УДК 004.056

Марковский А.П.,
Искаков Эмиль Русланович.,
Гарасимович Г.В.

КОМБИНАТОРНЫЙ АНАЛИЗБУЛЕВЫХ ФУНКЦИЙ, СПЕЦИАЛЬНЫХ КЛАССОВ ДЛЯ СИСТЕМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В статье предложен новый метод построения булевых балансных функций, которые соответствуют критерию строго лавинного эффекта. Преимуществом предложенного метода является простота реализации и существенно большее по сравнению с известными методами количество функций этого класса, которые могут быть синтезированы. Подробно описана формализованная процедура конструирования балансных функций, обладающих строгим лавинным эффектом. Определена нелинейность синтезируемых функций. Приведен пример синтеза функции.

Ключевые слова: криптографические алгоритмы, булевы функции, балансные функции, функции, обладающие лавинным эффектом.

In this paper new method for designing of Boolean balanced function that satisfies the Strict Avalanche Criterion (SAC) are presented.The advantage of the suggested method is the simplicity of realization and the significant greatest number of the generated functions compared to the known methods. The formalized procedure for construction balanced SAC-functions is described in detail. The nonlinearity of synthesized functions have been determined. Examples of function design are given.

Key-words: Cryptographic algorithms, Boolean functions, balance functions, SAC functions.

Актуальность темы исследования. Развитие распределенных систем в значительной мере зависит от уровня технологии защиты в них информации. В настоящее время в основе большинства систем защиты информации лежат криптографические механизмы, базирующиеся на аналитически неразрешимых математических задачах теории чисел, эллиптических кривых и булевых функций. Использование последних играет особенно важную роль, поскольку вычисление булевых преобразований выполняется на 3-4 порядка быстрее по сравнению со сложными мультипликативными операциями модулярной арифметики, выполняемыми над числами, длина которых на порядок превышает разрядность процессоров.

Исходя из этого развитие теории булевых функций применительно к их криптографическим применениям, а также совершенствование на этой основе технологических аспектов построения на основе таких функций алгоритмов и протоколов защиты информации является важной и актуальной задачей для современного этапа развития информационных и компьютерных технологий.

Постановка проблемы. Булевы функции, используемые в системах защиты информации должны обладать рядом специфических свойств, важнейшим из которых является свойство строгого лавинного эффекта (SAC-StrictAvalancheCriterion), которое характеризуется максимальным значением дифференциальной энтропии, что

обеспечивает устойчивость к нарушению защиты дифференциальным криптоанализом [1,2]. Помимо этого, булевы функции должны обладать высоко нелинейностью с тем, чтобы успешно противостоять линейному криптоанализу [3].

Для практического использования булевых балансных функций, которые удовлетворяют критерию строгого лавинного эффекта, стоит задача разработки формализованных методов их синтеза. Это позволит существенно повысить эффективность использования булевых функций специальных классов для многих применений.

Анализ известных исследований и публикаций. Быстрый прогресс интегральной технологии позволяет создавать эффективные аппаратные реализации таких реконфигурируемых функций с использованием матриц программируемых элементов.

Булева функция $f(x_1,x_2,\ldots,x_n)$, определенная на множестве Z состоящем из 2^n возможных значений наборов X из n переменных называется балансной, если она с равной вероятностью принимает нулевые и единичные значения:

$$\sum_{X \in Z} f(X) = 2^{n-1}$$

Булева функция $f(x_1,x_2,\ldots,x_n)$, удовлетворяет критерию строгого лавинного эффекта, если при изменении значения любой из n переменных значение функции меняется с вероятностью 0.5:

$$\begin{gathered}\sum_{X \in Z} f(X) \oplus f(X \oplus \Delta_j) = 2^{n-1}, \forall j \in \{1,\ldots, n\}, \\ \Delta_j = (d_1,\ldots, d_j,\ldots, d_n), d_j = 1, d_i = 0, \forall i \in \{1,\ldots, n\}, i \neq j,\end{gathered} \quad (1)$$

где Δ_j- n-компонентный двоичный вектор, j-тая компонента которого равна единице, а остальные – нулю. Любая булева функция $f(x_1,x_2,\ldots,x_n)$, может быть представлена в виде канонического разложения Шеннона по j–той переменной x_j:

$$f(x_1,x_2,\ldots,x_n) = x_j \cdot \varphi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n) \oplus \psi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$$

где φ_j и ψ_j – булевы функции, не зависящие от x_j. Поскольку $f(X) \oplus f(X \oplus \Delta_j) = \varphi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$, то булева функция $f(x_1,x_2,\ldots,x_n)$, удовлетворяет критерию строго лавинного эффекта, если при любом $j \in \{1,\ldots,n\}$ функции $\varphi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$ балансны, то есть $\sum_{X \in Z} \varphi_j(X) = 2^{n-1}, \forall j \in \{1,\ldots,n\}$. Поскольку функция $\varphi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$ не зависит от x_j, ее можно рассматривать как функцию от n-1 переменных, для которых существует 2^{n-1} возможных наборов X_j переменных $x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n$, образующих множество Z_j. Тогда условие соответствия функции $f(x_1,x_2,\ldots,x_n)$, критерию строгого лавинного эффекта может быть приведено к виду:

$$\sum_{X_j \in Z_j} \varphi_j(X_j) = 2^{n-2}, \forall j \in \{1,\ldots, n\}. \quad (2)$$

Функция $\varphi_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n)$ отождествляется рядом исследователей [3] с дифференциалом булевой функции $f(x_1,x_2,\ldots,x_n)$ по переменной x_j:

$$\frac{\partial f(x_1,\ldots, x_j,\ldots, x_n)}{\partial x_j} = \varphi_j(x_1,\ldots, x_{j-1}, x_{j+1},\ldots, x_n). \quad (3)$$

Соответственно, булева функция $f(x_1,x_2,\ldots,x_n)$ удовлетворяет SAC, если ее дифференциалы по всем переменным балансны.

Принимая во внимание практическую важность проблемы автоматизированного синтеза балансных SAC–функций для современных средств защиты информации, за последние 15 лет предложен ряд подходов по решению этой проблемы [1-3].

С начала 90-х годов опубликовано большое число работ, посвященных синтезу булевых функций специальных классов, ориентированных для использования в системах кодирования и защиты информации. Методы, синтеза SAC-функций можно условно разделить на три группы:

- генетические;
- на основе ортогонального базиса;
- комбинаторные.

Генетические методы синтеза булевых функций специальных классов, основаны на том, что каким-то образом получается одна функция класса, а потом из нее путем специальных математических преобразований формируется множество функций, обладающих такими же свойствами. Для практической реализации этого подхода чаще всего используются спектральные преобразования [1,4]. Общим недостатком генетических методов синтеза булевых SAC-функций с является то, что проблема получения первичной булевой функции этого класса остается открытой.

Другим, часто используемым на практике подходом к получению SAC-функций является использование свойств ортогональных систем булевых функций и преобразований над нами. В рамках этого подхода разработано большинство существующих на сегодняшний день методов синтеза балансных SAC–функций [3,4]. Наиболее известный метод получения балансовых SAC-функций на основе ортогональных преобразований предложен в работе [5]. Сущность предложенного ими метода состоит в том, что $_n$ переменных разделяются на два непересекающегося множества, с s и t переменных ($n=s+t$), дальше формируются линейная функция $g(x_1,...,x_s)$ от s переменных и бинарная матрица Q , размерностью $s \times t$, причем число единичных компонентов произведения $\mathrm{Q} \cdot \gamma_1$ матрицы Q на любой $_s$-компонентный вектор γ_1 с одним ненулевым компонентом и произведения $\gamma_2 \cdot Q$ любого t-компонентного вектора γ_2 с одним ненулевым компонентом больше или равно единице. Вектор образован коэффициентами функции $g(x_1,...,x_s)$ может быть линейно-независимой от векторов, образованных столбцами матрицы Q . Балансная SAC-функция формируется согласно формуле:

$$f(x_1,...,x_n)=[x_1,...,x_s]\cdot Q\cdot[x_{s+1},...,x_n]^T \oplus g(x_1,...,x_s)$$

Недостатками этого метода является сложность получения матрицы Q при достаточно больших значениях *n*.

Выделение неисследованных частей общей проблемы.Общим недостатком существующих методов синтеза булевых функций на является принципиально малое число SAC-функций. Основным их недостатком является то, что они позволяют получать относительно небольшое подмножество SAC-функций.

К настоящему времени не существует аналитического выражения для исчисления количества булевых SAC-функций от n переменных.

Постановка задачи.Целью исследований является повышение эффективности синтеза булевых функций, обладающих высокой нелинейностью и свойством лавинного эффекта за счет увеличения количества таких функций.

Комбинаторный анализ булевых функций специальных классов. Для решения задачи синтеза SAC-функций и оценки их количества предлагается использовать комбинаторный подход. Его сущность состоит в установлении комбинаторных зависимостей между значениями SAC-функций на различных наборах и использования этих зависимостей для синтеза функций и определения их количества.

Показано, что для того, чтобы булева функция $f(x_1,x_2,\ldots,x_n)$ была балансной и удовлетворяла SAC по переменной x_i, необходимо, чтобы на половине (2^{n-2}) 2^{n-1} возможных значений остальных n-1 переменных, функция при изменении x_i меняла свое значение на противоположное, на одной четвертой (2^{n-3}) пар наборов принимала строго единичное значение и на оставшихся (2^{n-3}) наборах принимала нулевое значение. Число вариантов размещения значений функций в таблице истинности, удовлетворяющее этим условиям определяет число KSAC-функций:

$$K = C_{2^{n-1}}^{2^{n-2}} \cdot C_{2^{n-2}}^{2^{n-3}} \cdot 2^{n-2} \approx \frac{2^{3\cdot n+2.5}}{\pi}. \quad (4)$$

В частности. при n=4 количество SAC-функций согласно формуле (4) составляет 1680 (или 26%) из общего числа 6435 балансных булевых функций от 4-х переменных. Для n=8 количество SAC-функций согласно формуле (4) составляет уже $3\cdot10^{7}$ (или $5\cdot10^{-65}$ %) из общего числа $5.8\cdot10^{75}$ балансных булевых функций от 8-х переменных. Из приведенных в качестве примера данных, а частности, следует, что поиск имеющих практическое значение SAC-функций от большого числа переменных, представляет собой сложную задачу.

Комбинаторные свойства SAC-функций могут быть использованы и для задач синтеза. Так, доказано, что можно определить базовые фрагменты таблицы истинности и правила складывания их них таблицы истинности SAC-функций. Например, можно определить набор фрагментов E={1000,0100,0010,0001} и набор их инверсий: N={0111,1011,1101,1110} и показать, что в таблице истинности SAC-функции число фрагментов множеств E и N должно быть одинаково, а номера фрагментов в симметричных участках таблицы истинности должны быть различными. Используя эти зависимости можно построить достаточно просто комбинаторно построить таблицы истинности SAC-функций.

Предложенный подход не только может быть использован как для задач практического синтеза криптографически устойчивых булевых преобразований, но и имеет значение для задач теории булевых функций.

Выводы. Предложенный метод является развитием подхода к синтезу балансных булевых функций, удовлетворяющих критерию строго лавинного эффекта на основе исследованных комбинаторных свойств булевых функций, удовлетворяющих критерию строго лавинного эффекта. Главной особенностью разработанного метода является то, что он может использоваться как для синтеза фиксированных балансных SAC-функций, так и для построения управляемого кодом генераторов таких функций. При синтезе фиксированных SAC-функций,

предложенный метод отличается от известных простотой и высокой технологичностью, поскольку не использует представления синтезируемых функций в виде таблицы истинности. Разработанный метод практически реализует построение функций со специфическими свойствами от *n* переменных на основе подмножества функций указанного класса от *n*/2 переменных. Благодаря использованию комбинаторных свойств функций, удовлетворяющих лавинному эффекту обеспечивается возможность построения большего числа SAC-функций по сравнению с известными методами.

Разработанный метод ориентирован на использование в перспективных алгоритмах защиты информации на основе булевых преобразований: алгоритмах симметричного шифрования, потоковых алгоритмах шифрования и хеш-алгоритмах.

Список использованных источников :

1. Forre R. The strict avalanche criterion: spectral properties of Boolean functions and extend definition. / R. Forre // Advanced in Cryptology – Crypto'88 Proceeding, Lecture Notes in Computer Sciences, 403 – 1990-P.450-468.

2. Самофалов К.Г. Комбинаторный подход к получению булевых функций, обладающих строгим лавинным эффектом. К.Г. / Самофалов, А.П. Марковский // Электронное моделирование.- 2004,- Том. 26, - № 3, - с.27-40.

3. Tang D. Highly Nonlinear Booleam Function with optimal algebraic immunity and good behavior against fast algebraic attack / D. Tang, C. Carlrt, X. Tang. // IEEE Transactions on Information theory.-Vol.59.- No. 1.- 2013.- P.653-664.

4. Gao G/ Recent recent result of balanced symmetric Boolean functions / G. Gao, Y. Zhao. // IEEE Transactions on Information theory.-Vol. 62.- No.9.- 2016.- P.5199-5203.

ДОВІДКА ПРО АВТОРІВ

Марковський Олександр Петрович – кандидат технічних наук, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»

Oleksandr Markovskyi – Associate Professor, *PhD,* Department of Computer Engineering, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute"

Марковский А. П.,
Искаков Эмиль Русланович.,
Гарасимович Г. В.

КОМБИНАТОРНЫЙ АНАЛИЗ БУЛЕВЫХ ФУНКЦИЙ, СПЕЦИАЛЬНЫХ КЛАССОВ ДЛЯ СИСТЕМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Актуальність теми дослідження. Виходячи з розвитку теорії булевих функцій стосовно їх криптографічним застосуванням, а також вдосконалення на цій основі технологічних аспектів побудови на основі таких функцій алгоритмів і протоколів захисту інформації є важливим і актуальним завданням для сучасного етапу розвитку інформаційних і комп'ютерних технологій

Постановка проблеми.Для практичного використання булевих балансних функцій, які відповідають критеріям суворого лавинного ефекту, стоїть завдання розробки формалізованих методів їх синтезу. Це дозволить істотно підвищити ефективність використання булевих функцій спеціальних класів для багатьох застосувань.

Аналіз останніх досліджень і публікацій. Швидкий прогрес інтегральної технології дозволяє створювати ефективні апаратні реалізації таких реконфігурованих функцій з використанням матриць програмованих елементів. Беручи до уваги практичну важливість проблеми автоматизованого синтезу балансних SAC-функцій для сучасних засобів захисту інформації, за останні 15 років запропонований ряд підходів щодо вирішення цієї проблеми

Виділення недосліджених частин загальної проблеми. Загальним недоліком існуючих методів синтезу булевих функцій на є принципово мале число SAC-функцій. Основним їх недоліком є те, що вони дозволяють отримувати відносно невелика підмножина SAC-функцій. До теперішнього часу не існує аналітичного виразу для обчислення кількості булевих SAC-функцій від n змінних.

Постановка завдання. Метою досліджень є підвищення ефективності синтезу булевих функцій, що володіють високою нелінійністю і властивістю лавинного ефекту за рахунок збільшення кількості таких функцій.

Викладення основного матеріалу. Для вирішення завдання синтезу SAC-функцій і оцінки їх кількості пропонується використовувати комбінаторний підхід. З наведених як приклад даних, а зокрема, випливає, що пошук мають практичне значення SAC-функцій від великого числа змінних, являє собою складну задачу.

Висновки. Запропонований метод є розвитком підходу до синтезу балансних булевих функцій, що задовольняють критерію строго лавинного ефекту на основі досліджених комбінаторних властивостей булевих функцій, що задовольняють критерію строго лавинного ефекту. Головною особливістю розробленого методу є те, що він може використовуватися як для синтезу фіксованих балансних SAC-функцій, так і для побудови керованого кодом генераторів таких функцій.

Ключові слова. Криптографічні алгоритми, булеві функції, балансні функції, функції, що володіють лавинним ефектом.