ОЦЕНКА ЭФФЕКТИВНОСТИ ГЕНЕРАЦИИ КРИПТОГРАФИЧЕСКИ ОРИЕНТИРОВАННЫХ БУЛЕВЫХ ФУНКЦИЙ НА ОСНОВЕ КВАЗИГРУПП

Е.Ц. АЛАВЕРДЯН

В традиционных системах шифрования, переводящих открытый текст в зашифрованное сообщение с помощью секретного ключа, решающую роль играет аппарат Булевых функций. К этим функциям предъявляется ряд требований, имеющих целью предельно осложнить дешифровку сообщения лицом, не являющимся его адресатом.

Криптографические свойства Булевых функций успешно применяются в частности при построении блоков подстановок, обеспечивающих случайное и нелинейное распределение исходных сообщений по пространству зашифрованных сообщений. Широкое применение Булевых функций в криптосистемах обусловлено легкостью и эффективностью их реализации.

Криптографические трансформации называются “стойкими”, если они соответствуют некоторым критериям: *конфузии* и *диффузии*, впервые представленных Шенноном [1]. Конфузия - метод, при котором зависимость ключа и выходных данных делается как можно более сложной, в частности, нелинейной. Как правило, конфузия реализуется применением блоков подстановок. Диффузия – метод, при котором изменение в статистике входных данных распределяется по всей структуре выходных данных, указывая на статистическую зависимость между открытым текстом и криптотекстом. Диффузия, как правило, реализуется применением блоков перестановок.

Для установления вышеуказанных критериев, криптографические трансформации должны обладать некоторыми характеристиками, среди которых *нелинейность*

– самое важное свойство [2]. Вспомним, что нелинейные преобразования, усложняющие обратимость применяемых операций, в большинстве случаев осуществляются применением Булевых функций. Наиболее общепринятое определение нелинейности Булевой функции – это степень ее логического расстояния от множества линейных функций.

Другой критерий, выдвинутый Фейстелом [3], касается *лавинного* свойства Булевой функции, когда выходные значения Булевой функции меняются с вероятностью 0.5 при изменении одного бита ее входных значений.

В отличие от классических криптографических алгоритмов, симметричных или асимметричных, преобразовавших открытый текст в шифрованный, в случае применения Булевых функций добавляется еще одно качество: *сбалансированность* Булевой функции. Аналогично, Булева функция – *сбаланасированная*, если ее таблица истинности содержит одинаковое количество единиц и нулей, т.е. $wt(f) = 2^{n-1}$, где wt означает вес Хемминга вектора выходных значений функции.

Чем меньше Булева функция близка своей конструкцией к аффинной или линейной, тем ее криптографические свойства - стойкие. В это неформальное пожелание можно вложить различные смысловые оттенки. Вот некоторые из них:

- “Функция с хорошей нелинейностью” далека от множества аффинных функций в смысле какой-либо метрики.
- “Функция с хорошей нелинейностью” не должна линейно зависеть ни от одной из своих переменных и не должна приобретать такую зависимость после какой-либо линейной замены переменной, т.е. функция не должна иметь ненулевых линейных структур.

- “Функция с хорошей нелинейностью” должна выражаться полиномом Жегалкина как можно более высокой степени.

Отметим, что полином Жегалкина явно указывает на алгебраическую степень данной Булевой функции.

Пусть R обозначает поле реальных чисел. Тогда для $\alpha \in F_2^n$ и каждой Булевой функции $f(x)$ над F_2^n имеется функция $W_f: F_2^n \to R$, определяемая преобразованием Уолша:

$$W_f(\alpha) = \sum_x (-1)^{f(x)+\alpha \cdot x}.$$

Обратное этого преобразования вычисляется следующим образом:

$$(-1)^{f(x)} = \frac{1}{2^n} \sum_\alpha W_f(\alpha)(-1)^{\alpha \cdot x}.$$

В таком случае имеем:

$$(W_f(\alpha_0), \ldots, W_f(\alpha_{2^n-1}))^t = H_n \cdot ((-1)^{f(\alpha_0)}, \ldots, (-1)^{f(\alpha_{2^n-1})})^t,$$

где H_n представляет собой матрицу Силвестера – Адамара порядка n, определенная следующим образом:

$$H_1 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \text{ а } H_n = \bigotimes^n H_1.$$

Упорядоченный одномерный массив значений Уолша Булевой функции называется *спектром Уолша* функции f. Заметим, что спектр Уолша включает целые числа в диапазоне $[-2^n; 2^n]$. Преобразование Уолша-Адамара представляет собой меру криптографической защищенности поточных и блочных шифров.

Сложность вычисления алгебраической нормальной формы, а также преобразование Уолша Булевой функции – порядка $O(2^{2n})$. Аналогичную сложность имеет обратное преобразование Уолша. Однако возможно достичь уменьше-

ния количества операций посредством факторизации H_n из обратной структуры, уменьшая сложность обратного преобразования до степени сложности $O(n2^n)$.

Рассмотрим A_n, обозначающей множество аффинных Булевых функций над F_2^n. Тогда, нелинейность Булевой функции над F_2^n определяется логическим расстоянием функции f от функций семейства A_n[4].

Высокая степень нелинейности Булевой функции – существенное свойство в проектировании стойкого криптографического алгоритма. Степень нелинейности Булевой функции определяет меру сложности построения ее аффинной аппроксимации, а последняя, в свою очередь, обуславливает стойкость криптографического алгоритма по отношению *к линейному криптоанализу* [5].

Итак, для оценки степени нелинейности Булевой функции используется спектр Уолша. Значения Уолша Булевой функции f представляют собой разницу между $w(f \oplus \varphi_i)$ и $w(f \oplus \varphi_i \oplus 1)$, где φ_i представляет собой линейную функцию $\varphi_i = a_i \cdot x$. Из этого следует, что $(-1)^{f(x)} = 1 - 2f(x)$, так как f принимает значения из $\{0,1\}$.

Спектр Уолша Булевой функции f вычисляется следующим образом:

$$W_f(\alpha) = \sum_x (-1)^{f(x)+\alpha\cdot x} = 2^n - 2\sum_x (f(x) + \alpha \cdot x)$$
$$= 2^n - 2H_d(f, \alpha \cdot x),$$

где $H_d(f, \alpha \cdot x)$ - расстояние Хемминга между функциями f и $\alpha \cdot x$.

Приведем другое определение нелинейности Булевой функции, основываясь на вышеприведенные преобразования. Заметим, что спектр Уолша линейной Булевой функции $f(x) = \beta \cdot x$ имеет вид

$$W_f(\alpha) = \sum_x (-1)^{(\beta+\alpha)\cdot x} = 2^n \delta_\alpha(\beta),$$

где $\delta_\alpha(\beta)$ функция Дирака, определяемая как

$$\delta_\alpha(\beta) = \begin{cases} 1, \text{если } \beta = \alpha \\ 0, \text{если } \beta \neq \alpha \end{cases}.$$

Отсюда следует, что для линейной функции $max_{\alpha \in F_2^n} \left| W_f(\alpha) \right| = 2^n$. Учитывая это обстоятельство, мерой нелинейности Булевой функции, определенной над F_2^n, считается величина

$$N_f = 2^{n-1} - \frac{1}{2} max_{a \in F_2^n} |W_f(a)|,$$

имеющая нулевое значение для произвольной линейной функции.

Генерация и тестирование требуемой коллекции сбалансированных Булевых функций высокой алгебраической степени, следовательно и высокого уровня нелинейности-трудоемкая процедура.

С целью упрощения данной процедуры, воспользуемся аппаратом так называемой “неассоциативной алгебры”, также позволяющей спроектировать стойкие к обращениям алгебраические структуры. Заметим, что сохранение при этом сочетания криптографических свойств Булевых функций, а именно, нелинейность, сбалансированность и устойчивость к корреляциям, также остается актуальным. Под неассоциативной алгеброй подразумевается векторное пространство над полем, определяющем операцию умножения, взаимодействующая с операцией сложения посредством обыкновенного закона дистрибутивности. Операция умножения, при этом, не обязательно коммутативна или ассоциативна.

Например, квазигруппы, в отличие от конечных групп, не обладают свойством ассоциативности, а также не имеют нейтрального элемента. Другое, и самое важное, свойство квазигрупп – это равномерное распределение их всевозможных элементов. Заметим, что тестирование свойств квазигрупп большого порядка – не тривиальная задача, так как до сих пор не было создано ни одного эффективного метода для такого анализа. Шифрование/дешифрование открытого текста с применением квазигруппы похоже на алгоритм Фейстеля в

том смысле, что текущее преобразование блока открытого текста (битовой строки символа) включает результат предыдущего раунда, обеспечивая последовательный процесс трансформаций. Вспомним, что последовательный тип процессов шифрования/дешифрования – отличное качество эксплуатирующей их криптосистемы, так как атака на основе вычисления открытого ключа из секретного становится настоящей головоломкой в том смысле, что открытый ключ используется только один раз во всем процессе шифрования/дешифрования и то лишь для обработки первого символа, а результат очередной обработки становится следующим, т.е. текущим ключом шифрования/дешифрования.

Учитывая вышеприведенные характеристики квазигрупп, рассмотрим возможность построения криптографически стойких Булевых функций на их основе. Последнее предоставит возможность представления квазигрупп посредством Булевых функций, заменяя при этом сложные абстрактные структуры гибким аппаратом дискретной математики, предлагающим широкий ряд классических методов обработки и оценки результирующих структур.

С этой целью определим квазигруппу $(Q,\cdot)$ конечного порядка, равной 2^d. Используя операцию $*$, возможно задание Булевой функции векторного значения(б. ф. в. з):

$a * b = c \iff *_{vv}(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_d) = (z_1, z_2, \ldots, z_d)$,

где $(x_1 \ldots x_d, y_1 \ldots y_d, z_1 \ldots z_d)$ представляют собой двоичное представление символов данного алфавита, a, b, c.

Каждый элемент z_i зависит от битов $x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_d$ и однозначно определяется ими. Таким образом, каждый z_i можно интерпретировать как Булеву функцию типа $2d$, уже не линейную, $z_i = f_i(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_d)$, где f_i: $\{0,1\}^{2d} \to 0,1\}$ представляет собой отображение однозначно определенное посредством $*$.

Итак, для каждой квазигруппы $(Q,*)$ порядка 2^d и каждой биекции $Q \longrightarrow \{0,1,\ldots,2^d-1\}$ существуют однозначно определенная $*$ б.ф.в.з и однозначно определенные Булевы функции $f_1, f_2, \ldots, f_d$ типа 2^d таким образом, что для каждой $a,b,c \in Q$ имеют место следующие соотношения:

$$a * b = c \Leftrightarrow *_{vv} (x_1,\ldots,x_d,y_1,\ldots,y_d)$$
$$= \big(f_1(x_1,\ldots,x_d,y_1,\ldots,y_d),\ldots,f_d(x_1,\ldots,x_d,y_1,\ldots,y_d)\big).$$

В свою очередь, каждая k - значная Булева функция $f(x_1,\ldots,x_k)$ может быть однозначно представлена суммой произведений в алгебраической нормальной форме, АНФ, с коэффициентами $\alpha_0, \alpha_i, \alpha_{i,j}, \ldots, \in \{0,1\}$, применяющими сложение и умножение над полем $GF(2)$.

Очевидно, что АНФ Булевых функций f_i описывает сложность квазигруппы $(Q,*)$ посредством алгебраической степени этих функций. Степени полиномов АНФ(f_i) увеличиваются в зависимости от порядка квазигруппы. В общем случае, для произвольно сгенерированной квазигруппы порядка 2^d, где $d \geq 4$, алгебраическая степень Булевой функции больше двух, что создает предпосылки для построения Булевых структур с высоким порядком нелинейности.

Соответствующее представление операции * в виде таблицы истинности трех Булевых функций производится в следующем порядке:

- количество входных параметров результирующих Булевых функций определяется сразу, умножая количество строк (или столбцов, так как математическая модель квазигруппы – это квадратная матрица соответсвующего порядка)
- наборы входных параметров в таблице истинности заполняются для каждой строки и столбца, а выходные значения функции заполняются согласно пересечению индексов строк и столбцов.

Булевой функции над 6-ю входными переменными с алгебраической степенью равной двум, нелинейность – порядка 24. Это означает, что из $2^6 = 64$ битов в коллекции выходных значений Булевой функции 24 должны меняться для того чтобы превратить эту функцию в ближайшую аффинную. Количество проб при этом равно $\binom{64}{24}$.

Очевидно, что повышение порядка квазигруппы приводит к повышению алгебраической степени и степени нелинейности Булевой функции, спроектированной на ее основе.

Заметим, что количество квазигрупп порядка $2^n, n \geq 3$ уже достаточно большое число. Для $n = 3$ это число приблизительно равно 2^{66}. Обращение таких структур без знания соответствующей ключевой информации – NP полная задача.

Сгенерировав квазигруппу порядка 2^{n}, мы наследуем сразу n количество сбалансированных Булевых функций желаемого порядка, ускоряя при этом процесс генерации этих функций. Заметим, что коллекция Булевых функций, полученные на основе данной квазигруппы коллизии не подлежит согласно определению квазигруппы. Генерация коллекции m количества нелинейных сбалансированных Булевой функций с применением квазигруппы позволяет упростить задачу на $2^{2\mathrm{n}}/\mathrm{n}^2 - \binom{\mathrm{m}}{2}$ - $2^{\frac{\mathrm{n}}{2}-1}$ порядка, где $2^{2\mathrm{n}}$ представляет сложность генерации требуемого класса Булевых функций над n переменными, $\binom{\mathrm{m}}{2}$ представляет количество проверки совпадений сгенерированных функций, $2^{\frac{\mathrm{n}}{2}-1}$ - количество битов, которые должны меняться в значениях Булевых функций для ее сбалансирования.

Итак, исследована возможность построения сбалансированных Булевых функций с нелинейностью высокого порядка с применением квазигрупп с целью ускорения процесса генерации коллекции криптографически ориентированных Булевых функций.

Ключевые слова: *криптосистема, Булева функция, квазигруппа, нелинейность, сбалансированность*.

ЛИТЕРАТУРА

1. C. E. Shannon. “Communication theory of secrecy systems”. Bell System Technical Journal 28 (1949), pp 656–715.
2. J. Pieprzyk and G. Finkelstein. “Towards effective nonlinear cryptosystem design”, IEEE Proceedings, PT. E 135 (1988), pp. 325–335.
3. H. Feistel. “Cryptography and computer privacy”. Scientific American 228, 5 (1973), pp. 15–23.
4. W. Meier and O. Staffelbach. “Nonlinearity criteria for cryptographic functions”, in Advances in Cryptology- EUROCRYPT’89 (1990), no. 434 in Lecture Notes, Springer-Verlag, pp. 549–562.
5. M. Matsui. “Linear cryptanalysis method for DES cipher”, in Advances in Cryptology- EUROCRYPT’93 (1994), no. 765 in Lecture Notes in Computer Science, Springer-Verlag, pp. 386–397.

Ե. Ծ. ԱԼԱՎԵՐԴՅԱՆ
ՔՎԱԶԻԽՄԲԵՐԻ ՀԻՄԱՆ ՎՐԱ ԳԱՂՏՆԱԳՐԱՅԻՆ ԲՈՒԼՅԱՆ ՖՈՒՆԿՑԻԱՆԵՐԻ ԳԵՆԵՐԱՑՄԱՆ ԱՐԴՅՈՒՆԱՎԵՏՈՒԹՅԱՆ ԳՆԱՀԱՏԱԿԱՆԸ

Ամփոփում

Քննարկված է քվազիխմբերի վրա գաղտնագրային Բուլյան ֆունկցիաների գեներացման արդյունավետությունը, որը, համեմատած ավանդական եղանակի հետ, զգալիորեն արագացնում է վերոհիշյալ ընթացակարգը: Բերված քանակական գնահատականը թույլ է տալիս եզրակացնել, որ քվազիխմբերի ներգրավումը գաղտնագրային Բուլյան ֆունկցիաների գենե-

րացման համար հնարավորություն է ստեղծում համադրել մաթեմատիկական տրամաբանության և վերացական հանրահաշվի կարևորագույն դրույթները կայուն և արդյունավետ գաղտնահամակարգերի կառուցման գործընթացում:

Առանցքային բառեր. *գաղտնահամակարգ, Բուլյան ֆունկցիա, քվազիխումբ, ոչ գծայնություն, բալանսավորվածություն:*

Y. TS. ALAVERDYAN
EFFICIENCY OF GENERATING CRYPTOGRAPHIC BOOLEAN FUNCTIONS BASED ON QUASIGROUPS

Resume

Given estimation of efficiency generating cryptographic Boolean functions based on quasigroups, which in comparasion to classical medods, significantly increases the efficiency of the mentioned procedure. The quantitative analysis allows concluding that involving quasigroups in generating Boolean functions gives another opportunity to combine important concepts in Anstract Algebra and Discrete Mathematics for designing efficient and strong cryptosystems.

Keywords: *Cryptosystem, Boolean function, quasigroup, non linearuty, balancedness.*