векторному отображению, в общем случае, могут быть различными и иметь различные степени. Рассматривается задача поиска такого неприводимого многочлена, чтобы степень полинома над конечным полем была минимальной, при условии, что соответствие между двоичными векторами и элементами конечного поля задаётся использованием полиномиального базиса конечного поля. Для решения задачи булевы функции представляются своими трейс-формами. Из этого представления коэффициенты полинома над конечным полем выражаются через элементы дуального базиса конечного поля. Затем элементы дуального базиса выражаются через полиномиальный базис конечного поля и коэффициенты неприводимого многочлена. Таким образом, коэффициент полинома над конечным полем выражаются в полиномиальном базисе конечного поля. Полученные уравнения сводятся к системе булевых уравнений для коэффициентов неприводимого многочлена. Для решения системы булевых уравнений используется SAT-решатель. Приведены оценки сложности получения указанной системы булевых уравнений.

Ключевые слова: конечное поле, булевы функции, трейс-форма, интерполяционный криптоанализ, SAT-решатели.

Для цитирования: *Белов С. А.* Вычисление минимальной степени многочлена над конечным полем для векторного булевого отображения, заданного полиномами Жегалкина // Современные информационные технологии и ИТ-образование. 2019. Т. 15, № 1. С. 52-58. DOI: 10.25559/SITITO.15.201901.52-58

Calculation of the Minimum Degree of a Polynomial over a Finite Field for a Vector Boolean Map Given in ANF

S. A. Belov
Lomonosov Moscow State University, Moscow, Russia
serbel.sci@gmail.com

Abstract

We consider vector mappings over the set of 0 and 1 given by the set of Boolean functions. Boolean functions included in the map are given in ANF. Having fixed the rule according to which the binary vectors are associated with the elements of a finite field of characteristic two, we obtain a one-to-one correspondence between the mappings of the vector space into itself and the functions over the finite field. The finite field is considered as a ring of polynomials with the operations of addition and multiplication modulo the selected irreducible polynomial. It is known that any function over a finite field can be written as a polynomial. Moreover, for various irreducible polynomials, the polynomials over a finite field, corresponding to a given vector map, may in general be different and have different properties. We consider the problem of finding an irreducible polynomial such that the degree of a polynomial over a finite field is minimal, provided that the correspondence between binary vectors and elements of a finite field is given by using a polynomial basis of a finite field. We present an algorithm to solve this problem. Firstly we rewrite Boolean functions in trace form and calculate expressions for finite field polynomial coefficients. Then we calculate elements of dual basis as an expression of polynomial basis. Using them we obtain system pf Boolean equations. Finaly we solve system of Boolean equations by SAT-solver and filter reducible polynomials. We estimate of the complexity of obtaining the specified system of Boolean equations is $O\left(rd!\mathrm{d}^4 nlog\left(n\right)\right)$ bitwise operations.

Keywords: Finite Field, Boolean Function, Trace Form, Interpolation Cryptanalysis, SAT-Solvers.

For citation: Belov S.A. Calculation of the Minimum Degree of a Polynomial over a Finite Field for a Vector Boolean Map Given in ANF. *Sovremennye informacionnye tehnologii i IT-obrazovanie* = Modern Information Technologies and IT-Education. 2019; 15(1):52-58. DOI: 10.25559/SITITO.15.201901.52-58

1. Введение

В работе [1] Якобсеном и Кнудсеном был предложен метод криптоанализа блочных шифров, названный ими «Интерполяционный криптоанализ». Авторами было показано, что атака эффективна, когда степень полинома раундовой функции блочного шифра над конечным полем невелика. В работе [2] показано, что степень полинома над конечным полем, соответствующего булевому отображению, может сильно различаться в зависимости от выбора неприводимого многочлена для построения конечного поля. В этой работе была исследована структура ненулевых коэффициентов полиномов над конечным полем булевого отображения при выборе различных неприводимых многочленов. Авторы показали, как связаны коэффициенты полиномов одного и того же булевого отображения при выборе различных неприводимых многочленов для построения конечного поля. В представленной работе рассматривается вопрос нахождения таких неприводимых многочленов путём сведения этой задачи к задаче решения системы булевых уравнений. При этом считается, что булевы функции задаются своими полиномами Жегалкина. Представленный метод особенно эффективен при условии, что степени булевых функций невелики по сравнению с количеством переменных.

1.2 SAT-решатели

Вопросы, связанные с алгебраическими характеристиками криптографических отображений широко освещены в алгебраическом криптоанализе. Основной идеей алгебраического криптоанализа является сведение исходной задачи криптоанализа к системе булевых уравнений и решению полученной системы. В общем случае, решение произвольной системы булевых уравнений является сложной задачей. Для решения возникающих на практике при решении задач криптоанализа используются SAT-решатели. Впервые идея сведения задачи криптоанализа к проблеме SAT была предложена в работе [3], где SAT-решатель использовался для восстановления ключей DES. Предложенный метод был назван авторами «Логический криптоанализ». Авторы работы [4] предложили метод анализа стойкости хэш-функций MD4 и MD5 к атаке нахождения прообраза. В работе [5] SAT-решатель был использован для автоматизации части атаки для поиска коллизий, описанной в [6]. Также в работе [5] было упомянуто, что хотя прямое использование SAT-решателей не в состоянии взломать современные криптографические системы, но их использование является полезным в комбинации с другими методами криптоанализа. В работе [7] авторы продемонстрировали это, рассмотрев атаку на хэш-функцию MD4 [8]. Примеры использования SAT-решателей для анализа потоковых шифров можно найти, например, в [9], [10]. Работа [11] посвящена алгебраическому криптоанализу шифра Keeloq. Сравнение эффективности SAT-решателей и методов, основанных на бизисах Грёбнера можно найти в [12]. SAT-решатели также применяются в задачах программной верификации [13, 14], проверки моделей [15, 16] и других. Существует множество программных реализаций SAT-решателей, например, Z3[1], MiniSAT[2], Cryptominisat[3] и другие.

1.3 Определения и обозначения

Введём определения и обозначения, которые будут использованы в дальнейшем, а также необходимые утверждения из теории конечных полей:

$GF(q)$ — конечное поле из q элементов. Для конечного поля $GF(q)$ число q имеет вид $q=p^n$, где p — простое число, а n — натуральное. Число p называется характеристикой конечного поля. Далее записи $GF(q)$ и $GF(p^n)$ будем считать равнозначными.

$F_q[x]$ — множество многочленов переменной x над полем $GF(q)$. Любая функция $f:GF(q)\to GF(q)$ может быть представлена в виде многочлена одной переменной над полем $GF(q)$ степени не более $q-1$.

$Tr(x)=\sum_{i=0}^{n-1}x^{2^i}$ — функция «след» в поле $GF(2^n)$. Определённая таким образом функция является отображением из $GF(2^n)$ в $GF(2)$.

Два базиса $\alpha_0,\ldots,\alpha_{n-1}$ и $\beta_0,\ldots,\beta_{n-1}$ конечного поля будем называть дуальными, если $Tr(\alpha_i\beta_j)=\begin{cases}0, & i\neq j\\ 1, & i=j\end{cases}$

Пусть F — функция над $GF(q)$. Через $deg(F)$ будем обозначать степень полинома этой функции над конечным полем.

Через $Perm(K)$ будем обозначать множество всех перестановок элементов множества K.

Булева функция от n переменных $f(x_1,\ldots,x_n)$ может быть единственным образом представлена в виде многочлена от переменных $x_1,\ldots,x_n$. Такое представление называется полиномом Жегалкина и имеет вид

$$a_0 \bigoplus_{1\le i_1\le\ldots\le i_m\le n, m\in\{1,2,\ldots,n\}} a_{i_1,i_2,\ldots,i_k}x_{i_1}x_{i_2}\ldots x_{i_m}$$

Пусть f — булева функция от n переменных. Через $def(f)$ будем обозначать степень булевой функции, т.е. число переменных в самом длинном слагаемом полинома Жегалкина функции f.

Старшими мономами булевой функции называются мономы её полинома Жегалкина, имеющие длину, равную степени булевой функции.

При изложении будем рассматривать функцию $F:\{0,1\}^n\to\{0,1\}^n$, с одной стороны, как функцию над конечным полем $F:GF(2^n)\to GF(2^n)$, с другой стороны, как вектор булевых функций $F(x)=(f_1(x_1,\ldots,x_n),\ldots,f_n(x_1,\ldots,x_n))$, где $f_i(x_1,\ldots,x_n)$ — булева функция от n переменных. В таком случае будем говорить, что булевы функции $f_1,\ldots,f_n$ составляют функцию F.

2. Полиномы Жегалкина

Пусть $GF(2)$ — поле из двух элементов, а $GF(2^n)$ — его расширение степени n. Тогда булеву функцию от n переменных f $(x_0,\ldots,x_{n-1})$ можно представить в виде функции $F:GF(2^n)\to GF(2)$. Или, так как $GF(2)$ является подполем $GF(2^n)$, $F:GF(2^n)\to GF(2^n)$.

Обозначим через $\alpha_0,\ldots,\alpha_{n-1}$ базис конечного поля, а через

[1] Z3 Theorem Prover/z3 [Электронный ресурс]. URL: https://github.com/Z3Prover/z3 (дата обращения: 21.01.2019).

[2] MiniSat Page [Электронный ресурс]. URL: http://minisat.se/ (дата обращения: 21.01.2019).

[3] *Soos M.* Cryptominisat [Электронный ресурс]. URL: https://github.com/msoos/cryptominisat (дата обращения: 21.01.2019).

$\beta_0, ..., \beta_{n-1}$ — дуальный к нему базис. Тогда для любого $x \in GF(2^n)$ однозначно определено разложение по базису $x = \sum_{i=0}^{n-1} \alpha_i x^i$, а в силу двойственности базисов верно $x_i = Tr(\beta_i x)$.

Таким образом, для любой булевой функции $f(x_0, ..., x_{n-1})$ имеет место равенство

$$f(x_0, ..., x_{n-1}) = f(Tr(\beta_0 x), Tr(\beta_1 x), ..., Tr(\beta_{n-1} x)) = \sum_{i=0}^{2^n-1} c_i x^i, c_i \in GF(2^n)$$

.

Такое представление булевой функции называется трейс-представлением. Трейс-представления булевых функций используется для анализа криптографических свойств булевых функций, [18, 19, 20].

Раскрывая скобки в предыдущем выражении и используя представления полинома Жегалкина получаем формулу для коэффициента c_i многочлена булевой функции над конечным полем.

$$c_i = \sum_{\substack{(k_0,...,k_{n-1}) = Perm(i_0 i_1 ... i_{n-1}) \\ a_{i_0 i_1 ... i_{n-1}} = 1 \\ \left(\sum_{j=0}^{n-1} k_j\right) mod\,(2^n - 1) = i}} \beta_0^{2^{k_0}} ... \beta_{n-1}^{2^{k_{n-1}}}$$

Теорема 1. [21] Пусть f — булева функция от n переменных, $deg(f) = d$. $F(x): GF(2^n) \to GF(2)$ — представление f над полем $GF(2^n)$.

Тогда $deg(F) \le 2^n - 2^{n-d}$, количество мономов в F не превосходит $\sum_{i=0}^{d} C_n^i$.

Теорема 2. Пусть $f(x_0, ..., x_{n-1}) = x_{i_1} ... x_{i_d}$ — булева функция степени d, состоящая из одного монома.

$F(x) = \sum_{i=0}^{2^n-1} c_i x^i, w = 2^n - 2^{n-d}$.

Тогда $c_w = \sum_{(k_1,...,k_d) \in Perm(\{i_1,...,i_d\}),} \beta_{k_1}^{2^{n-d}} \beta_{k_2}^{2^{n-d+1}} ... \beta_{k_d}^{2^{n-1}}$

Доказательство. Для старшего коэффициента существует (с точностью до перестановки) только один набор, дающий максимальную сумму по модулю $2^n - 1$. Из этого и выражения для произвольного коэффициента следует утверждение теоремы.

Теорема 3.

Пусть $F(x): GF(2^n) \to GF(2^n), F(x) = \sum_{i=0}^{2^n-1} c_i x^i$

$F(x) = (f_0(x), ..., f_{n-1}(x))$, где $f_0, ..., f_{n-1}$ — булевы функции, $F_j(x) = \sum_{i=0}^{2^n-1} c_i^{(j)} x^i$ — полином булевой функции f_j над конечным полем $GF(2^n)$ в полиномиальном базисе $\{1, \theta, \theta^2, ..., \theta^{n-1}\}$. $d = \max_{0 \le k \le n-1} deg(f_k)$, $w = 2^n - 2^{n-d}$. Тогда $c_w = \sum_{i=0}^{n-1} \theta^i c_w^{(i)}$

3. Выражения для дуального базиса

Пусть $F(x) = (f_0(x), ..., f_{n-1}(x))$ - полином над полем $GF(2^n)$. Обозначим $g(x) = 1 + a_1\theta + .. + a_{n-1}\theta^{n-1} + \theta^n, a_1, ..., a_{n-1} \in \{0,1\}$ — неприводимый многочлен степени n над полем $GF(2)$. $\{1, \theta, ..., \theta^{n-1}\}$ — полиномиальный базис поля $GF(2^n)$, $\beta_0, ..., \beta_{n-1}$ — дуальный к нему базис.$d = \max_{0 \le k \le n-1} deg(f_k)$, $w = 2^n - 2^{n-d}$. D_i - множество номеров переменных, входящих в старшие мономы полинома Жегалкина булевой функции $f_i(x)$. $F(x) = \sum_{i=0}^{w} c_i x^i$.

Согласно теореме 3

$$c_w = \sum_{i=0}^{n-1} \theta^i c_w^{(i)} = = \sum_{i=0}^{n-1} \theta^i \sum_{K \in D_i} \left(\sum_{(k_1,...,k_d) \in Perm(K)} \beta_{k_1}^{2^{n-d}} \beta_{k_2}^{2^{n-d+1}} ... \beta_{k_d}^{2^{n-1}} \right)$$

$$= \left(\sum_{i=0}^{n-1} \theta^{i 2^d} \sum_{K \in D_i} \left(\sum_{(k_1,...,k_d) \in Perm(K)} \beta_{k_1} \beta_{k_2}^2 ... \beta_{k_d}^{2^{d-1}} \right) \right)^{2^{n-d}}$$

Рассмотрим задачу определения при каком неприводимом многочлене старшая степень равно нулю (что равносильно $c_w = 0$) и покажем, как свести эту задачу к задаче решения системы булевых уравнений с неизвестными $a_1, ..., a_{n-1}$.

Теорема 4. [17] Пусть $\bar{\alpha} = \{1, \theta, ..., \theta^{n-1}\}$ -- полиномиальный базис поля $GF(p^n)$ и $g(x)$ — минимальный многочлен элемента θ над $GF(p)$.

Пусть $g(x) = (x - \theta)(b_0 + b_1 x + ... + b_{n-1} x^{n-1}), \beta_0, \beta_1, ... \beta_{n-1}, \theta \in GF(p^n)$

Тогда дуальным базисом к базису $\bar{\alpha}$ является базис $\bar{\beta} = \{\beta_0, \beta_1, ..., \beta_{n-1}\}$, где $\beta_i = \frac{b_i}{g'(\theta)}, i = 0,1, ..., n-1$.

Утверждение 1. В $GF(2^n)$ $b_{n-1} = 1, b_{i-1} = \theta b_i + a_i, i = n-1, ..., 1$

Доказательство.

$$(x + \theta)(b_{n-1} x^{n-1} + b_{n-2} x^{n-2} + ... + b_1 x + b_0) = (x + \theta)\left(\sum_{i=0}^{n-1} b_i x^i\right) =$$

$$\sum_{i=0}^{n-1} b_i x^{i+1} + \theta \sum_{i=0}^{n-1} b_i x^i = \theta b_0 + \sum_{i=1}^{n-1} (b_{i-1} + \theta b_i) x^i + b_{n-1} x^n$$

Утверждение 2. Пусть в $GF(2^n)$ $x^m = \sum_{i=0}^{n-1} c_i x^i, m > n$.

Тогда $x^{m+1} = c_{n-1} + \sum_{i=1}^{n-1} (c_{i-1} + c_{n-1} a_i) x^i$.

Доказательство.

$$x^{m+1} = x x^m = \sum_{i=0}^{n-1} c_i x^{i+1} + c_{n-1} x^n = \sum_{i=0}^{n-1} c_i x^{i+1} + c_{n-1}\left(\sum_{i=1}^{n-1} a_i x^i + 1\right) =$$

$$\sum_{i=1}^{n-1} c_{i-1} x^i + c_{n-1}\left(\sum_{i=1}^{n-1} a_i x^i + 1\right) = c_{n-1} + \sum_{1}^{n-1} (c_{i-1} + c_{n-1} a_i) x^i$$

Подставляя выражения из теоремы 4 в выражение для c_w имеем:

$$c_w = 0 \Leftrightarrow \left(\sum_{i=0}^{n-1} \theta^{i 2^d} \sum_{K \in D_i} \left(\sum_{(k_1,...,k_d) \in Perm(K)} \beta_{k_1} \beta_{k_2}^2 ... \beta_{k_d}^{2^{d-1}} \right) \right)^{2^{n-d}} = 0 \Leftrightarrow$$

$$\left(g'(\theta)^{-1} \sum_{i=0}^{n-1} \theta^{i 2^d} \sum_{K \in D_i} \left(\sum_{(k_1,...,k_d) \in Perm(K)} b_{k_1} b_{k_2}^2 ... b_{k_d}^{2^{d-1}} \right) \right)^{2^{n-d}} = 0 \Leftrightarrow$$

$$\sum_{i=0}^{n-1} \theta^{i 2^d} \sum_{K \in D_i} \left(\sum_{(k_1,...,k_d) \in Perm(K)} b_{k_1} b_{k_2}^2 ... b_{k_d}^{2^{d-1}} \right) = 0$$

Используя формулы из утверждения 1, производим замену $b_0, ..., b_{n-1}$ на многочлены переменной θ, содержащие только неизвестные a_i. Используя формулы из утверждения 2, преобразуем все выражения вида $\theta^m, m \ge n$. В результате получим многочлен $h(\theta) = \sum_{i=0}^{n-1} h_i(a_1, ..., a_{n-1}) \theta^i = 0$. Из которого получаем

систему булевых уравнений:

$$\begin{cases} h_0(a_1,\ldots,a_{n-1})=0 \\ h_1(a_1,\ldots,a_{n-1})=0 \\ \quad\ldots \\ h_{n-1}(a_1,\ldots,a_{n-1})=0 \end{cases}$$

Теорема 5. Пусть $f(x_0,\ldots,x_{n-1})$ - булева функция n переменных степени d, содержащая r мономов степени d. Сложность перехода для старшего коэффициента не превосходит $O\left(rd!\mathrm{d}^4 nlog(n)\right)$ битовых операций.

Доказательство. Согласно формуле для старшего коэффициента, необходимо подсчитать $rd!$ выражений вида $b_{k_1}b_{k_2}^2\ldots b_{k_d}^{2^{d-1}}$. Изначально каждый элемент b представляет собой полином степени n с коэффициентами, являющимися полиномами Жегалкина степени 1. Возведение b в степень m требует $O\left(\log(m)n\log(n)\right)$ операций умножения коэффициентов (полиномов Жегалкина При возведении элемента b в степень m длина этих полиномов Жегалкина не может стать более m. Для умножения двух полиномов Жегалкина длины t требуется $O\left(t^2\right)$. битовых операций. Тогда для вычисления одного выражения вида $b_{k_1}b_{k_2}^2\ldots b_{k_d}^{2^{d-1}}$ требуется $\sum_{i=1}^{d}\log\left(2^i\right)i^2 nlog(n)=O\left(\mathrm{d}^4 nlog(n)\right)$ битовых операций, а общая сложность $O\left(rd!\mathrm{d}^4 nlog(n)\right)$

Обобщая вышеописанное получаем алгоритм сведения исходной задачи к системе булевых уравнений:

Алгоритм 1:

1. Рассчитать $b_0,\ldots,b_{n-1}$ по формуле из утверждения 1;
2. Рассчитать $\theta^m, m\ge n$ по формуле из утверждения 2;
3. Рассчитать коэффициент по формуле (1);
4. Решить систему булевых уравнений, используя SAT-решатель;
5. Отсеять решения, которые соответствуют приводимым многочленам;
6. Если остались решения — выдать соответствующие неприводимые многочлены. Иначе выдать НЕТ.
7. **Пример**

В качестве примера рассмотрим S-box №2 для симметричного шифра ГОСТ 28147-89 из набора id-Gost28147-89-CryptoPro-B-ParamSet.

$s=[0,1,2,10,4,13,5,12,9,7,3,15,11,8,6,14]: GF(16)\to GF(16)$

В неприводимый многочлен имеет степень 4:

$g(x)=1+a_1\theta+a_2\theta^2+a_3\theta^3+\theta^4,\ a_1,a_2,a_3\in\{0,1\}$

$$s(x)=s_0(x_0,x_1,x_2,x_3)+s_1(x_0,x_1,x_2,x_3)\theta+$$
$$s_2(x_0,x_1,x_2,x_3)\theta^2+s_3(x_0,x_1,x_2,x_3)\theta^3$$

Булевы функции, составляющие $s(x)$ равны:

$$s_0(x_0,x_1,x_2,x_3)=x_0x_1x_2\oplus x_0x_1x_3\oplus x_0x_2x_3\oplus x_0x_1\oplus x_1x_2\oplus x_0x_3\oplus x_1\oplus x_3$$

$$s_1(x_0,x_1,x_2,x_3)=x_0x_1x_3\oplus x_1x_2\oplus x_0x_3\oplus x_2x_3\oplus x_1$$
$$s_2(x_0,x_1,x_2,x_3)=x_0x_2x_3\oplus x_1x_2x_3\oplus x_0x_3\oplus x_2x_3\oplus x_2$$
$$s_3(x_0,x_1,x_2,x_3)=x_0x_1x_2\oplus x_0x_1x_3\oplus x_0x_1\oplus x_0x_2\oplus x_0x_3\oplus x_1x_3\oplus x_3$$

Максимальная степень равна булевой функции 3, поэтому максимальная степень полинома над конечным полем не превосходит 14. Старшие мономы равны:

$s_0: x_0x_1x_2, x_0x_1x_3, x_0x_2x_3$

$s_1: x_0x_1x_3$

$s_2: x_0x_2x_3, x_1x_2x_3$

$s_3: x_0x_1x_2, x_0x_1x_3$

Вычислим элементы дуального базиса $b_0,\ldots,b_3$:

$b_3=1$

$b_2=a_3+\theta$

$b_1=a_2+a_3\theta+\theta^2$

$b_0=a_1+a_2\theta+a_3\theta^2+\theta^3$

Рассчитаем таблицу значений степеней θ:

$\theta^4=1+a_1\theta+a_2\theta^2+a_3\theta^3$

$\theta^5=a_3+(1+a_1a_3)\theta+(a_1+a_3a_2)\theta^2+(a_3+a_2)\theta^3.$

$$\theta^7=(a_1+a_3)+(a_1+a_1a_3+a_2+a_3)\theta$$
$$+(a_3+a_1a_3+a_3a_2)\theta^2+(1+a_2+a_3+a_3a_2)\theta^3$$

Подставив вычисленные значения получаем выражение для старшего коэффициента:

$$c_{14}=a_2+a_2\theta+(a_1a_2+a_3a_2+a_2)\theta^2+(a_3+a_1a_3+a_3a_2)\theta^3$$

Приравнивая коэффициент к 0, получаем систему уравнений:

$$\begin{cases} a_2=0 \\ a_2=0 \\ a_1a_2\oplus a_3a_2\oplus a_2=0 \\ a_3\oplus a_1a_3\oplus a_3a_2=0 \end{cases}$$

Решениями являются наборы:

$(a_1=0,a_2=0,a_3=0)$

$(a_1=1,a_2=0,a_3=0)$

$(a_1=1,a_2=0,a_3=1)$

Им соответствуют многочлены

$1+\theta^4$

$1+\theta+\theta^4$

$1+\theta+\theta^3+\theta^4$

Так как многочлены $1+\theta^4$ и $1+\theta+\theta^3+\theta^4$ являются приводимыми, решением является многочлен $1+\theta+\theta^4$. Таким образом в конечном поле, построенном как факторкольцо многочлена $1+\theta+\theta^4$, этот полином имеет степень строго меньше 14. При остальных неприводимых многочленах степень полинома этой функции над конечным полем равна 14.

Заключение

В работе представлен метод сведения задачи поиска неприводимого многочлена, при котором заданное отображение над векторным пространством, как полином над конечным полем, будет иметь минимальную степень к решению системы булевых уравнений для коэффициентов неприводимого многочлена. При составлении системы булевых уравнений используются выражения, полученные из трейс-формы булевых функций. Для решения полученных систем булевых уравнений используются SAT-решатели.

Список использованных источников

[1] *Jakobsen T., Knudsen L.R.* The interpolation attack on block ciphers // Fast Software Encryption. FSE 1997. Lecture Notes in Computer Science / E. Biham (eds). Springer, Berlin, Heidelberg, 1997. Vol. 1267. Pp. 28-40. DOI: 10.1007/BFb0052332

[2] *Youssef A.M., Gong G.* On the Interpolation Attacks on Block Ciphers // Fast Software Encryption. FSE 2000. Lecture

Notes in Computer Science / G. Goos, J. Hartmanis., J. van Leeuwen, B. Schneier (eds). Springer, Berlin, Heidelberg, 2001. Vol. 1978. Pp. 109-120. DOI: 10.1007/3-540-44706-7_8

[3] *Massacci F., Marraro L.* Logical Cryptanalysis as a SAT Problem // Journal of Automated Reasoning. 2000. Vol. 24, Issue 1-2. Pp. 165-203. DOI: 10.1023/A:1006326723002

[4] *Jovanović D., Janičić P.* Logical Analysis of Hash Functions // Frontiers of Combining Systems. FroCoS 2005. Lecture Notes in Computer Science / B. Gramlich (eds). Springer, Berlin, Heidelberg, 2005. Vol. 3717. Pp. 200-215. DOI: 10.1007/11559306_11

[5] *Mironov I., Zhang L.* Applications of SAT Solvers to Cryptanalysis of Hash Functions // Theory and Applications of Satisfiability Testing - SAT 2006. SAT 2006. Lecture Notes in Computer Science / A. Biere, C.P. Gomes (eds). Springer, Berlin, Heidelberg, 2006. Vol. 4121. Pp. 102-115. DOI: 10.1007/11814948_13

[6] *Wang X., Yu H.* How to Break MD5 and Other Hash Functions // Advances in Cryptology — EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science / R. Cramer (eds). Springer, Berlin, Heidelberg, 2005. Vol. 3494. Pp. 19-35. DOI: 10.1007/11426639_2

[7] *De D., Kumarasubramanian A., Venkatesan R.* Inversion Attacks on Secure Hash Functions Using sat Solvers // Theory and Applications of Satisfiability Testing — SAT 2007. SAT 2007. Lecture Notes in Computer Science / J. Marques-Silva, K.A. Sakallah (eds). Springer, Berlin, Heidelberg, 2007. Vol. 4501. Pp. 377-382. DOI: 10.1007/978-3-540-72788-0_36

[8] *Dobbertin H.* Cryptanalysis of MD4 // Fast Software Encryption. FSE 1996. Lecture Notes in Computer Science / D. Gollmann (eds). Springer, Berlin, Heidelberg, 1996. Vol. 1039. Pp. 53-69. DOI: 10.1007/3-540-60865-6_43

[9] *Eibach T., Pilz E., Völkel G.* Attacking Bivium Using SAT Solvers // Theory and Applications of Satisfiability Testing — SAT 2008. SAT 2008. Lecture Notes in Computer Science / H. Kleine Büning, X. Zhao (eds). Springer, Berlin, Heidelberg, 2008. Vol. 4996. Pp. 63-76. DOI: 10.1007/978-3-540-79719-7_7

[10] *Soos M., Nohl K., Castelluccia C.* Extending SAT Solvers to Cryptographic Problems // Theory and Applications of Satisfiability Testing - SAT 2009. SAT 2009. Lecture Notes in Computer Science / O. Kullmann (eds). Springer, Berlin, Heidelberg, 2009. Vol. 5584. Pp. 244-257. DOI: 10.1007/978-3-642-02777-2_24

[11] *Courtois N.T., Bard G.V., Wagner D.* Algebraic and Slide Attacks on KeeLoq // Fast Software Encryption. FSE 2008. Lecture Notes in Computer Science / K. Nyberg (eds). Springer, Berlin, Heidelberg, 2008. Vol. 5086. Pp. 97-115. DOI: 10.1007/978-3-540-71039-4_6

[12] *Erickson J., Ding J., Christensen C.* Algebraic Cryptanalysis of SMS4: Gröbner Basis Attack and SAT Attack Compared // Information, Security and Cryptology — ICISC 2009. ICISC 2009. Lecture Notes in Computer Science / D. Lee, S. Hong (eds). Springer, Berlin, Heidelberg, 2010. Vol. 5984. Pp. 73-86. DOI: 10.1007/978-3-642-14423-3_6

[13] *Chaki S., Clarke E.M., Groce A., Jha S., Veith H.* Modular verification of software components in C // IEEE Transactions on Software Engineering. 2004. Vol. 30, Issue 6. Pp. 388-402. DOI: 10.1109/TSE.2004.22

[14] *Cook B., Kroening D., Sharygina N.* Cogent: Accurate Theorem Proving for Program Verification // Computer Aided Verification. CAV 2005. Lecture Notes in Computer Science / K. Etessami, S.K. Rajamani (eds). Springer, Berlin, Heidelberg, 2005. Vol. 3576. Pp. 296-300. DOI: 10.1007/11513988_30

[15] *Biere A., Cimatti A., Clarke E., Zhu Y.* Symbolic Model Checking without BDDs // Tools and Algorithms for the Construction and Analysis of Systems. TACAS 1999. Lecture Notes in Computer Science / W.R. Cleaveland (eds). Springer, Berlin, Heidelberg, 1999. Vol. 1579. Pp. 193-207. DOI: 10.1007/3-540-49059-0_14

[16] *McMillan K.L.* Applying SAT Methods in Unbounded Symbolic Model Checking // Computer Aided Verification. CAV 2002. Lecture Notes in Computer Science / E. Brinksma, K.G. Larsen (eds). Springer, Berlin, Heidelberg, 2002. Vol. 2404. Pp. 250-264. DOI: 10.1007/3-540-45657-0_19

[17] *Menezes A.J.* et al. Applications of Finite Fields // The Springer International Series in Engineering and Computer Science / M. Ismail (eds). Springer US, 1993. Vol. 199. 218 p. DOI: 10.1007/978-1-4757-2226-0

[18] *Баев В.В.* Некоторые нижние оценки на алгебраическую иммунность функций, заданных своими след-формами // Проблемы передачи информации. 2008. Т. 44, № 3. С. 81-104. URL: http://www.mathnet.ru/links/c84fdb912415b6034762dbf94bdd1558/ppi1282.pdf (дата обращения: 21.01.2019).

[19] *Кузьмин А.С. , Марков В.Т. , Нечаев А.А. , Шишков А.Б.* Приближение булевых функций мономиальными // Дискретная математика. 2006. Т. 18, № 1. С. 9-29. URL: https://elibrary.ru/item.asp?id=9188329 (дата обращения: 21.01.2019).

[20] *Кузьмин А.С., Ноздрунов В.И.* Взаимосвязь коэффициентов полинома над полем и веса булевой функции // Прикладная дискретная математика. 2014. № 4(26). С. 28-36. URL: https://elibrary.ru/item.asp?id=22636126 дата обращения: 21.01.2019).

[21] *Carlet C.* Boolean Functions for Cryptography and Error-Correcting Codes // Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications) / Y. Crama, P. Hammer (eds). Cambridge: Cambridge University Press, 2010. Pp. 257-397. DOI: 10.1017/CBO9780511780448.011

Поступила 21.01.2019; принята к публикации 05.03.2019;
опубликована онлайн 19.04.2019.

Об авторе:

Белов Сергей Алексеевич, аспирант, факультет вычислительной математики и кибернетики, Московский государственный университет имени М.В. Ломоносова (119991, Россия, г. Москва, Ленинские горы, д. 1), ORCID: http://orcid.org/0000-0002-7923-0129, serbel.sci@gmail.com

Автор прочитал и одобрил окончательный вариант рукописи.

References

[1] Jakobsen T., Knudsen L.R. The interpolation attack on block ciphers. In: Biham E. (eds) Fast Software Encryption. FSE 1997. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1997; 1267: 28-40. (In Eng.) DOI: 10.1007/BFb0052332

[2] Youssef A.M., Gong G. On the Interpolation Attacks on Block Ciphers. In: Goos G., Hartmanis J., van Leeuwen J., Schneier B. (eds) Fast Software Encryption. FSE 2000. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2001; 1978:109-120. (In Eng.) DOI: 10.1007/3-540-44706-7_8

[3] Massacci F., Marraro L. Logical Cryptanalysis as a SAT Problem. *Journal of Automated Reasoning*. 2000; 24(1-2):165-203. (In Eng.) DOI: 10.1023/A:1006326723002

[4] Jovanović D., Janičić P. Logical Analysis of Hash Functions. In: Gramlich B. (eds) Frontiers of Combining Systems. FroCoS 2005. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2005; 3717:200-215. (In Eng.) DOI: 10.1007/11559306_11

[5] Mironov I., Zhang L. Applications of SAT Solvers to Cryptanalysis of Hash Functions. In: Biere A., Gomes C.P. (eds) Theory and Applications of Satisfiability Testing - SAT 2006. SAT 2006. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2006; 4121:102-115. (In Eng.) DOI: 10.1007/11814948_13

[6] Wang X., Yu H. How to Break MD5 and Other Hash Functions. In: Cramer R. (eds) Advances in Cryptology — EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2005; 3494:19-35. (In Eng.) DOI: 10.1007/11426639_2

[7] De D., Kumarasubramanian A., Venkatesan R. Inversion Attacks on Secure Hash Functions Using satSolvers. In: Marques-Silva J., Sakallah K.A. (eds) Theory and Applications of Satisfiability Testing — SAT 2007. SAT 2007. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2007; 4501:377-382. (In Eng.) DOI: 10.1007/978-3-540-72788-0_36

[8] Dobbertin H. Cryptanalysis of MD4. In: Gollmann D. (eds) Fast Software Encryption. FSE 1996. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1996; 1039:53-69. (In Eng.) DOI: 10.1007/3-540-60865-6_43

[9] Eibach T., Pilz E., Völkel G. Attacking Bivium Using SAT Solvers. In: Kleine Büning H., Zhao X. (eds) Theory and Applications of Satisfiability Testing — SAT 2008. SAT 2008. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2008; 4996:63-76. (In Eng.) DOI: 10.1007/978-3-540-79719-7_7

[10] Soos M., Nohl K., Castelluccia C. Extending SAT Solvers to Cryptographic Problems. In: Kullmann O. (eds) Theory and Applications of Satisfiability Testing - SAT 2009. SAT 2009. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2009; 5584:244-257. (In Eng.) DOI: 10.1007/978-3-642-02777-2_24

[11] Courtois N.T., Bard G.V., Wagner D. Algebraic and Slide Attacks on KeeLoq. In: Nyberg K. (eds) Fast Software Encryption. FSE 2008. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2008; 5086:97-115. (In Eng.) DOI: 10.1007/978-3-540-71039-4_6

[12] Erickson J., Ding J., Christensen C. Algebraic Cryptanalysis of SMS4: Gröbner Basis Attack and SAT Attack Compared. In: Lee D., Hong S. (eds) Information, Security and Cryptology — ICISC 2009. ICISC 2009. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2010; 5984:73-86. (In Eng.) DOI: 10.1007/978-3-642-14423-3_6

[13] Chaki S., Clarke E.M., Groce A., Jha S., Veith H. Modular verification of software components in C. *IEEE Transactions on Software Engineering*. 2004; 30(6):388-402. (In Eng.) DOI: 10.1109/TSE.2004.22

[14] Cook B., Kroening D., Sharygina N. Cogent: Accurate Theorem Proving for Program Verification. In: Etessami K., Rajamani S.K. (eds) Computer Aided Verification. CAV 2005. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2005; 3576:296-300. (In Eng.) DOI: 10.1007/11513988_30

[15] Biere A., Cimatti A., Clarke E., Zhu Y. Symbolic Model Checking without BDDs. In: Cleaveland W.R. (eds) Tools and Algorithms for the Construction and Analysis of Systems. TACAS 1999. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 1999; 1579:193-207. (In Eng.) DOI: 10.1007/3-540-49059-0_14

[16] McMillan K.L. Applying SAT Methods in Unbounded Symbolic Model Checking. In: Brinksma E., Larsen K.G. (eds) Computer Aided Verification. CAV 2002. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. 2002; 2404:250-264. (In Eng.) DOI: 10.1007/3-540-45657-0_19

[17] Menezes A.J. et al. Applications of Finite Fields. In: Ismail M. (eds) The Springer International Series in Engineering and Computer Science. Springer US. 1993; 199. (In Eng.) DOI: 10.1007/978-1-4757-2226-0

[18] Bayev V.V. Some lower bounds on the algebraic immunity of functions given by their trace forms. *Problems of Information Transmission*. 2008; 44(3):243-265. (In Eng.) DOI: 10.1134/S0032946008030071

[19] Kuzmin A.S., Markov V.T., Nechaev A.A., Shishkov A.B. Approximation of Boolean functions by monomial ones. *Discrete Mathematics and Applications*. 2006; 16(1):7-28. (In Eng.) DOI: 10.1515/156939206776241255

[20] Kuzmin A.S., Nozdrunov V.I. Relationship between the coefficients of polynomials over GF(2^n) and weights of Boolean functions represented by them. *Prikladnaya Diskretnaya Matematika*. 2014; 4(26):28-36. Available at: https://elibrary.ru/item.asp?id=22636126 (accessed 21.01.2019). (In Russ.)

[21] Carlet C. Boolean Functions for Cryptography and Error-Correcting Codes. Boolean Models and Methods in Mathematics, Computer Science, and Engineering (Encyclopedia of Mathematics and its Applications). Crama Y., Hammer P. (eds). Cambridge: Cambridge University Press, pp. 257-397. 2010. (In Eng.) DOI: 10.1017/CBO9780511780448.011

Submitted 21.01.2019; revised 05.03.2019;
published online 19.04.2019.

About the author:

Sergey A. Belov, graduate student, Faculty of Computational Mathematics and Cybernetics, Lomonosov Moscow State University (1, Leninskie gory, Moscow 119991, Russia), ORCID: http://orcid.org/0000-0002-7923-0129, serbel.sci@gmail.com

The author has read and approved the final manuscript.