ФІЗИКО-МАТЕМАТИЧНІ НАУКИ

Билашевская А.В.
студентка;
Шани Хайдер Талиб Шани
магистр,
Национальный технический университет Украины
«Киевский политехнический інститут»

КОМБИНАТОРНЫЙ АНАЛИЗ БУЛЕВЫХ ФУНКЦИЙ, ОБЛАДАЮЩИХ ЛАВИННЫМ ЭФФЕКТОМ ДЛЯ СИСТЕМ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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. Булевы функции, используемые в системах защиты информации должны обладать рядом специфических свойств, важнейшим из которых является свойство строгого лавинного эффекта (SAC-Strict Avalanche Criterion), которое характеризуется максимальным значением дифференциальной энтропии, что обеспечивает устойчивость к нарушению защиты дифференциальным и линейным криптоанализом [1; 2].

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. В частности, это даст существенно уменьшить негативное влияние группировки записей в хеш-памяти за счет использования единого перестраиваемого механизма первичной и вторичной хеш-адресации.

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:

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

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]. 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.

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 K SAC-функций:

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

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.

Список использованных источников:

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

2. Самофалов К. Г., Марковский А. П. Комбинаторный подход к получению булевых функций, обладающих строгим лавинным эффектом // 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 / Carlrt C., Tang X. // IEEE Transactions on Information theory. – Vol. 59. – № 1. – 2013. – P. 653-664.