УДК 004.9 https://doi.org/10.51301/vest.su.2021.i4.12

Е.Н. Сейткулов*, Р.М. Оспанов, Б.Б. Ергалиева
Евразийский национальный университет им. Л.Н. Гумилева, Нур-Султан, Казахстан
*e-mail: yerzhan.seitkulov@gmail.com

О КРИПТОГРАФИЧЕСКИХ СВОЙСТВАХ S-БЛОКОВ

Аннотация. Статья посвящена изучению криптографических свойств S-блоков. S-блок - функция, принимающая на входе n бит, преобразующая их по определенному алгоритму и возвращающая на выходе m бит. n и m не обязательно равны. S-блоки являются одним из основных компонентов современных криптографических алгоритмов, определяющих их нелинейность. Для защиты криптографических алгоритмов от различных типов атак S-блоки должны соответствовать ряду критериев. Целью настоящей работы является исследование существующих криптографических свойств S-блоков, которое позволит в дальнейшем провести анализ существующих критериев, которым должны удовлетворять S-блоки и сделать обоснованный выбор набора критериев оптимальных S-блоков. В данной статье дается обзор основных свойств S-блоков, имеющих важное значение при формировании критериев оптимальности. Рассматриваются дифференциальная равномерность, таблица распределения разностей, нелинейность, таблица линейного распределения, алгебраическая степень, алгебраическая иммунность, алгебраическая сложность, лавинный эффект, строгий лавинный эффект, расстояние до строго лавинного эффекта, полнота, линейные структуры, сбалансированность, корреляционная иммунность, критерий независимости битов, критерий распространения, период, количество неподвижных точек и противоположных неподвижных точек, циклы, инверсии, возрастания, таблица бумеранговой связи, таблица бумеранговой разности. Также рассматриваются существующие методы генерации S-блоков, обладающих необходимыми оптимальными характеристиками.

Ключевые слова: криптографический алгоритм, S-блок, свойства, критерии оптимальности.

Введение. S-блоки (блок подстановок, s-box, substitution box) являются одним из основных компонентов, определяющих нелинейность и уровень стойкости современных симметричных криптографических алгоритмов. В частности, они особенно важны для стойкости против дифференциальных атак, линейных атак, алгебраических атак и других методов криптоанализа. Можно сделать вывод, что S-блоки и их свойства имеют первостепенное значение для безопасности криптографического алгоритма в целом. Для защиты криптографических алгоритмов от различных типов атак S-блоки должны соответствовать ряду критериев. Из-за большого количества существующих критериев, их противоречивости или частичной взаимозависимости проблематично сформировать S-блок, обладающий всеми известными заданными свойствами. Поэтому на практике используются S-блоки, удовлетворяющие основным критериям, существенным для конкретного симметричного алгоритма. Такие S-блоки принято называть оптимальными. Целью настоящей работы является исследование существующих криптографических свойств S-блоков, которое позволит в дальнейшем провести анализ существующих критериев, которым должны удовлетворять S-блоки и сделать обоснованный выбор набора критериев оптимальных S-блоков. В данной статье дается обзор основных свойств S-блоков, имеющих важное значение при формировании критериев оптимальности. Рассматриваются дифференциальная равномерность, таблица распределения разностей, нелинейность, таблица линейного распределения, алгебраическая степень, алгебраическая иммунность, алгебраическая сложность, лавинный эффект, строгий лавинный эффект, расстояние до строго лавинного эффекта, полнота, линейные структуры, сбалансированность, корреляционная иммунность, критерий независимости битов, критерий распространения, период, количество неподвижных точек и противоположных неподвижных точек, циклы, инверсии, возрастания, таблица

бумеранговой связи, таблица бумеранговой разности. Также рассматриваются существующие методы генерации S-блоков, обладающих необходимыми оптимальными характеристиками.

Методы. Критерии оптимального S-блока могут быть установлены для целого класса криптографических алгоритмов, а также заданы и для отдельно взятого криптопримитива. При выборе S-блоков при проектировании криптоалгоритмов основными критериями являются нелинейность и дифференциальная равномерность. Дифференциальная равномерность является показателем стойкости против дифференциальной атаки. Например, для 8-битных подстановок оптимальными значениями дифференциальной равномерности являются значения не больше 8. Нелинейность является показателем стойкости против линейной атаки. Оптимальными значениями для 8-битных подстановок являются значения не меньше 100. Алгебраическая степень и алгебраический иммунитет являются показателями стойкости против алгебраических атак. В случае 8-битных подстановок оптимальными значениями алгебраической степени являются значения не меньше 7, а максимальным значением алгебраического иммунитета считается 3 при 441 уравнениях. А в случае подстановок 4 в 4 бита критерий алгебраического иммунитета не играет большой роли, так как они могут быть описаны системой уравнений второй степени. Но в тоже время он не может равняться 1. Ещё одним критерием является отсутствие циклов длины 1, т.е. неподвижных (фиксированных) точек. Существует и множество других критериев. До сих пор не была доказана необходимость большинства из критериев. Многие из них не применимы к блочным шифрам, но в то же время применяются в поточных шифрах. Свойства S-блоков блочных шифров DES и ГОСТ 28147 на сегодняшний день не являются актуальными. Современные критерии ориентированы на защиту от существующих видов криптоанализа: линейного, алгебраического и различных вариаций дифференциального. Еще один критерий связан с принадлежностью подстановок к различным классам эквивалентности векторных булевых функций. Этот критерий применим лишь в том случае, когда в алгоритме применяется более одного узла нелинейной замены. Многие исследования показывают, что идеальных S-блоков, вероятнее всего, не существует. Поэтому было введено понятие оптимального S-блока, критерии которого определяются для конкретного криптографического алгоритма или класса криптографических алгоритмов) и являются оптимальными с точки зрения защиты от существующих видов атак.

Результат. Пусть $B = GF(2)$. S-блоком называется векторная булева функция $F: B^n \to B^m$. Координатными функциями (координатами) S-блока $F: B^n \to B^m$ называются булевы функции $f_i: B^n \to B$, $1 \le i \le m$, такие что $F = (f_1, f_2, \dots, f_m)$. Компонентными функциями (компонентами) S-блока $F: B^n \to B^m$ называются линейные комбинации m координатных функций S-блока.

Основными способами представления S-блока являются таблица истинности, алгебраическая нормальная форма, преобразование Фурье, преобразование Уолша, автокорреляционная функция. Таблица истинности S-блока есть конкатенация таблиц истинности всех его координатных функций. Алгебраическая нормальная форма, преобразование Фурье, преобразование Уолша, автокорреляционная функция определяются с помощью соответствующих представлений компонентных функций S-блока.

Алгебраической нормальной формой булевой функции $f: B^n \to B$ называется представляющий ее многочлен от n переменных над полем B вида $f(x_1, x_2, \dots, x_n) = a \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n$, где $a, a_1, a_2, \dots a_n, a_{12}, a_{13}, \dots, a_{12\dots n} \in B$.

Замечание. Другое название алгебраической нормальной формы булевой функции - полином Жегалкина.

Алгебраической нормальной формой S-блока $F: B^n \to B^m$ называется представляющий его многочлен от n переменных над полем B^m вида $F(x_1, x_2, \dots, x_n) = a \oplus a_1 x_1 \oplus a_2 x_2 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus a_{13} x_1 x_3 \oplus \dots \oplus a_{12\dots n} x_1 x_2 \dots x_n$, где $a, a_1, a_2, \dots a_n, a_{12}, a_{13}, \dots, a_{12\dots n} \in B^m$.

Преобразованием Фурье булевой функции $f: B^n \to B$ называется функция $\underline{W_f}: B^n \to Z$, определяемая равенством $\underline{W_f}(u) = \sum_{x \in B^n} (-1)^{\langle x,u \rangle} f(x)$. Значение $\underline{W_f}(u)$ для каждого $u \in B^n$ называется коэффициентом Фурье.

Преобразованием Уолша булевой функции $f: B^n \to B$ называется функция $W_f: B^n \to Z$, определяемая равенством $W_f(u) = \sum_{x \in B^n} (-1)^{\langle x,u \rangle} (-1)^{f(x)}$. Значение $W_f(u)$ для каждого $u \in B^n$ называется коэффициентом Уолша.

Далее дадим обзор основных криптографических свойств S-блоков. Эти свойства являются достаточно общими и имеют важное значение для противодействия широко применяемым атакам.

Дифференциальная атака использует неравномерное распределение выходных разностей, когда входные данные выбираются с фиксированной разницей. Хотя линейные компоненты в криптографических алгоритмах могут эффективно рассеивать различия, они не могут помочь уменьшить неравномерность в отношении разностей. Таким образом, равномерное дифференциальное распределение в основном исходит из нелинейных компонентов. Показателем стойкости против дифференциальной атаки является дифференциальная равномерность.

S-блок $F: B^n \to B^m$ называется дифференциально -равномерным, если для каждого $a \in B^n$, $a \neq 0$, и каждого $b \in B^m$ уравнение $F(x) \oplus F(x \oplus a) = b$ имеет не более δ решений.

Например, для 8-битных подстановок оптимальными значениями дифференциальной равномерности являются значения не больше 8.

Также для оценки стойкости к дифференциальным атакам применяется таблица распределения разностей.

Таблицей распределения разностей (XOR-таблицей) S-блока $F: B^n \to B^m$ называется матрица T^{XOR} размера $2^n \times 2^m$ с элементами $T^{XOR}_{a,b} = |\{x \in B^n | F(x) \oplus F(x \oplus a) = b\}|$, $a \in B^n$, $b \in B^m$.

Высокие значения в XOR-таблице могут быть использованы для выполнения дифференциального криптоанализа, поэтому для устойчивости к дифференциальному криптоанализу важно избегать высоких значений.

Показателем стойкости против линейной атаки является нелинейность S-блока.

Расстоянием Хэмминга $d(f,g)$ между булевыми функциями f и g от n переменных называется количество значений аргументов, на которых значения функций различаются, т.е. $d(f,g) = |\{x \in B^n | f(x) \neq g(x)\}|$.

Расстоянием Хэмминга $d(f,M)$ от булевой функции f от n переменных до некоторого множества M булевых функций от n переменных называется следующая величина $d(f,M) = min_{g \in M} d(f,g)$.

Нелинейностью $N(f)$ булевой функции $f: B^n \to B$ называется расстояние Хэмминга между f и множеством всех аффинных функций от n переменных.

Булевы функции с линейностью, достигающей нижней границы, т. е. с наибольшей нелинейностью, являются бент-функциями.

Булева функция $f: B^n \to B$ называется максимально нелинейной, если она обладает наибольшей нелинейностью среди всех булевых функций от n переменных.

Булева функция $f: B^n \to B$ называется бент-функцией, если все коэффициенты Уолша этой функции равны $\pm 2^{n/2}$.

Замечание. При нечетном n бент-функции не существуют.

Нелинейностью $N(F)$ S-блока $F: B^n \to B^m$ называется минимальная из нелинейностей компонентных функций S-блока.

S-блок $F: B^n \to B^m$ называется бент-функцией, если его нелинейность достигает своего максимального возможного значения, т.е. если каждая его компонентная функция является бент-функцией.

Оптимальными значениями нелинейности для 8-битных подстановок являются значения не меньше 100.

Также для оценки стойкости к линейным атакам применяется таблица линейного распределения.

Таблицей линейного распределения (таблицей линейной аппроксимации) S-блока $F: B^n \to B^m$ называется матрица T^{LAT} размера $2^n \times 2^m$ с элементами $T_{a,b}^{LAT} = |\{x \in B^n | (x, a) = (F(x), b)\}|$, $a \in B^n$, $b \in B^m$.

Показателями стойкости против алгебраических атак являются алгебраическая степень и алгебраический иммунитет, а также алгебраическая сложность S-блока.

Алгебраической степенью $deg(F)$ S-блока $F: B^n \to B^m$ называется число переменных в самом длинном слагаемом его алгебраической нормальной формы.

Булева функция $g: B^n \to B$ называется аннигилятором булевой функции $f: B^n \to B$, если $g \neq 0$ и $fg = 0$.

Алгебраической иммунностью булевой функции $f: B^n \to B$ называется минимальная из степеней аннигиляторов f и $f \oplus 1$.

Аннигилятором подмножества $E \subset B^n$ называется любая булева функция от n переменных, принимающая нулевое значение на этом подмножестве.

Алгебраической иммунностью подмножества $E \subset B^n$ называется минимальная алгебраическая степень всех ненулевых аннигиляторов этого подмножества.

(Базовой) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется минимальная алгебраическая иммунность всех прообразов $F^{-1}(z)$ элементов $z \in B^m$.

(Графической) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется алгебраическая иммунность графа $\{(x, F(x)) | x \in B^n\}$ S-блока F.

(Компонентной) алгебраической иммунностью S-блока $F: B^n \to B^m$ называется минимальная алгебраическая иммунность компонентов S-блока F.

Алгебраической сложность S-блока $F: B^n \to B^m$ называется количество ненулевых одночленов интерполяционного многочлена Лагранжа, представляющего $F: B^n \to B^m$.

В случае 8-битных подстановок оптимальными значениями (компонентной) алгебраической степени являются значения не меньше 7, а максимальным значением алгебраического иммунитета считается 3 при 441 уравнениях. А в случае подстановок 4 в 4 бита критерий алгебраического иммунитета не играет большой роли, так как они могут быть описаны системой уравнений второй степени. Но в тоже время он не может равняться 1.

Важным свойством, определяющим оптимальность S-блока, является биективность.

S-блок $F: B^n \to B^n$ называется биективным, если она инъективна и сюръективна, то есть одновременно выполняются следующие условия:

1) для любых элементов $a', a'' \in B^n$, если $a' \neq a''$, то $F(a') \neq F(a'')$ (инъекция),

2) для любого элемента $b \in B^n$ существует элемент $a \in B^n$такой , что $F(a) = b$ (сюръекция).

Это свойство эквивалентно обратимости S-блока.

Показателями случайности S-блока являются инверсии, циклы, возрастания.

Инверсией S-блока $F: B^n \to B^n$ называется пара элементов $a', a'' \in B^n$ таких, что $n(a') < n(a'')$ и $n\big(F(a')\big) > n\big(F(a'')\big)$.

Циклом длины k S-блока $F: B^n \to B^n$ называется последовательность элементов $(a_1, \ldots, a_k)$ из B^n таких, что $F(a_1) = a_2$, ..., $F(a_i) = a_{i+1}$, …, $F(a_k) = a_1$.

Возрастанием S-блока $F: B^n \to B^n$ называется пара элементов $F(a'), F(a'') \in B^n$ таких, что $F(a') < F(a'')$ и $n(a'') = n(a') + 1$.

Еще в набор критериев оптимального S-блока можно включить период и количество неподвижных точек и противоположных неподвижных точек.

Периодом элемента $a \in B^n$ относительно S-блока $F: B^n \to B^n$ называется наименьшее положительное целое число r такое, что $F^r(a) = a$.

Элемент $a \in B^n$ называется неподвижной (фиксированной) точкой S-блока $F: B^n \to B^n$, если $F(a) = a$.

Элемент $a \in B^n$ называется противоположной неподвижной (фиксированной) точкой S-блока $F: B^n \to B^n$, если $F(a) = \bar{a}$, где $\bar{a} \in B^m$ такой, что $a \oplus \bar{a} = 0$.

Количество неподвижных и противоположных неподвижных точек должно быть как можно меньше для обеспечения стойкости против статистического криптоанализа.

Для оценки стойкости к бумеранг атакам применяются таблица бумеранговой связи и таблица бумеранговой разности.

Таблицей бумеранговой связи обратимого S-блока $F: B^n \to B^n$называется матрица T^{BCT} размера $2^n \times 2^n$ с элементами $T^{BCT}_{a,b} = |\{x \in B^n | F^{-1}(F(x) \oplus b) \oplus F^{-1}(F(x \oplus a) \oplus b) = a\}|$, $a \in B^n$, $b \in B^n$.

Таблицей бумеранговой разности обратимого S-блока $F: B^n \to B^n$называется матрица T^{BCT} размера $2^n \times 2^n \times 2^n$ с элементами $T^{BDT}_{a,b,c} = |\{x \in B^n | F^{-1}(F(x) \oplus c) \oplus F^{-1}(F(x \oplus a) \oplus c) = a, F(x) \oplus F(x \oplus a) = b\}|$, $a \in B^n$, $b \in B^n$, $c \in B^n$.

Важной характеристикой S-блока является лавинный эффект.

S-блок $F: B^n \to B^m$ обладает лавинным эффектом, если и только если $\sum_{x \in B^n} w\big(F(x) \oplus F(x \oplus e_i)\big) = m2^{n-1}$ для всех единичных векторов $e_i \in B^n$, $i = 1,2,\dots,n$.

S-блок $F: B^n \to B^m$ удовлетворяет строгому лавинному критерию, если и только если $\sum_{x \in B^n}\big(F(x) \oplus F(x \oplus e_i)\big) = (2^{n-1}, 2^{n-1}, \dots, 2^{n-1})$ для всех единичных векторов $e_i \in B^n$, $i = 1,2,\dots,n$.

Расстояние до строгого лавинного критерия для S-блока $F: B^n \to B^n$ определяется, как $DSAC(F) = \sum_{i=1}^{n} \sum_{a \in B^n, w(a)=1} \big| w\big(f_i(x \oplus a) \oplus f_i(x)\big) - 2^{n-1} \big|$.

S-блок $F: B^n \to B^m$ удовлетворяет критерию распространения степени k, если и только если $\sum_{x \in B^n}\big(F(x) \oplus F(x \oplus a)\big) = (2^{n-1}, 2^{n-1}, \dots, 2^{n-1})$ для всех элементов $a \in B^n$, где$1 \le w(a) \le k$.

S-блок $F: B^n \to B^n$ удовлетворяет критерию независимости битов, если для любых $i, j, k \in \{1,2,\dots,n\}$, $j \neq k$ инвертирование входного -го бита приводит к независимым изменениям выходных j-го и k-го битов.

Для измерения критерия независимости битов применяется коэффициент корреляции между -ым и k-ым битами лавинного вектора $A^{e_i} = F(x) \oplus F\big(x \oplus e^i\big) = \big(a_1^{e_i}, \dots, a_n^{e_i}\big)$. Соответствующий параметр меры независимости j-го и k-го битов определяется, как $BIC\big(a_j, a_k\big) = max_{1 \le i \le n} \left| corr\left(a_j^{e_i}, a_k^{e_i}\right) \right|$. Параметр, показывающий насколько $F: B^n \to B^n$ удовлетворяет критерию независимости битов определяется, как $BIC(F) = max_{1 \le j,k \le n, j \neq k} BIC\big(a_j, a_k\big)$. $BIC(F)$ принимает значения в промежутке [0,1]. В наилучшем случае $BIC(F)$ равен 0, в наихудшем 1.

Также полезными криптографическими характеристиками S-блока являются полнота, линейные структуры, сбалансированность, корреляционная иммунность.

S-блок $F: B^n \to B^m$ называется полным, если и только если $\sum_{x \in B^n}\big(F(x) \oplus F(x \oplus e_i)\big) > (0,0,\dots,0)$ для всех единичных векторов $e_i \in B^n$, $i = 1,2,\dots,n$. Единичный вектор e^i - это вектор, -ый бит которого равен 1, а остальные биты равны 0.

S-блок $F: B^n \to B^m$ обладает линейной структурой, если существует $a \in B^n$, $a \neq 0$, такой, что $D_a(F) \equiv const$.

Булева функция $f: B^n \to B$ называется уравновешенной (равновероятной, сбалансированной), если $|\{x \in B^n | f(x) = 1\}| = |\{x \in B^n | f(x) = 0\}|$, т.е. вес булевой функции $w(f) = 2^{n-1}$. Весом булевой функции $f: B^n \to B$ называется величина $w(f) = |\{x \in B^n | f(x) = 1\}|$.

S-блок $F: B^n \to B^m$ называется уравновешенным (сбалансированным), если для любого $y \in B^m$ имеет место равенство $|\{x \in B^n | F(x) = y\}| = 2^{n-m}$.

S-блок $F: B^n \to B^m$ является уравновешенным (сбалансированным) тогда и только тогда, когда его компонентные функции являются уравновешенными (сбалансированными).

Булева функция $g: B^k \to B$ называется подфункцией булевой функции $f: B^n \to B$, $k < n$, если g получена из f подстановкой констант вместо некоторых $n - k$ переменных.

Булева функция $f: B^n \to B$ называется корреляционно-иммунной порядка k, $0 < k \leq n$, если для любой её подфункции g от $n - k$ переменных имеет место равенство $w(g) = w(f)/2^k$.

Булева функция $f: B^n \to B$ называется -устойчивой, если она является уравновешенной (сбалансированной) и корреляционно-иммунной порядка k.

S-блок $F: B^n \to B^m$ называется корреляционно-иммунным порядка k, $0 < k \leq n$, если каждая его компонентная функция является корреляционно-иммунной порядка k.

S-блок $F: B^n \to B^m$ называется -устойчивым, если он является уравновешенным (сбалансированным) и корреляционно-иммунным порядка k.

Обсуждение. Генерация оптимальных S-блоков является трудоемкой задачей. Существующие методы получения S-блоков можно разделить на три основных направления: алгебраические конструкции, псевдослучайная генерация, эвристический подход.

В первом подходе S-блоки проектируются в соответствии с некоторыми доказанными математическими соотношениями и принципами. Наиболее известными представителями этого подхода являются биективные (n × n) S-блоки (перестановки), основанные на инверсии в конечном поле GF(2^n). Они являются лучшими S-блоками, найденными и одновременно оптимальными по отношению к большинству желаемых критериев. Например, S-блок в AES является таким S-блоком, который имеет высокую алгебраическую степень - 7, высокую нелинейность - 112, низкую автокорреляцию - 32 и низкую дифференциальную равномерность – 4. А в работе [1] предлагается конструкция на основе дробно-линейного преобразования и функции перестановки. В работе [2] рассматривается метод проектирования S-блоков, основанный на использовании кубических полиномиальных отображений. В работе [3] синтезируются (8 × 8) S-блоки на основе проективной общей линейной группы PGL(2,GF(2^8)) над полем Галуа GF(2^8). Существует множество других алгебраических методов генерации подстановок, например, [4], [5]. Несмотря на то, что такие S-блоки часто предпочтительны из-за их превосходных криптографических свойств, существуют некоторые проблемы, связанные с их простой алгебраической структурой и возможной будущей уязвимостью к алгебраическим атакам. Кроме того, число этих S-блоков невелико, и все они аффинно эквивалентны.

Второй подход состоит в построении S-блоков из таблицы случайных чисел с последующей проверкой его соответствия. Этот подход обречен на провал с самого начала, так как большинство искомых криптографических критериев часто противоречат друг другу, что значительно уменьшает количество S-блоков, которые хороши по всем критериям, и уменьшает вероятность подбора хорошего S-блоков.

При третьем подходе происходит процесс итеративного улучшения S-блока или целого набора S-блоков по отношению к одному или нескольким свойствам. В отличие от алгебраических конструкций, эвристические методы способны создавать большие наборы S-блоков, поскольку они используют методы прямого поиска. Чаще всего криптографические свойства S-блоков, полученные с помощью эвристических алгоритмов, не так хороши, как у алгебраически построенных S-блоков. Однако в последние годы разница между этими свойствами становится все более неразличимой. Последнее достигается с помощью некоторых специфических эвристических методов, таких как метод поиска восхождением к вершине, метод имитации отжига, генетические алгоритмы или различные их комбинации. Хотя большинство описанных методов дают хорошие результаты для построения биективных S-блоков только по одному из основных критериев, это становится гораздо более сложным, когда одновременно следует рассматривать как нелинейность, так и дифференциальную равномерность. Известен метод генерации высоко нелинейных S-блоков на основе градиентного спуска [6] требует последовательного применения нескольких критериев для каждой сформированной подстановки. В работе [7] представлено усовершенствование этого

метода путем соответствующего выбора порядка применения критериев, что снижает требуемую вычислительную мощность для генерации S-блоков. В работе [8] предлагается эвристический метод генерации больших множеств (n × n) биективных S-блоков, обладающих хорошим сочетанием целевых свойств, таких как высокая нелинейность, высокая алгебраическая степень, низкая дифференциальная однородность и низкая автокорреляция, основанный на использовании специфического искусственного иммунного алгоритма в сочетании с модификацией метода восхождения к вершине для S-блоков. В работе [9] обоснованы перспективы дальнейших исследований с целью совершенствования эвристических методов синтеза случайных S-блоков. А в работе [10] описывается обобщенная методология проектирования и тестирования S-блоков для симметричных шифров. Эта методология включает в себя применение трех хорошо зарекомендовавших себя тестов, которые должны использоваться для проектирования и тестирования каждого S-блока. Исследование также показывает, что по крайней мере некоторые математические методы проектирования S-блоков, будучи безопасными, не более безопасны, чем не математические методы, но более вычислительно интенсивны.

Таким образом актуальным вопросом является анализ существующих критериев для S-блоков и обоснованный выбор необходимого набора критериев для конкретных криптографических алгоритмов или классов криптографических алгоритмов; поиск и разработка теоретически обоснованных эффективных практических методов получения оптимальных S-блоков, обеспечивающих высокие показатели стойкости в симметричных криптографических алгоритмах. Проведенный анализ критериев и методов позволит построить наиболее эффективный алгоритм генерации оптимальных S-блоков.

Источник финансирования. Данная работа выполнена при финансовой поддержке грантового финансирования КН МОН РК, № AP09258274.

REFERENCES

[1] Nizam Chew L.C., Ismail E.S. S-box Construction Based on Linear Fractional Transformation and Permutation Function. *Symmetry* 2020, *12*, 826.

[2] Zahid A.H., Arshad M.J. An Innovative Design of Substitution-Boxes Using Cubic Polynomial Mapping. Symmetry 2019, *11*, 437.

[3] Altaleb A., Saeed M.S., Hussain I., Aslam M. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. AIP Advances. 2017, 7, 035116

[4] Hussain S., Jamal S. S., Shah T., Hussain I. A Power Associative Loop Structure for the Construction of Non-Linear Components of Block Cipher. *IEEE Access*, vol. 8, pp. 123492-123506, 2020

[5] Gao W., Idrees B., Zafar S., Rashid T. Construction of Nonlinear Component of Block Cipher by Action of Modular Group PSL(2, Z) on Projective Line PL(GF(28)). *IEEE Access*, vol. 8, pp. 136736-136749, 2020

[6] Kazimirov A.V. Metody i sredstva generatsii nelineinykh uzlov zameny dlya simmetrichnykh kriptoalgoritmov. Dissertatsiya na soiskanie uchenoi stepeni kandidata tekhnicheskikh nauk, spetsial'nost' 05.13.21 – sistemy zashchity informatsii. Khar'kovskii natsional'nyi universitet radioelektroniki, Khar'kov, 2013.

[7] Rodinko M., Oliynykov R., Gorbenko Y. Optimization of the high nonlinear s-boxes generation method. Tatra Mountains Mathematical Publications, Mathematical Institute, Slovak Academy of Sciences, Bratislava, 2017, Volume 70: Issue 1, pp. 93-105.

[8] Ivanov G., Nikolov N., Nikova S. Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm. In: Pasalic E., Knudsen L. (eds) Cryptography and Information Security in the Balkans. BalkanCryptSec 2015. Lecture Notes in Computer Science, vol 9540. Springer, Cham. 2016, pp 31-42.

[9] Gorbenko I., Kuznetsov A., Gorbenko Y., Pushkar'ov A., Kotukh Y., Kuznetsova K. Random S-Boxes Generation Methods for Symmetric Cryptography. 2019 IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), Lviv, Ukraine, 2019, pp. 947-950.

[10] Easttom C. A generalized methodology for designing non-linear elements in symmetric cryptographic primitives. 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 2018, pp. 444-449.

Е.Н. Сейткұлов*, Р.М. Оспанов, Б.Б. Ергалиева
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан, Қазақстан
*e-mail: yerzhan.seitkulov@gmail.com

S-БЛОКТАРДЫҢ КРИПТОГРАФИЯЛЫҚ ҚАСИЕТТЕРІ ТУРАЛЫ

Аңдатпа. Мақала S-блоктардың криптографиялық қасиеттерін зерттеуге арналған. S-блок - кірісте n бит қабылдайтын, оларды белгілі бір алгоритм бойынша түрлендіретін және шығуда m бит қайтаратын функция. n және m міндетті түрде тең емес. S-блоктар қазіргі заманғы криптографиялық алгоритмдердің негізгі компоненттерінің бірі болып табылады, олардың сызықты емес екендігін анықтайды. Криптографиялық алгоритмдерді әртүрлі шабуылдардан қорғау үшін S-блоктар бірқатар өлшемдерге сәйкес келуі керек. Бұл жұмыстың мақсаты S-блоктардың қолданыстағы криптографиялық қасиеттерін зерттеу болып табылады, бұл S-блоктарды қанағаттандыратын және оңтайлы S-блоктардың критерийлерінің жиынтығын негізделген таңдауды қажет ететін қолданыстағы критерийлерді одан әрі талдауға мүмкіндік береді. Бұл мақалада оптималдылық критерийлерін қалыптастыруда маңызды S-блоктарының негізгі қасиеттеріне шолу жасалады. Дифференциалдық біркелкілік, айырмашылықтардың таралу кестесі, сызықтық емес, сызықтық таралу кестесі, алгебралық дәреже, алгебралық иммундылық, алгебралық күрделілік, көшкін эффектісі, қатаң көшкін эффектісі, қатаң көшкін эффектіне дейінгі қашықтық, толықтығы, сызықтық құрылымдар, тепе-теңдік, корреляциялық иммундылық, биттердің тәуелсіздігі критерийі, таралу критерийі, период, бекітілген нүктелер саны және қарама-қарсы бекітілген нүктелер, циклдар, инверсиялар, өсу, бумеранг байланысы кестесі, бумеранг айырмашылығы кестесі. Қажетті оңтайлы сипаттамалары бар S-блоктарын құрудың қолданыстағы әдістері де қарастырылады.

Негізгі сөздер: криптографиялық алгоритм, S-блок, қасиеттер, оптималдылық критерийлері.

Y.N. Seitkulov*, R.M. Ospanov, B.B. Yergaliyeva
L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan
*e-mail: yerzhan.seitkulov@gmail.com

ON CRYPTOGRAPHIC PROPERTIES OF S-BOXES

Abstract. The article is devoted to the study of cryptographic properties of S-boxes. S-box is a function that accepts n bits at the input, converts them according to a certain algorithm and returns m bits at the output. n and m are not necessarily equal. S-boxes are one of the main components of modern cryptographic algorithms that determine their nonlinearity. To protect cryptographic algorithms from various types of attacks, S-boxes must meet a number of criteria. The purpose of this work is to study the existing cryptographic properties of S-boxes, which will allow us to further analyze the existing criteria that S-boxes must meet and make a reasonable choice of a set of criteria for optimal S-boxes. This article provides an overview of the main properties of S-boxes that are important in the formation of optimality criteria. Differential uniformity, difference distribution table, nonlinearity, linear distribution table, algebraic degree, algebraic immunity, algebraic complexity, avalanche effect, strict avalanche effect, distance to strictly avalanche effect, completeness, linear structures, balancedness, correlation immunity, bit independence criterion, propagation criterion, period, number of fixed points and opposite fixed points, cycles, inversions, increases, boomerang connection table, boomerang difference table are considered. The existing methods of generating S-boxes with the necessary optimal characteristics are also considered.

Keywords: cryptographic algorithm, S-box, properties, optimality criteria.