Компьютерные инструменты в образовании, 2017
№ 3: 20–28
УДК: 519.719.2
http://ipo.spb.ru/journal

ОГРАНИЧЕННЫЙ ПОИСК КРИПТОГРАФИЧЕСКИ СИЛЬНЫХ БУЛЕВЫХ ФУНКЦИЙ

Агафонова И.В.[1], Дмитриева О.М.[2]

[1]СПбГУ, Санкт-Петербург, Россия
[2]СПбГУТ, Санкт-Петербург, Россия

Аннотация

В статье рассмотрены способы получения булевых функций с желательными криптографическими свойствами, основанные на поисковых алгоритмах. Исследованы возможности оптимизации таких алгоритмов, прежде всего за счет значительного сокращения области поиска. Использованы общая идея разбиения множества функций на классы эквивалентности в соответствии с какой-либо группой преобразований и идея перебора этих классов как вершин особого графа, называемого графом классов.

Предложенная в статье P-эквивалентность, рассматриваемая на множестве сбалансированных булевых функций, обеспечивает сохранение практически всех криптографически значимых свойств функций внутри одного класса эквивалентности.

Ключевые слова: *булевы функции, криптографические свойства, аффинная эквивалентность.*

Цитирование: Агафонова И.В., Дмитриева О.М. Ограниченный поиск криптографически сильных булевых функций // Компьютерные инструменты в образовании. 2017. № 3. С. 20–28.

1. ВВЕДЕНИЕ

Булева функция n переменных $f(x) = f(x_1, x_2, \dots, x_n)$ — это отображение из V_n в F_2, где F_2 — конечное поле с элементами 0 и 1, а через V_n обозначено n-мерное векторное пространство всех двоичных векторов, $V_n = (F_2)^n$.

Операции в F_2 — умножение и сложение по модулю 2. Для обозначения операции сложения по модулю 2 в F_2 примем знак $\oplus$, и этим же знаком будем обозначать операцию побитового сложения векторов в пространстве V_n.

Множество всех булевых функций от n переменных обозначим BF_n. Их число равно 2^{2^n}.

Булева функция $f(x) \in BF_n$ может быть задана списком ее значений при всех $x \in V_n$ (вектор значений, таблица истинности) или набором коэффициентов её полинома Жегалкина (алгебраическая нормальная форма, АНФ). В обоих способах задания булева функция однозначно определяется двоичным вектором длины 2^n при следующих договорённостях.

Запись f в виде двоичного вектора, например, $f = 01101001$ для $n = 3$, означает, что i-я координата вектора f есть значение $f(i)$, где аргумент i понимается уже как вектор длины n с координатами, соответствующими двоичному представлению числа i. Задание $f_{\text{АНФ}}$ как двоичного вектора, например, $f_{\text{АНФ}} = 01101000$, означает, что i-я координата есть коэффициент полинома Жегалкина при одночлене $x^i = x_1^{(i_1)} \cdot x_2^{(i_2)} \cdot \ldots \cdot x_n^{(i_n)}$.

Здесь обозначено

$$x_i^{(\alpha)} = \begin{cases} x_i, \alpha = 1, \\ 1, \alpha = 0, \end{cases} \quad x_i \in F_2, \quad \alpha \in F_2.$$

Имеется несколько базовых алгоритмов построения АНФ, о которых можно прочесть, например, в [1–3].

С представлением булевой функции в виде АНФ связаны следующие характеристики функции.

Алгебраическая степень булевой функции f есть степень АНФ этой функции как многочлена от нескольких переменных. Обозначать алгебраическую степень будем $\deg f$. При $\deg f \leqslant 1$ булева функция называется аффинной.

Алгебраическая иммунность $\mathrm{AI}(f)$ булевой функции f есть наименьшая степень булевой функции $g \neq 0$ такой, что $f(x)g(x) \equiv 0$ или $(f(x) \oplus 1)g(x) \equiv 0$. (Функции перемножаются как многочлены.)

Нелинейность $N(f)$ булевой функции f есть расстояние Хэмминга между f и множеством аффинных функций, то есть минимально возможное расстояние Хэмминга (равное числу несовпадающих координат) между вектором значений функции f и вектором значений аффинной функции. Как правило, для возможного применения функции f в криптосистемах требуется высокое значение $N(f)$.

2. ПРЕОБРАЗОВАНИЕ УОЛША-АДАМАРА И АВТОКОРРЕЛЯЦИЯ

Булева функция $f(x) \in BF_n$ называется сбалансированной (или уравновешенной), если она принимает значение 1 ровно на половине двоичных наборов длины n. Другими словами, сбалансированная функция — это функция веса 2^{n-1}, где вес (Хэмминга) функции f есть число единиц в её векторе значений.

Нелинейность, алгебраическая степень, алгебраическая иммунность и сбалансированность функции $f \in BF_n$ относятся к криптографическим характеристикам этой функции, то есть к характеристикам, которые следует учитывать для оценки стойкости криптосистем, использующих эту функцию.

Есть и другие важные показатели, по которым оценивают криптографическую ценность булевых функций. Всевозможные числовые характеристики такого рода и связывающие их ограничения широко обсуждаются в литературе, см. [1, 4–6]. Нередко криптографически значимые величины можно определить в терминах двух целочисленных функций на V_n, вычисляемых по заданной $f \in BF_n$.

Этими функциями являются:

- преобразование Уолша-Адамара $W_f(u) = \sum_{x \in V_n} (-1)^{\langle x,u \rangle \oplus f(x)}, u \in V_n$;
- автокорреляция $\Delta_f(u) = \sum_{x \in V_n} (-1)^{f(x) \oplus f(x \oplus u)}, u \in V_n$.

Здесь обозначено $\langle x, u \rangle = x_1 u_1 \oplus \ldots \oplus x_n u_n$.

Совокупности коэффициентов $\{W_f(u)\}, \{\Delta_f(u)\}$ при всех $u \in V_n$ называют спектрами соответственно Уолша-Адамара и автокорреляции.

Функцию $f \in BF_n$ называют корреляционно-иммунной порядка m, если $W_f(u) = 0$ для всех $u \in V_n$ веса от 1 до m, и m-эластичной, если $W_f(u) = 0$ для всех $u \in V_n$ веса от 0 до m. Таким образом, m-эластичная функция — это корреляционно-иммунная функция порядка m, для которой выполняется $W_f(0) = 0$. Последнее равенство эквивалентно условию сбалансированности функции f.

Если функция f имеет корреляционную иммунность порядка $m > 1$, то она будет также корреляционно-иммунной порядка i для всех $i = 1, 2, \ldots, m–1$.

Если для функции $f \in BF_n$ имеет место равенство $\Delta_f(u) = 0$ для всех $u \in V_n$ веса от 1 до k включительно, то говорят, что f удовлетворяет критерию распространения степени k (обозначение PC(k)). В случае PC(1) говорят также, что она удовлетворяет строгому лавинному критерию (SAC). Показатели PC(k) и SAC относят к локальным лавинным характеристикам.

По спектру автокорреляции вычисляются также глобальные лавинные характеристики (GAC): сумма квадратов $\sigma_f = \sum\limits_{u \in V_n} \Delta_f^2(u)$ и абсолютный показатель $\Delta_f = \max\limits_{\substack{u \in V_n \\ u \neq 0}} \left| \Delta_f(u) \right|$.

На практике нелинейность $N(f)$ функции $f \in BF_n$ вычисляется на основании её спектра Уолша-Адамара $\{W_f(u) \mid u \in V_n\}$ по широко известной формуле $N(f) = 2^{n-1} - \frac{1}{2} \max\limits_{u \in V_n} \left| W_f(u) \right|$.

Помимо высокого значения $N(f)$, отметим такой признак «хорошей нелинейности» булевой функции: она не должна линейно или фиктивно зависеть ни от одной из своих переменных и не должна приобретать такую зависимость после какой-либо линейной замены переменной (см, например, [1], утв. 14.) Этот признак формулируют так: функция не должна иметь ненулевых линейных структур. Оказывается, необходимым и достаточным условием этого является $\Delta_f \neq 2^n$ ([4], задача 8.100).

О том, как именно на криптостойкость булевых функций влияют её алгебраическая степень, нелинейность, сбалансированность, корреляционная иммунность и другие упомянутые здесь характеристики, можно подробнее узнать, например, из [7]. Здесь отметим только, что:

- сбалансированность булевой функции весьма желательна, как и выполнение SAC;
- отсутствие ненулевых линейных структур необходимо для булевых функций, используемых в блоковых шифрах [1];
- ценными для криптографического применения являются:
  - высокая алгебраическая степень, нелинейность, алгебраическая иммунность, корреляционная иммунность;
  - низкие значения глобальных лавинных характеристик;
- все характеристики функции не могут быть наилучшими одновременно. (Это подтверждает, например, приводимое ниже известное неравенство (1)).

3. ОГРАНИЧЕНИЯ НА ПАРАМЕТРЫ. ДОПОЛНИТЕЛЬНЫЕ ТРЕБОВАНИЯ К ФУНКЦИИ f

Поставим следующую задачу: при заданных целых m, d найти m-эластичную функцию f такую, что $\deg f \geqslant d$ и значение нелинейности $N(f)$ максимальное из возможных. Будем также отслеживать приемлемость других перечисленных выше криптографических характеристик.

На параметры этой задачи имеются ограничения, сужающие диапазоны значений параметров n, m, d. Отметим следующие факты [5, 8]:

- Если f из BF_n является m-эластичной функцией и $0 < m \leqslant n–2$, то
$$\deg f \leqslant n–m–1 \tag{1}$$
(неравенство Зигенталера).
- Если f из BF_n является m-эластичной функцией и $0 < m \leqslant n–2$, то
(a) $N(f) \leqslant 2^{n–1}–2^{m+1}$,
(b) $N(f) \leqslant 2^{n–1}–2^{m+1+[(n–m–2)/d]}$ при обозначении $d = \deg f$ (оценка (b) лучше оценки (a) в случае $d \leqslant n/2$).
- Если f из BF_n является m-эластичной функцией и $0 < m \leqslant n–3$, то $N(f) \leqslant 2^{n–1}–2^{m+2}$.

Далее мы рассматриваем поставленную задачу только на множестве сбалансированных функций из BF_n, существенно (не фиктивно) зависящих от всех n переменных.

Такие функции остаются сбалансированными и не приобретают фиктивных переменных при таких преобразованиях, как:

- Переименование переменных и/или добавление $\oplus 1$ к каким-то переменным, $x := xP \oplus b$, P — перестановочная матрица $n \times n, b \in V_n$ — вектор сдвигов.
- Инвертирование вектора значений функции, $f(x) := f(x) \oplus 1$.

4. КЛАССЫ ЭКВИВАЛЕНТНОСТИ БУЛЕВЫХ ФУНКЦИЙ

Нетрудно убедиться напрямую или получить из более общих формул для случая аффинной эквивалентности (3), приведённых, например, в [9], что спектры Уолша-Адамара функции $f(x)$ и полученной из неё после описанных в конце раздела 3 преобразований функции
$$f'(x) = f(xP \oplus b) \oplus \lambda \tag{2}$$
связаны соотношением
$$W_{f'}(u) = (-1)^{\langle b, uP\rangle \oplus \lambda} W_f(uP), \quad u \in V_n,$$
а спектры автокорреляции этих функций — соотношением
$$\Delta_{f'}(u) = \Delta_f(uP), \quad u \in V_n.$$

Важно, что, как показывают эти формулы, значения нелинейности и порядки корреляционной иммунности функций f и f' совпадают. Очевидно также, что две эти функции имеют одну и ту же алгебраическую степень и одно и то же значение AI(f), одни и те же показатели GAC и обе одновременно удовлетворяют либо не удовлетворяют PC(k) при конкретном k и SAC.

Таким образом, имея сбалансированную булеву функцию, мы имеем сразу целый класс получаемых из неё функций вида (2) при всевозможных перестановочных матрицах P, векторах b и $\lambda \in \{0,1\}$. Все функции этого класса будут иметь те же характеристики, что и f. Например, в одном классе с функцией $x_1x_2 + x_2x_3 + x_1x_3$ находятся ещё семь функций, полученных добавлением к ней одного из многочленов $x_1 + x_2$, $x_1 + x_3$, $x_2 + x_3$, 1, $1+x_1+x_2$, $1+x_1+x_3$, $1+x_2+x_3$. Все восемь функций сбалансированы и удовлетворяют PC(2).

В рамках этой статьи условимся использовать для преобразования (2) наименование «P-аффинное преобразование». Функции f и f', связанные такими соотношениями, будем называть P-эквивалентными, а подмножества эквивалентных друг другу функций — классами P-эквивалентности. Такая терминология удобна, чтобы отличать друг от друга классы, порождённые разными, хотя и похожими, преобразованиями. Отметим здесь, что в книге [10] описаны классы эквивалентности, порождённые пятью группами преобразований, и ни одна из разновидностей не совпадает в точности с классами P-эквивалентности.

P-эквивалентность является частным случаем аффинной эквивалентности булевых функций, которая в современной литературе определяется соответствием

$$f'(x) = f(xA \oplus b) \oplus \langle c, x\rangle \oplus \lambda \tag{3}$$

(см. [11]). Здесь A — невырожденная матрица, b и c — n-мерные двоичные векторы, λ равно 0 или 1,$\langle c, x\rangle = c_1x_1 \oplus \ldots \oplus c_nx_n$.

Часто упоминаемые в литературе аффинные преобразования вида $f'(x) = f(xA \oplus b)$ (полная аффинная группа преобразований AGL$(n,2)$, см. [4, 10, 12]), приводящие к другим классам эквивалентности (исследованным, например, в [16]), не обеспечивают сохранения порядка корреляционной иммунности и выполнения PC(k) и потому здесь не используются. Для наглядности можем рассмотреть функцию $x_1 + x_2 + x_3$ трех переменных, корреляционно-иммунную порядка 2. После подстановки переменных $x_1 := x_1$, $x_2 := x_2, x_3 := x_1 + x_3$ получаем функцию $x_2 + x_3$ двух переменных, а после подстановки переменных $x_1 := x_2, x_2 := x_1 + x_3, x_3 := x_2 + x_3$ — функцию x_2 одной переменной. В первом случае функция будет корреляционно-иммунной порядка 1, во втором случае функция будет не корреляционно-иммунной. Можем видеть также, что уже встречавшаяся сбалансированная функция $x_1x_2 + x_2x_1 + x_1x_3$, удовлетворяющая PC(2), после подстановки $x_1 := x_1 + x_2, x_2 := x_2, x_3 := x_2 + x_3$ принимает вид $x_2x_3 + x_1x_3$, удовлетворяет только PC(1) и не является сбалансированной.

Классы эквивалентности, полученные на основе полной аффинной группы преобразований, можно укрупнить, считая «одноклассниками» функции, отличающиеся аффинным слагаемым вида $\langle c, x\rangle \oplus \lambda$, как в (3). При этом как раз получатся классы аффинной эквивалентности, в [10] они обозначены как классы группы AGL$(n,2)U_1$. Число классов после этого станет значительно меньше. Например, при $n = 6$ укрупнённых классов будет около 70 тысяч против 15 768 919 исходных классов. (Всё-таки, конечно, и таких классов эквивалентности очень много, и их число быстро растёт с ростом n.) В [12] предлагается отдельно рассматривать классы группы AGL$(n,2)U_0$, когда объединяются функции, отличающиеся свободным членом. По аналогии с этими обозначениями P-аффинное преобразование (2) можно было бы обозначить PGL$(n,2)U_0$.

В работе [12] приведены для $n = 3$ и $n = 4$ количества классов P-эквивалентности, на которые разбивается BF_n по отношению, задаваемому формулой (2). При $n = 3$ таких классов имеется 14, при $n = 4$ их 222. Мощности классов сильно различаются. Так, для $n = 3$ имеются по два класса мощностей 2, 6, 8, 16, 48 и четыре класса мощности 24.

Как уже отмечалось, функции одного класса совпадают по исследуемым криптографическим показателям. Поэтому достаточно одного представителя класса для оценки всего класса с точки зрения его криптографической пригодности. Найдя функцию, интересную для криптографических приложений, мы получим сразу весь класс таких же полезных функций.

Задача выбора представителя класса, как и задача вообще классификации булевых функций и подсчёта количества и мощности классов, нетривиальна и имеет самостоятельный интерес. Рекомендации по решению таких задач можно найти в [10, 14, 15]. Для выявления возможной эквивалентности двух функций может быть использован алгоритм, приведенный в [16] (Algoritm 1).

5. ОБЩИЙ ПОДХОД К ЗАДАЧЕ ПОИСКА ФУНКЦИЙ С НАИЛУЧШИМИ ХАРАКТЕРИСТИКАМИ

Можно выделить следующие пути получения булевой функции, пригодной для криптографических целей:

– случайная генерация;
– алгебраическое конструирование;
– эвристики.

Случайной генерацией непросто получить хорошую функцию, так как из огромного числа булевых функций лишь очень немногие обладают требуемым набором свойств. В качестве эксперимента (см. [17]) был сгенерирован миллион сбалансированных функций шести переменных (всего таких функций примерно $1.8 \cdot 10^{18}$), и только 55 из них оказались корреляционно-иммунными. Напротив, алгебраические построения сразу обеспечивают определённые свойства функции. При этом обычно прибегают к рекурсии, конструируя функцию из функций меньших размерностей. Но такой подход заведомо значительно сужает множество возможных решений. Кроме того, алгебраически построенная функция может проявлять нестойкость относительно атак, не предусмотренных её построением.

Мы выделим подход, основанный на случайном и эвристическом поиске. Уже при $n = 6$ количество булевых функций n переменных огромно (см. выше). Естественно, к полному перебору таких функций с целью выявления криптографически сильных не прибегают. Вспомним, что криптографические характеристики булевых функций взаимозависимы и что часто оптимизация одних из них ухудшает другие. Поэтому широко используются те или иные методы поиска, не гарантирующие, например, максимальной нелинейности, но отыскивающие функции высокой нелинейности, удовлетворительные и по другим криптографическим характеристикам. Для сужения пространства поиска целесообразно использовать те или иные классы эквивалентности булевых функций.

У. Миллан, Д. Фуллер и Э. Даусон в работе [17] предлагают исследовать классы эквивалентности, используя понятие графа классов. У авторов это были классы аффинной эквивалентности. Вершины такого графа соответствовали классам эквивалентности. Две вершины A и B соединялись ребром, если в классах A, B имелась хотя бы одна пара $f \in A, g \in B$ такая, что расстояние Хэмминга между f и g равно 1. В работе [18] (раздел 2.5) специально подчеркивается, что для функций, входящих в один класс эквивалентности, множества соседних (отличающихся ровно одним битом вектора значений) функций совпадают. Совпадают и множества функций, отличающихся от того или иного представителя класса ровно m битами, $m > 1$.

Подобный граф можно построить и для определенных в разделе 4 классов P-эквивалентности. Если при этом мы решили ограничиться множеством сбалансированных функций, то построение графа классов несколько изменится. Две вершины A и B будут соединяться ребром, если в классах A, B найдётся хотя бы одна пара $f \in A, g \in B$, в которой вектор значений одной функции можно получить заменой в векторе значений другой функции одного нуля единицей и одной единицы нулём. Или, что то же самое, функция g получается из функции f транспозицией двух битов с разными значениями. Например, $f = 10101001$ и $g = 01101001$ принадлежат разным классам (достаточно заметить, что $N(f) = 2, N(g) = 0$). При этом вектор g получается из f, если инвертировать каждый из первых двух битов в f. Соответствующие вершины графа классов будут соединены ребром. Смежные вершины графа в этом случае будут находиться друг от друга на расстоянии Хэмминга, равном 2.

Такое представление классов эквивалентности удобно иметь в виду при построении полной классификации сбалансированных булевых функций. Оно позволяет передвигаться транспозициями от вершины к вершине графа, выделяя представителей классов и гарантируя, что пропущенных функций не будет. Как и все переборные алгоритмы, такой подход при больших n имеет ограничения по времени и памяти. В связи с этим данный подход можно рассматривать как инструмент при поиске криптографически сильных булевых функций, а сам поиск, как уже говорилось выше, предполагает использование эвристик.

В ходе исследований, посвящённых эвристическому поиску, выделились как подходящие для работы с булевыми функциями такие общие методы, как генетические алгоритмы (genetic algorithms), восхождение на холм (hill climbing), моделирование отжига (simulated annealing) и другие. Такие методы нахождения булевых функций с нужными свойствами разнообразно конкретизированы и реализованы во многих работах (см., например, [19–22]). В области эвристик появились и появляются плодотворные идеи и перспективные направления исследования, модифицируются уже имеющиеся методы. Работа [17] может быть рекомендована как вводная при первом знакомстве с данной тематикой. Помимо предложений о графическом описании классов эквивалентности, работа содержит также краткую обзорную часть с характеристиками нескольких эвристик с точки зрения их применения в рассматриваемой области.

Список литературы

1. *Carlet C.* Boolean functions for cryptography and error correcting codes // in: Boolean models and methods in mathematics, computer science and engineering. Y. Crama and P. L. Hammer (eds.). Cambridge University Press, 2010. P. 257–397.
2. *Pieprzyk J.* Möbius transforms, coincident Boolean functions and non-coincidence property of Boolean functions // International Journal of Computer Mathematics. 2011. № 7. P. 1398–1416.
3. *Агафонова И.В., Дмитриева О.М.* Методы построения полиномов Жегалкина для булевых функций // Материалы III Международной научно-технической и научно-методической конференции «Актуальные проблемы инфотелекоммуникаций в науке и образовании», 25–26 февраля 2014 г.). СПб.: Санкт-Петерб. гос. университет им. проф. М.А.Бонч-Бруевича, 2014. С. 525–530.
4. *Логачев О.А., Сальников А.А., Ященко В.В.* Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
5. *Таранников Ю.В.* О корреляционно-иммунных и устойчивых булевых функциях // Математические вопросы кибернетики. М.: Физматлит, 2002. Вып. 11. С. 91–148.
6. *Агафонова И.В.* Криптографические свойства нелинейных булевых функций // В сб.: Избранные главы дискретного гармонического анализа и геометрического моделирования. Часть I. Издание 2-е. Под ред. проф. В.Н. Малозёмова. СПб.: ВВМ, 2014. С. 428–451.
7. *Городилова А.А.* От криптоанализа шифра к криптографическому свойству булевой функции // Прикладная дискретная математика. 2016. № 3. С. 16–44.
8. *Cusick T.W., and Stanica P.* Cryptographic Boolean functions and applications. Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sidney, Tokio: Academic Press, 2009.
9. *Braeken A., Borissov Y., Nikova S., and Preneel B.* Classification on Boolean functions of 6 variables or less with respect to some cryptographic properties // In Proc. 32nd Int. Colloq. Automata, Lang. Program. 2005. P. 324–334.
10. *Фомичев В.М.* Дискретная математика и криптология. Курс лекций / Под общ. ред. д-ра физ.-мат. н. Н.Д. Подуфалова. М.: ДИАЛОГ-МИФИ, 2003.

11. *Токарева Н.Н.* Симметричная криптография. Краткий курс: учебное пособие. Новосибирск.: Новосиб. гос. ун-т., 2012.
12. *Черёмушкин А.В.* Методы аффинной и линейной классификации двоичных функций // В сб.: Российская Академия наук. Академия криптографии Российской Федерации. Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
13. *Lechner R.J.* A transform approach to logic design // IEEE Trans. on Computers. Jul. 1970. Vol. C-19. № 7. P. 627–640.
14. *Millan W.* New cryptographic applications of Boolean function equivalence classes // in ACISP. 2005. LNCS 3574. Brisbane. Australia. 2005. P. 572–583.
15. *Zhang Y., Yang G., Hung W.N.N., and Zhang J.* Computing Affine Equivalence Classes of Boolean functions by group isomorphism // IEEE Trans. on Computers. Dec. 2016. Vol. 65. № 7. P. 3606–3616.
16. *Meng Q., Zhang G., Yang M., and Wang Z.* Analysis of affinely equivalent Boolean functions // Sci China Ser F-Inf Sci. June 2007. Vol. 50. № 3. P. 299–306.
17. *Millan W., Fuller J., and E. Dawson E.* New concepts in evolutionary search for Boolean functions in cryptology // In Proc. of CEC 2003. IEEE. 2003. P. 2157–2164.
18. *Fuller J.* Analysis of affine equivalent Boolean functions for cryptography. PhD thesis. Queensland University of Technology. Brisbane. Australia. 2003.
19. *Burnett L., Millan W., Dawson E., and Clark A.* Simpler methods for generating better Boolean functions with good cryptographic properties // Australasian Journal of Combinatorics. 2004. Vol. 29. P. 231–247.
20. *Picek S., Jakobovic D., Miller J.F., Marchiori E., and Batina L.* Evolutionary methods for the construction of cryptographic Boolean functions // In Proc. EuroGP 2015. LNCS 9025. P. Machado, MI. Heywood, J. McDermott, M. Castelli, P. Garcia-Sanchez, P. Burelli, S. Risi, K. Sim (eds.) Switzerland: Springer, 2015. P. 192–204.
21. *Izbenko Y., Kovtun V., and Kuznetsov A.* The design of Boolean functions by modified hill climbing method // Cryptology ePrint Archive. Report 2008/111. 2008.
22. *McLaughlin J., Clark J.A.* Evolving balanced Boolean functions with optimal resistance to algebraic and fast algebraic attacks, maximal algebraic degree, and very high nonlinearity // Cryptology ePrint Archive. Report 2013/011. 2013.

Поступила в редакцию 24.04.2017, окончательный вариант — 08.06.2017.

Computer tools in education, 2017

№ 3: 20–28

http://ipo.spb.ru/journal

BOUNDED SEARCH OF CRYPTOGRAPHICALLY STRONG BOOLEAN FUNCTIONS

Agafonova I.V. [1], Dmitrieva O.M.[2]

[1]SPbSU, Saint-Petersburg, Russia

[2]SPbSUT, Saint-Petersburg, Russia

Abstract

In this paper we consider methods for obtaining Boolean functions with desirable cryptographic properties based on search algorithms. We investigate the possibility of optimizing such algorithms, primarily due to a significant reduction in the search space. Here we use the general idea of partition of the set of Boolean functions into equivalence classes in accordance to some transformation group and the idea of exhaustive search among these classes as vertices of a specific graph called class graph.

The P-equivalence proposed in this paper if considered on the set of balanced Boolean functions ensures the preservation of almost all cryptographically significant properties of functions within one equivalence class.

Keywords: *Boolean functions, cryptographic properties, affine equivalence.*

Citation: : I.V. Agafonova & O.M. Dmitrieva, "Ogranichennyi poisk kriptograficheski sil'nykh bulevykh funktsii" [Bounded Search of Cryptographically Strong Boolean Functions], *Computer tools in education*, no. 3, pp. 20–28, 2017 (in Russian).

Received 24.04.2017, the final version — 08.06.2017.

Irina V. Agafonova, Associate Professor, Saint-Petersburg University, Faculty of Mathematics and Mechanics, Department of Operations Research, i.agafonofa@spbu.ru

Oksana M. Dmitrieva, Associate Professor, Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Faculty of Fundamental Training, Department of Higher Mathematics; 193232 Saint-Petersburg, Bolshevikov pr., 22, bldg. 1, dmitrieva-oksana@bk.ru

Агафонова Ирина Витальевна,
кандидат физико-математических наук, доцент кафедры исследования операций математико-механического факультета СПбГУ,
i.agafonofa@spbu.ru

Дмитриева Оксана Михайловна,
кандидат физико-математических наук, доцент кафедры высшей математики, Санкт-Петербургского государственного университета телекоммуникаций;
193232, Санкт-Петербург, пр. Большевиков, д. 22, корп. 1,
dmitrieva-oksana@bk.ru