УДК 004.9
https://doi.org/10.47533/2020.1606-146X.144

Е. Н. СЕЙТКУЛОВ*, Р. М. ОСПАНОВ, Н. Н. ТАШАТОВ, Б. Б. ЕРГАЛИЕВА, Д. Ж. САТЫБАЛДИНА

Евразийский национальный университет им. Л.Н.Гумилева, Нур-Султан, Казахстан

НАБОР БЕЗУСЛОВНЫХ КРИТЕРИЕВ ОПТИМАЛЬНОСТИ S-БЛОКОВ

В работе проведена работа по систематизации и анализу основных критериев, которым должны удовлетворять S-блоки, чтобы обеспечить высокий уровень криптостойкости симметричных криптографических алгоритмов. Множество всех возможных критериев для их оценки можно разделить на безусловные и условные. К безусловным относятся критерии, которым S-блоки должны удовлетворять в обязательном порядке, чтобы обеспечить их стойкость к основным криптоаналитическим атакам. К условным относятся дополнительные критерии, которым S-блоки должны удовлетворять, чтобы сравнивать S-блоки, удовлетворяющие безусловным критериям. В работе представлен обоснованный выбор набора безусловных критериев, определяющих оптимальность S-блоков.

***Ключевые слова**: S-блоки, таблица замен, криптография, симметричное шифрование, информационная безопасность, защита информации.*

Введение. Обеспечение свойств информационной безопасности, таких как конфиденциальность, целостность и т.д. обычно предполагает использование симметричного шифрования. Поскольку симметричные криптографические преобразования обладают рядом преимуществ при практическом использовании с точки зрения их эффективности, скорости и надежности. S-блоки играют важную роль в обеспечении стойкости симметричных преобразований. В частности, криптографические свойства S-блоков напрямую влияют на стойкость шифров к различным криптоаналитическим атакам. Таким образом, генерация S-боксов с необходимыми криптографическими характеристиками является актуальной и важной задачей.

Большинство известных работ в области анализа и синтеза S-блоков для современных криптографических алгоритмов используют математический аппарат криптографических булевых функций. Математически S-блок определяется с помощью булевых функций и векторных булевых функций. В этом случае векторные булевые функции (S-блоки) представляются набором компонентных булевых функций, свойства которых характеризуют эффективность всего S-блока.

При выборе S-блоков для новых криптографических алгоритмов основными критериями являются нелинейность и дифференциальная равномерность. Дифференциальная равномерность является показателем стойкости против дифференциальной атаки. Нелинейность является показателем стойкости против линейной атаки. Алгебраическая степень и алгебраический иммунитет являются показателями стойкости против алгебраических атак. 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.

* E-mail корреспондирующего автора: yerzhan.seitkulov@gmail.com

Многие из них не применимы к блочным шифрам, но в то же время применяются в поточных шифрах. 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.

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.

Набор безусловных критериев оптимальности s-блоков. S-блоки (блоки подстановок) отображают блок из n битов в выходной блок из m битов (n и m не обязательно равны). S-блоки являются одним из основных компонентов, определяющих нелинейность криптографического алгоритма. Для защиты алгоритмов от различных видов атак S-блоки должны обладать рядом криптографических свойств. В настоящее время основными атаками, для которых имеют значения свойства S-блоков, используемых в криптографических алгоритмах, являются атаки, основанные на линейном, дифференциальном, алгебраическом методах криптоанализа. Другие методы анализа достаточно специфичны для отдельно взятого алгоритма, и, как правило, используют общую структуру алгоритма, а не отдельные его составляющие компоненты, как, например, S-блоки. При генерации S-блоков стремятся к достижению либо предельных показателей, обеспечивающих защиту от определенных видов атак, либо характеристик, обеспечивающих защиту от всех известных на текущий момент времени атак. Множество всех возможных критериев для оценки S-блоков можно разделить на безусловные критерии и условные критерии [1]. К безусловным относятся критерии, которым S-блоки должны удовлетворять в обязательном порядке, чтобы обеспечить их стойкость к основным криптоаналитическим атакам. К условным относятся дополнительные критерии, которым S-блоки должны удовлетворять, чтобы сравнивать S-блоки, удовлетворяющие безусловным критериям. 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 [2].

S-блок $F{:}B^n \to B^m$ называется оптимальным, если он удовлетворяет набору критериев, определяющих криптографическую стойкость алгоритма, в котором исполь-

зуется данный S-блок, к основным видам криптоаналитических атак (линейной, дифференциальной, алгебраической).

Критерии оптимального S-блока могут быть установлены для целого класса криптографических алгоритмов, а также заданы и для отдельно взятого криптоалгоритма. Можно сформировать контрольный список критериев для проектирования S-блока. Это не значит, что выбранный S-блок должен соответствовать всем критериям, но, скорее, когда проектировщик алгоритма меняет некоторые критерии ради достижения каких-нибудь других преимуществ, он должен внимательно рассмотреть любое нежелательное свойство, которое может возникнуть при этом, и должен проверить, есть ли другие компоненты в проектируемом алгоритме, которые могут исправить слабость без особых затрат. Искусство таких компромиссов было показано при проектировании ряда алгоритмов. Известным примером является криптографический алгоритм хеширования Keccak, в котором нелинейный компонент, представленный 5-битным S-блоком, не является сильным, если его оценивать с использованием ряда критериев, таких как, например, дифференциальная однородность, линейность, алгебраическая степень. Однако с точки зрения реализации этот алгоритм лучше. Выбор S-блока в алгоритме Keccak направлен в сторону от безопасности к производительности, в то же время тщательно разработанный линейный слой, правильная комбинация между различными компонентами и количество раундов исправляет слабость нелинейного слоя. Критерии для проектирования S-блоков могут быть расширены до критериев проектирования раундовых функций в целом всего алгоритма. Обычно возможно применить критерии для S-блока к небольшому количеству раундов, например, для двух раундов, что полезно для поиска потенциальных слабых мест в проектируемом алгоритме.

Далее сформируем примерный набор критериев, которым должны удовлетворять оптимальные S-блоки.

Критерий 1. (Дифференциальная равномерность). При выборе блоков подстановок одним из основных критериев является дифференциальная равномерность. Свойство дифференциальной равномерности определяется следующим образом [3]. S-блок $F{:}B^n \to B^m$ называется дифференциально δ-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. Порядком дифференциальной равномерности S-блока $F{:}B^n \to B^m$ называется минимальное δ такое, что $F{:}B^n \to B^m$ является дифференциально δ-равномерной. Легко видеть, что минимально возможный порядок равен 2^{n-m}. Функции минимального порядка дифференциальной равномерности 2^{n-m} называют совершенно нелинейными функциями (PN-функциями). Заметим, что при m = n PN-функций не существует, поскольку если x_0 – решение уравнения $F(x) \oplus F(x \oplus a) = b$, то и $x_0 \oplus a$ также является решением. При $m = n$ функции порядка дифференциальной равномерности 2 называются почти совершенно нелинейными (APN-функциями). Дифференциальная равномерность является показателем стойкости против дифференциальной атаки. Также для оценки стойкости против дифференциальной атаки используется таблица распределения разностей или XOR-таблица. Между дифференциальной δ-равномерностью и таблицей распределения разностей существует очевидная связь: $\delta = \max(T_{a,b}^{XOR})$. На-

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

Критерий 2. (Нелинейность). Также при выборе блоков подстановок к основным критериям относят нелинейность. Свойство нелинейности булевой функции определяется следующим образом [2]. Нелинейностью $N(f)$ булевой функции $f:B^n \to B$ называется расстояние Хэмминга между f и множеством всех аффинных функций от n переменных. Известно, что нелинейность булевой функции всегда удовлетворяет следующему неравенству: $N(f) \le 2^{n-1} - 2^{n/2-1}$. Булевые функции, обладающие наибольшей нелинейностью среди всех булевых функций от n переменных, называются максимально нелинейными. В случае четного числа переменных максимально нелинейные функции также называются бент-функциями, т.е. функциями, все коэффициенты Уолша которых равны $\pm 2^{n/2}$. При нечетном n бент-функции не существуют. Другими словами бент-функциями являются булевые функции с линейностью, достигающей нижней границы, т.е. с наибольшей нелинейностью. Нелинейность S-блоков определяется через нелинейность компонентных функций S-блоков, т.е. нелинейностью $N(F)$ S-блока $F:B^n \to B^m$ называется минимальная из нелинейностей компонентных функций S-блока. Также для S-блоков определяется понятие бент-функции. 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. Нелинейность является показателем стойкости против линейной атаки. Также для оценки стойкости используется таблица линейного распределения или таблица линейной аппроксимации. Между нелинейностью и таблицей линейного распределения S-блока существует непосредственная связь, выражаемая следующим соотношением: $N(F) = 2^{n-1} - \max(T_{a,b}^{LAT})$. Это позволяет легко находить значение нелинейности S-блока при известном значении максимума элементов таблицы линейного распределения, и наоборот. Таким образом, эти два свойства являются взаимозаменяемыми при оценке криптографической стойкости S-блока. Оптимальными значениями нелинейности для 8-битных подстановок являются значения не меньше 100.

Критерии 3 и 4. (Алгебраическая степень и алгебраическая иммунность). Важной криптографической характеристикой булевой функции является ее алгебраическая степень $\deg(f)$, т.е. число переменных в самом длинном слагаемом алгебраической нормальной формы булевой функции. В криптографических алгоритмах, в частности, в симметричных блочных алгоритмах шифрования следует выбирать функции с достаточно большой степенью. Повышение алгебраической степени приводит к повышению линейной сложности генерируемой последовательности; к повышению степени системы нелинейных уравнений, описывающих шифр. Аналогично алгебраическая степень S-блока также имеет важное значение. Алгебраической степенью $\deg(F)$ S-блока $F:B^n \to B^m$ называется число переменных в самом длинном слагаемом его алгебраической нормальной формы.

Важным криптографическим свойством, определяющим стойкость против алгебраических атак, является алгебраическая иммунность (или алгебраический иммунитет). Существует несколько подходов к определению этого понятия [4]. Определяются базовая алгебраическая иммунность, графическая алгебраическая иммунность и компонентная алгебраическая иммунность.

Базовой алгебраической иммунностью S-блока $F:B^n \to B^m$ называется минимальная алгебраическая иммунность всех прообразов $F^{-1}(z)$ элементов $z \in B^m$. Здесь алгебраической иммунностью подмножества $E \subset B^n$ называется минимальная алгебраическая степень всех ненулевых аннигиляторов этого подмножества. Аннигилятором подмножества $E \subset B^n$ называется любая булева функция от n переменных, принимающая нулевое значение на этом подмножестве.

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 иммунностью булевой функции $f:B^n \to B$ называется минимальная из степеней аннигиляторов f и $f \oplus 1$. Булева функция $g:B^n \to B$ называется аннигилятором булевой функции $f:B^n \to B$, если $g \neq 0$ и $fg = 0$.

Алгебраическая степень и алгебраическая иммунность являются показателями стойкости против алгебраических атак. Алгебраическая атака – это метод криптографического анализа, основанный на алгебраических свойствах шифра. Впервые этот метод был применён к блочным шифрам Н. Куртуа (N. Courtois) в 2002 г. Алгебраические атаки используют внутреннюю структуру шифра, то есть для получения ключа необходимо представить алгоритм шифрования в виде системы уравнений с минимальной степенью многочленов и впоследствии решить данную систему. В случае 8-битных подстановок оптимальными значениями алгебраической степени являются значения не меньше 7, а максимальным значением алгебраической иммунности считается 3 при 441 уравнениях. А в случае подстановок 4 в 4 бита критерий алгебраической иммунности не играет большой роли, так как они могут быть описаны системой уравнений второй степени. Но в то же время он не может равняться 1.

Критерии 5 и 6. (Период, количество неподвижных точек и противоположных неподвижных точек). Еще в набор критериев оптимального S-блока можно включить период и количество неподвижных точек и противоположных неподвижных точек. Эти понятия определяются следующим образом [2].

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 $F(a) = a$, т.е. период равен 1.

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.

Критерий 7. (Биективность). Важным свойством, определяющим оптимальность S-блока, является биективность. Биективность S-блока определяется следующим образом. S-блок $F:B^n \to B^n$ называется биективным, если она инъективна и сюръектив-

на, 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.

Таким образом, в случае $n = m = 8$ набор критериев оптимальных S-блоков состоит из 7 критериев: дифференциальной равномерности, нелинейности, алгебраической степени, алгебраической иммунности, количества неподвижных и противоположных неподвижных точек и периода, а также биективности.

Заключение. В данной работе рассмотрен важный вопрос критериального подхода к оценке криптографической стойкости S-блоков. S-блоки являются одним из основных компонентов, определяющих нелинейность и уровень стойкости современных симметричных криптографических алгоритмов. Для защиты алгоритмов от различных видов атак S-блоки должны удовлетворять целому ряду критериев. В работе проведена работа по систематизации и анализу существующих критериев, которым должны удовлетворять S-блоки, чтобы обеспечить высокий уровень криптостойкости криптографических алгоритмов, структура которых использует S-блоки. Множество всех возможных критериев для оценки S-блоков можно разделить на безусловные критерии и условные критерии. К безусловным относятся критерии, которым S-блоки должны удовлетворять в обязательном порядке, чтобы обеспечить их стойкость к основным криптоаналитическим атакам. К условным относятся дополнительные критерии, которым S-блоки должны удовлетворять, чтобы сравнивать S-блоки, удовлетворяющие безусловным критериям. Многие исследования показывают, что идеальных S-блоков, вероятнее всего, не существует. В работе исследовано понятие оптимальности S-блоков, критерии которых определяются для конкретного криптографического алгоритма или класса криптографических алгоритмов и являются оптимальными с точки зрения защиты от существующих видов атак. Осуществлен обоснованный выбор набора критериев, определяющих оптимальность S-блоков.

Благодарности. Работа выполнена при финансовой поддержке КН МОН РК, № AP09258274

ЛИТЕРАТУРА

1 Горбенко И., Кузнецов А., Горбенко Ю., Пушкарев А., Котух Ю., Кузнецова К. Методы генерации случайных S-блоков для симметричной криптографии / 2-я Украинская конференция IEEE по электротехнике и вычислительной технике (UKRCON), 2019, стр. 947-950, doi: 10.1109/UKRCON.2019.8879962.

2 Казимиров А.В. Методы и инструменты генерации узлов нелинейной подстановки для симметричных криптоалгоритмов. Диссертация на соискание ученой степени кандидата технических наук по специальности 05.13.21 – системы информационной безопасности. Харьковский национальный университет радиоэлектроники, Харьков, 2013.

3 Нюберг К. Дифференциально однородные отображения для криптографии // Eurocrypt'93. LNCS. 1994. V. 765. C. 55-64.

4 Карле С. Векторные булевы функции для криптографии. Глава монографии по булевым моделям и методам в математике, информатике и инженерии. Под ред. Ю.Крамы, П.Хаммера, Издательство Кембриджского университета, Кембридж, 2010, стр.398-469.

REFERENCES

1 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), 2019, pp. 947-950, doi: 10.1109/UKRCON.2019.8879962.

2 Kazimirov A.V. Methods and tools for generating nonlinear substitution nodes for symmetric cryptoalgorithms. Dissertation for the degree of candidate of technical sciences, specialty 05.13.21 - information security systems. Kharkiv National University of Radio Electronics, Kharkiv, 2013.

3 Nyberg K. Differentially uniform mappings for cryptography // Eurocrypt'93. LNCS. 1994. V. 765. P. 55–64.

4 Carlet C. Vectorial Boolean functions for cryptography. Chapter of the monography in Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Ed. by Y.Crama, P.Hammer, Cambridge University Press, Cambridge, 2010, pp.398-469.

Е. Н. СЕЙТҚҰЛОВ, Р. М. ОСПАНОВ, Н. Н. ТАШАТОВ, Б. Б. ЕРҒАЛИЕВА, Д. Ж. САТЫБАЛДИНА

Л.Н.Гумилев атындағы Еуразия ұлттық университеті.
Нұр-Сұлтан, Қазақстан
e-mail: yerzhan.seitkulov@gmail.com

ОПТИМАЛДЫ S-БЛОКТАР ҮШІН ШАРТСЫЗ КРИТЕРИЙЛЕР ЖИНАҒЫ

Бұл жұмыста симметриялық криптографиялық алгоритмдердің криптографиялық беріктігінің жоғары деңгейін қамтамасыз ету үшін S-жәшіктері қанағаттандыруға тиіс негізгі критерийлерді жүйелеу және талдау жұмыстары жүргізілді. Оларды бағалаудың барлық мүмкін критерийлерінің жиынтығын шартсыз және шартты деп бөлуге болады. Шартсыз критерийлер негізгі криптоаналитикалық шабуылдарға төзімділігін қамтамасыз ету үшін S-қораптары қанағаттандыруы керек критерийлер болып табылады. Шартты шартсыз критерийлерге сәйкес келетін S-жәшіктерін салыстыру үшін S-жәшіктері сәйкес келуі керек қосымша критерийлерге жатады. Жұмыста S-қораптарының оңтайлылығын анықтайтын шартсыз критерийлер жиынтығының ақылға қонымды таңдауы ұсынылған.

Түйін сөздер*: S-қораптары, алмастыру кестесі, криптография, симметриялық шифрлау, ақпаратты қорғау, ақпаратты қорғау.*

YERZHAN N. SEITKULOV, RASLAN M. OSPANOV, NURLAN N. TASHATOV, BANU B. YERGALIYEVA, DINA ZH. SATYBALDINA

Gumilyov Eurasian National University
Nur-Sultan, Kazakhstan
e-mail: yerzhan.seitkulov@gmail.com

SET OF UNCONDITIONAL CRITERIA FOR OPTIMAL S-BLOCKS

In this work, work has been carried out to systematize and analyze the main criteria that S-boxes must satisfy in order to ensure a high level of cryptographic strength of symmetric cryptographic algorithms.

The set of all possible criteria for their assessment can be divided into unconditional and conditional. The unconditional criteria are those that must be met by S-boxes in order to ensure their resistance to major cryptanalytic attacks. Conditional refers to additional criteria that S-boxes must meet in order to compare S-boxes that meet the unconditional criteria. The paper presents a reasonable choice of a set of unconditional criteria that determine the optimality of S-boxes.

***Keywords**: S-boxes, substitution table, cryptography, symmetric encryption, information security, information protection.*