Множину головних ідеалів Z[α] простої норми визначають пари чисел p і c_p, де p- просте число і $c_p \in \{0,1,\ldots,p-1\}$.Число c_p повинно задовольняти умову $f(c_p) \equiv 0 \bmod p$. Під час пошуку пар можна використовувати головні ідеали норми p породжені p і $\alpha - c_p$ або еквівалентні головні ідеали Z[α], що перетворюються гомоморфізмом в Z / pZ і α відображається в c_p. Зокрема, число $a + \alpha b$ знаходиться в головному ідеалі, що відповідає парі чисел p і c_p, якщо тільки $a + c_p b \equiv 0 \bmod p$. Головний ідеал $a + \alpha b$ характеризується нормою $N(a + \alpha b) = a^d - c(-b)^d \in Z$, де a і b - взаємопрості числа.

Для того щоб знайти конкретні значення чисел a і b поступають таким чином: зафіксуємо b і перевіряємо $a+mb$ на гладкість за допомогою решета поля. Для простого p стартова точка для решета є $-mb$ mod p кінцева точка b+1. Якщо $f(c_p) \equiv 0 \bmod p$, то значення a обчислюємо за формулою $a \equiv -c_p b \bmod p$. Згідно алгоритму p ділить $N(a + \alpha b) = a^d - c(-b)^d \in Z$, якщо $a \equiv -c_p b \bmod p$. Отже ми знайшли пару чисел a і b, котрі будуть використані для факторизації числа n.

Результат роботи алгоритму дозволяє визначити таємний ключ системи шифрування RSA за відкритим ключем. Час роботи алгоритму, що реалізує метод решета числового поля, оцінюється виразом $\exp\left((c + o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}\right)$, c=1,526.

Література: 1. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 247 с., 2. Lenstra A.K., Lenstra H.W., Manasse Jr, M.S., Pollard J.M. The number field sieve. Online access through WWW: http://www.rsasecurity.com/rsalabs/faq/., 3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К.: Держстандарт України, 1997. – 11 с.

УДК 638.322

ИСПОЛЬЗОВАНИЕ АППАРАТА БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ

Константин Самофалов, Эль-Хами Иад, Святослав Кожемякин
Национальный Технический Университет Украины "КПИ"

Анотація: **Ціллю досліджень є розробка підходу до визначення рівня захищеності широкого класу криптографічних алгоритмів, що базується на використанні апарату булевих функцій. Показано, що криптографічні властивості широкого класу алгоритмів мають за основу математичну задачу віднаходження коренів системи булевих нелінійних рівнянь, що не має аналітичного вирішення. Доведена тотожність проблеми порушення захисту та проблеми розв'язання систем нелінійних булевих рівнянь. Запропоновано оцінювати стійкість алгоритмів за допомогою досліджень специфічних властивостей еквівалентних булевих функцій.**

Summary: **The aim of the study is to develop an approach to analysis of the security level of cryptographic algorithm on the basis of Boolean function tool application. It has been shown that security of the broad class of cryptographic algorithms, is based on the difficulty to solve an analytically intractable problem of finding the roots of a nonlinear Boolean equation system. The break methods for cryptographic algorithms of this class are identical with strategy of search diminishing at finding the roots of such a system. Criteria for evaluation of equivalent Boolean equation system solution difficulty are worked out as well as means of their practical identification are presented.**

Ключові слова: **булеві функції, повна та умовна ентропія булевих функцій, критерій лавинного ефекту, алгоритми захисту інформації**.

I Введение

Одним из наиболее важных компонент современных систем защиты информации являются криптографические алгоритмы. Определение обьективного уровня устойчивости криптографических алгоритмов к вскрытиям аналитическими и комбинированными методами представляет собой практически важную

проблему. К настоящему времени устойчивость алгоритмов к вскрытиям в большинстве случаев оценивается только по отношению к перебору. Трудность выработки единого подхода к оценке устойчивости криптографических алгоритмов к аналитическим методам вскрытия находит свое обьяснение в следующем:

- каждый из широкого спектра используемых и предлагаемых к использованию криптографических алгоритмов обладает специфическими особенностями, затрудняющими или наоборот, способствующими применение тех или иных аналитических методов вскрытия:

- существует достаточно широкое многообразие аналитических методов вскрытия, эффективность которых зависит не только от вскрываемого криптографического алгоритма, но и от особенностей протоколов их использования.

К настоящему времени для оценки устойчивости криптографических алгоритмов к аналитическим методам вскрытия широко применяется метод, состоящий в открытой публикации алгоритма и организации его широкого обсуждения в форме конференций, издании тематических сборников статей, посвященных вопросам его криптостойкости, экспертного оценивания по сети Интернет . По такому пути идет в настоящее время выбор и оценка криптостойкости алгоритмов симметричного шифрования, призванного заменить устаревший к настоящему времени DES в рамках проекта AES. Однако такой подход оправдан далеко не всегда и сопряжен с большой задержкой внедрения алгоритма, а также не гарантирует того, что со временем не будет найден эффективный аналитический метод вскрытия. Так, DES был опубликован еще в конце 70-х годов, и только в середине 90-х были опубликованы достаточно эффективные методы его вскрытия [2].

В основе всех криптографических алгоритмов лежит трудно решаемая математическая задача, которая не может быть решена аналитически. Единственным способом решения таких задач является перебор. В основе достаточно широкого класса криптографических алгоритмов лежит задача отыскания корней систем нелинейных булевых уравнений, которая не может быть решена аналитически. К числу таких алгоритмов относятся такие широко используемые алгоритмы как DES, IDEA, RC-5, SHA и большая часть алгоритмов, опубликованных для изучения в рамках проекта AES.

Для решения актуальной задачи единого способа оценки устойчивости достаточно широкого класса криптографических алгоритмов к аналитическим методам вскрытия, предлагается излагаемый ниже подход, основанный на достаточно общем способе представления криптографических преобразований и сведении большей части задач вскрытия к единой математической проблеме.

II Представление алгоритмов защиты информации булевыми функциями

Анализ большинства используемых в настоящее время алгоритмов криптографического показывает, что практически все из них имеют блочную структуру, так, что h-разрядный двоичный вектор $\underline{Y} = (y_1, y_2, ..., y_h)$ выходного сообщения зависит только от входного n-разрядного двоичного вектора $\underline{X}=(x1,x2,...,xn)$ входного сообщения и r-разрядного двоичного вектора ключа $\underline{K}=(k_1,k_2,...,k_r)$, причем для обратимых алгоритмов n=h. Поэтому практически задача вскрытия алгоритма трансформируется в задачу вскрытия блока этого алгоритма с конечным числом входов и выходов. Независимо от используемого криптографического алгоритма, компоненты $y_i \{0,1\}$, i=1,...,h выходного вектора $\underline{Y}$ могут быть представлены системой h булевых функций:

$$
\begin{aligned}
& f_1(x_1,x_2,...,x_n,k_1,k_2,...,k_r) = y_1 \\
& f_2(x_1,x_2,...,x_n,k_1,k_2,...,k_r) = y_2 \\
& \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\
& f_h(x_1,x_2,...,x_n,k_1,k_2,...,k_r) = y_h
\end{aligned} \qquad (1)
$$

На практике каждая из функций системы (1) является достаточно сложной и для большинства криптографических алгоритмов содержит десятки тысячи термов. Для некоторых алгоритмов, в которых не используется ключ (например, SHA), функции системы (1) зависят только от компонент вектора $\underline{X}$.

Применительно к задачам вскрытия симметричных криптографических алгоритмов [5] наиболее часто встречается задача определения ключа по известным входному сообщению и выходному коду блока.

При решении этой задачи вскрытия, когда известны значения компонент векторов $\underline{X}$ и $\underline{Y}$ система (1) булевых функций преобразуется к приведенной ниже системе булевых уравнений:

$$
\begin{aligned}
& \varphi_1(k_1,k_2,...,k_r) = 0 \\
& \varphi_2(k_1,k_2,...,k_r) = 0 \\
& \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \\
& \varphi_h(k_1,k_2,...,k_r) = 0
\end{aligned} \qquad (2)
$$

Таким образом, задача вскрытия эквивалентна задаче решения приведенной системы (2) булевых уравнений относительно $k_1,k_2,...,k_r$.

Применительно к необратимым алгоритмам (хеш-алгоритмам), задача вскрытия блока формулируется как нахождение такого входного информационного кода, который обеспечивает формирование на выходе блока заданного выходного кода, то есть когда известными элементами являются ключ $\underline{K}$ (если он используется) и выходной вектор $\underline{Y}$, и необходимо найти входной вектор $\underline{X}$ [5]. Система (1) булевых функций, описывающих работы блока хеш-алгоритма в этом случае также сводится к системе булевых уравнений:

$$(3)\quad \begin{aligned} \psi_1(x_1,x_2,...,x_n) &= 0 \\ \psi_2(x_1,x_2,...,x_n) &= 0 \\ &\cdots\cdots\cdots \\ \psi_h(x_1,x_2,...,x_n) &= 0 \end{aligned}$$

Следовательно, и применительно к необратимым криптографическим алгоритмам, задача вскрытия эквивалентна в математическом плане решению системы булевых уравнений.

Таким образом, задачи вскрытия симметричных обратимых и необратимых криптографических алгоритмов сводится к решению систем булевых уравнений. Соответственно, сложность задачи вскрытия криптографического алгоритма может быть оценена через сложность решения эквивалентной системы булевых уравнений.

Решение систем линейных булевых уравнений не представляет большого труда. Однако, решение системы нелинейных булевых уравнений представляет собой сложную математическую задачу, которая в полной мере может быть отнесена к категории трудно решаемых задач булевой алгебры, то есть нахождение корней такой системы может быть выполнено только методом перебора. Полный перебор при решении системы нелинейных булевых уравнений с n неизвестными предусматривает перебор всех 2^n вариантов входных наборов, подстановку их в уравнения системы до получения тождеств. Однако на практике, исходя их характерных особенностей булевых функций, составляющих уравнения систем (2) или (3), в большинстве случаев существуют возможности уменьшения объема перебора.

Рассмотрим подробнее методы решения систем нелинейных булевых уравнений. Наибольшее распространение [3] получили методы решения систем булевых уравнений, сочетающие аналитические методы с направленным перебором, который многократно может быть уменьшен за счет направленного использования результатов, полученных аналитически. Наиболее распространенным на практике методом является метод линейной аппроксимации. Суть его состоит в том, что каждая из нелинейных булевых функций, составляющих систему (1), заменяется на ближайшую по Хеммингу расстоянию линейную функцию. Таким образом, выполняется переход от системы (1) нелинейных булевых уравнений к системе линейных булевых уравнений:

$$(4)\quad \begin{aligned} \phi_1(x_1,...,x_n) &= y_1 \\ \phi_2(x_1,...,x_n) &= y_2 \\ &\cdots\cdots\cdots \\ \phi_h(x_1,...,x_n) &= y_h \end{aligned}$$

причем $\phi_j(x_1,...,x_n) = a_{0j} \oplus a_{1j}\cdot x_1 \oplus a_{2j}\cdot x_2 \oplus ... \oplus a_{nj}\cdot x_n$. Функция выбирается исходя из следующего условия:

$$(5)\quad \phi_j(x_1,...,x_n) = \min_{j} \sum_{\underline{x}\in Z} \phi_j(x_1,...,x_n) \oplus f_j(x_1,...,x_n)$$

Система (4) линейных булевых уравнений может быть решена аналитически и получен вектор $X_0 = \{x_{o1},...,x_{on}\}$. В соответствии с [2] истинное решение системы уравнений (1) следует искать перебором, начиная с вектора X_0, увеличивая постепенно в процессе перебора хеммингово расстояние от опорного вектора. Хеммингово расстояние между вектором решений системы (1) и (4) зависит от суммарной нелинейности всех булевых функций, входящих в систему (1), поэтому для того, чтобы увеличить перебор, необходимым представляется максимально увеличить суммарную нелинейность всех булевых функций, а для этого нелинейность каждой из булевых функций системы (1) должна быть максимальной. Если криптографический алгоритм недостаточно устойчив к аналитическим методам вскрытия, то уравнения эквивалентной ему системы булевых функций (1) обладают малой нелинейностью, и они могут быть заменены их линейными аппроксимациями, что в конечном итоге, позволит многократно уменьшить объем требуемого перебора и

решить задачу вскрытия за приемлемое время. В частности, широко известный DES-алгоритм был вскрыт [2] методами комбинированного использования линейной аппроксимации и направленного перебора с увеличивающимся хемминговым расстоянием. Для вскрытия методом линейной аппроксимации требуется, в среднем 2^{43} проб, в то время как полный перебор при вскрытии DES требует 2^{56} проб.

Другим, часто используемым в практике криптоанализа методом вскрытий алгоритмов защиты информации, является метод исключения переменных. Суть этого метода состоит в том, что проводится анализ значимости каждой из переменных в уравнениях и исключаются переменные с наименьшей значимостью. При этом значимость обычно оценивается статистически или с использованием теоретико-вероятностного подхода. После исключения мало значимых переменных достигается уменьшение размерности задачи решения системы булевых функций и, в дальнейшем она решается методами перебора или направленной аппроксимации или другими методами. Доказано [4], что полученное решение также может быть использовано в качестве базового и позволяет многократно уменьшить перебор.

Для повышения эффективности описанного метода решения систем уравнений необходимо, чтобы каждая из переменных была максимально значима, то есть вносила максимальное значение энтропии, или, что то же самое, после исключения любой переменной из функции $f(x_1,...,x_n)$ функция бы оставалась балансной. Это условие можно назвать условием максимума условной энтропии каждой из булевых функций, входящих в систему (1). Учитывая большую важность указанного критерия теории и практики криптографических систем защиты информации, этот критерий получил специальное название - критерия строго лавинного эффекта (Strict avalance criterion или сокращенно - SAC-критерий [4]).

Таким образом, для того, чтобы максимально усложнить решение эквивалентных систем булевых уравнений методами исключения переменных необходимо, чтобы каждая из булевых функций этой системы отвечала SAC-критерию. На практике криптоанализа исключение переменных и уменьшение размерности задачи выполняется чаще всего в сочетании с другими методами - в частности, в виде широко известного метода дифференциального криптоанализа [5].

Сам метод дифференциального криптоанализа также представляет собой по существу метод решения системы нелинейных булевых уравнений, основанный на вероятностной "реконструкции" булевых функций, составляющих систему. Дифференциальный криптоанализ не может быть использован прямо для решения системы нелинейных булевых уравнений системы (2) или (3), как математической задачи, то есть когда число уравнений ограничено h. На практике криптоанализа, как правило, в распоряжении стороны, выполняющей криптоанализ, имеется достаточно большое число блоков выходного сообщения, так, что число m уравнений значительно превышает h. Именно это обстоятельство позволяет в рамках метода дифференциального криптоанализа осуществлять вероятностное "реконструирование" булевой функции, при котором выполняется вероятностное определение неизвестных переменных. Причем, если булевы функции, составляющие систему - "слабы" в криптографическом плане, то есть исключение одной из переменных приводит к частной булевой функции, не обладающей максимумом энтропии, то есть принимающей единичные и нулевые значения не с равной вероятностью, что, собственно и позволяет выполнять определение вероятности того, что переменные равны 0 или 1 с вероятностью, отличной от 0.5, то метод "реконструкции" требует меньшего числа конкретных уравнений m, чем метод простого перебора. Таким образом, эффективность дифференциального криптоанализа определяется видом булевых функций, составляющих систему (1): если эти функции обладают максимумом полной и условной энтропии, то вычислительные его затраты приближаются к полному перебору.

Еще один способ решения систем нелинейных булевых уравнений основан на уменьшении перебора за счет статистического анализа выходного вектора шифроблока. Для обеспечения минимальной эффективности этого метода вскрытия необходимо, чтобы каждый из разрядов выходного кода с равной вероятностью принимал значение нуля или единицы при любом входном коде. Другими словами, для защиты от статистических методов решения систем булевых уравнений необходимо, чтобы каждая из булевых функций эквивалентной криптографическому алгоритму системы обладала максимумом полной энтропии или, что то же самое, была балансной принимала единичное значение на ровно половине возможных наборов переменных.

Решение систем булевых уравнений может быть упрощено, если булевы функции, составляющие систему (1), коррелированны.

Таким образом, проведенный анализ методов решения нелинейных булевых уравнений показывает, что:

- решение ни в коем случае не может быть выполнено полностью аналитическим путем и всегда предполагает использование перебора: в этом плане все рассмотренные методы по существу являются комбинированными, причем аналитическая их составляющая имеет целью уменьшение числа вариантов перебора;
- все рассмотренные выше аналитические методы вскрытия криптографических алгоритмов по существу являются, с учетом специфических условий криптоанализа, методами решения систем нелинейных булевых уравнений;
- сложность решения систем нелинейных булевых уравнений изложенными выше комбинированными методами полностью определяется наличием специфических свойств у булевых функций, составляющих систему (1).

Основным отличием задач вскрытия от математической задачи решения систем булевых уравнений является часто имеющаяся на практике возможность наличия не n попарно некоррелированных уравнений, где n-соотвествует числу неизвестных переменных, а иных ситуаций, при которых имеется m>>n уравнений, причем только n из них независимы [4].

Таким образом, обоснованным представляется вывод о том, что оценка сложности вскрытия криптографических алгоритмов аналитическими и комбинированными методами может быть выполнена через оценку сложности решения эквивалентной алгоритму системы булевых функций, которая, в свою очередь, может быть определена через наличие у булевых функций, составляющих эквивалентную алгоритму систему, специфических свойств. Если эти специфические свойства в полной мере присущи каждой из булевых функций, составляющих систему (1), то решение такой системы является максимально сложным в вычислительном плане: рассмотренные выше методы уменьшения перебора оказываются неэффективными и затраты времени при их использовании практически не отличаются от полного перебора. На практике эквивалентные алгоритму системы булевых функций в виду их громоздкости не могут быть получены и исследованы в явном виде, поэтому исследование наличия специфических свойств булевых функций предлагается осуществлять статистическими методами.

III Свойства булевых функций, влияющие на эффективность алгоритмов, и методики их определения

Проведенный выше анализ методов решения систем булевых уравнений показывает, что максимальная сложность решения достигается при выполнении следующих условий:

1. Каждая из булевых функций $f_i(x_1,...,x_n,k_1,...,k_r)$, $\forall$ i=1,...,h эквивалентной криптографическому симметричному алгоритму системы (1) должна обладать свойством максимальной полной энтропии, то есть быть балансной.

2. Каждая из булевых функций $f_i(x_1,...,x_n,k_1,...,k_r)$, $\forall$ i=1,...,h эквивалентной криптографическому алгоритму системы (1) должна обладать максимальной условной энтропией, то есть частная функция, получающаяся при исключении любой из переменных $x_1,...,x_n,k_1,...,k_r$ должна обладать максимумом энтропии, или, что то же самое, быть балансной.

3. Каждая из булевых функций $f_i(x_1,...,x_n,k_1,...,k_r)$, $\forall$ i=1,...,h эквивалентной криптографическому алгоритму системы (1) должна обладать максимальным значением нелинейности, то есть быть bent-функцией.

4. Булевы функции, составляющие эквивалентную криптографическому алгоритму систему (1), должны быть попарно некоррелированными или, что то же самое, булева функция $\zeta_{ij}(a,x_1,...,x_n,k_1,...,k_r) = a\cdot f_i(x_1,...,x_n,k_1,...,k_r) \oplus a\cdot f_j(x_1,...,x_n,k_1,...,k_r) \oplus f_j(x_1,...,x_n,k_1,...,k_r)$, $\forall$ j,i=1,..h, i≠j должна обладать максимумом условной энтропии по каждой из переменных, на которых она определена [4] .

5. Число h уравнений системы должно быть возможно большим, то есть возможно большей должна быть разрядность блоков, обрабатываемых криптографическим алгоритмом.

Таким образом, для оценки криптостойкости симметричных алгоритмов и необратимых алгоритмов предлагается исследовать эквивалентные этим алгоритмам системы булевых функций на предмет соответствия указанным выше критериям. Получение эквивалентных алгоритмам систем булевых функций в алгебраической нормальной форме (АНФ) принципиально может быть выполнено, однако такая форма представления функций требует технологически неприемлемо больших объемов памяти, поскольку АНФ булевых функций реальных алгоритмов содержит десятки тысяч термов. Поэтому для практического использования предложенного подхода более приемлемым является исследование криптографических свойств эквивалентных алгоритмам булевых функций статистическими методами.

Методика статистической проверки соответствия булевой функции SAC-критерию состоит в следующем:

1. Для h-й входной переменной (h=1,...,n) формируются случайным образом M пар наборов входных переменных $< X_j^{\,1}, X_j^{\,2} >$, j=1,...,M, таких, что наборы $X_j^{\,1}$ и $X_j^{\,2}$ отличны между собой значением h-той переменной.

2. Для каждой j-той пары вычисляется $t_j = F(X_j^{\,1}) \oplus F(X_j^{\,2})$. Накапливается сумма $U = t_1+t_2 +...+t_M$.

3. Вероятность P_h того, что функция соответствует SAC-критерию по h-той переменной определяется следующим образом:

$$P_h = 1- 2\cdot\Phi(|U-0.5\cdot M| / 0.5\cdot\sqrt{M}) \quad (6)$$

где Φ(...) - функция Лапласа.

4. Пункты 1-3 выполняются для каждой из n переменных, на которых определена булева функция.

Для криптографического алгоритма, который можно рассматривать как систему булевых функций, процедура статистического определения криптографических свойств несколько усложняется с тем, чтобы минимизировать затраты вычислительных ресурсов на исследование системы булевых функций.

Статистическое исследование балансности для каждого из выходных разрядов состоит в том, что для случайным образом генерируемого множества ключей $\Theta=\{K_1,K_2,...,K_m\}$ и множества данных $\Delta=\{M_1,M_2,...,M_k\}$ определяются статистические параметры каждого из выходных разрядов $\mathbf{y_i}$, i=1,...,n шифроблока.

Исследования криптографических свойств булевых функций криптографического преобразования могут быть проведены на множестве значений входных переменных, определяемых произведением множества возможных значений ключа и множества возможных значений данных. Однако при этом объем статистических исследований резко возрастает и достоверность полученных результатов падает. На практике при определении кода ключа при известных значениях входного кода данных и выходного кода, в качестве блока входных данных фиксируется известный входной блок информационного сообщения, а статистические исследования выполняются только на элементах множества Θ. Обозначим через N - количество элементов множества, на которых выполняется статистическое исследование. Если статистическое исследование криптографических свойств выполняется для произведения множеств ключа и данных, то N=mn, а если статистические исследования ведутся на множестве ключей, то N=m.

Статистическое исследование соответствия SAC-критерию булевых функций криптографических преобразований состоит в том, что для фиксированного набора входного информационного блока выбирается множество ϑ, состоящее из m пар значений ключевого слова $\vartheta=\{<K_{11},K_{12}>,<K_{21},K_2>,...,<K_{m1},K_{m2}>\}$, причем для каждой пары ключей выполняется условие:

$$\sum_{q=1,...,n} (k_{qi1} \oplus k_{qi2}) = 1 \qquad \forall\ i \in \{1,...,N\} \tag{7}$$

то есть ключевые слова, принадлежащие одной паре множества ϑ отличны между собой только в одном, t-том разряде. Тогда в качестве статистической оценки η_t соответствия булевой функции SAC-критерию по t-тому разряду можно использовать следующее выражение:

$$\eta_t = \sum \sum (f_t(X, K_{i1}) \oplus f_t(X, K_{i2})) / N \tag{8}$$

Если функция соответствует SAC-критерию, то с увеличением N величина η_t будет стремиться к 0.5. Теоретическое значение дисперсии величины η_t равно 0.25 и эта величина также может быть использована для статистического контроля соответствия булевых функций SAC-критерию.

По аналогии с предложенным способом статистической проверки факта соответствия SAC-критерию нулевого порядка, можно предложить метод статистической проверки факта соответствия SAC-критерию более высоких порядков. Для этого в состав множества ϑ пар ключей, подвергаемых анализу, должны подбираться коды, отличающиеся в u разрядах.

Статистическое исследование нелинейности булевых функций требует существенно больших затрат вычислительных ресурсов по сравнению с определением балансности и соответствия SAC-критерию.

Предложенный подход и изложенная выше методика были практически опробованы при исследовании широко используемых алгоритмов DES, ГОСТ 28147-89, SHA-1. Полученные результаты достаточно хорошо согласуются с результатами исследования этих алгоритмов с использованием других частных методов [1,3,4]. Ниже приведены результаты исследования SAC-свойств булевых функций, эквивалентных DES-алгоритму.

Для экспериментальных исследований была написана специальная программа, в которой процедура, реализующая шифроблок DES написан на языке Ассемблере для возможности проведения широкомасштабных статистических исследований в приемлемое время.

Для статистического определения соответствия булевых функций битовых преобразований DES была выполнена генерация 10 случайно выбираемых входных 64-разрядных кодов и для каждого из этих кодов осуществлена генерация 50000 пар $<G_1,G_2>$ выборок ключей, где G_1 и G_2 - случайно выбираемые ключи, отличные только в одном случайно выбираемом разряде. При фиксированном коде на информационном входе шифроблока для каждой пары $<G_1,G_2>$ ключей выполнялось вычисление пары $< C_1,C_2>$ кодов зашифрованного представления кодов. Далее вычислялось число разрядов, в которых коды $C_1=\{c_{11},c_{12},...,c_{1\ 64}\}$ и $C2=\{c21,c22,...,c_{2\ 64}\}$ отличаются друг от друга (то есть расстояние по Хеммингу между кодами C_1 и C_2) . Таким образом, для j-той пары η_j определяется в виде:

$$\eta_j = \sum_{i=1,\ldots,64} (c_{1i} \oplus c_{2i}) \quad (9)$$

В рамках проведенных статистических исследований выполнено вычисление математического ожидания $\mu(\eta)$ и дисперсии $D(\eta)$. Теоретически, если булевы функции битового преобразования, реализованные в DES, удовлетворяют критерию SAC, то $\mu(\eta)\rightarrow 32$, а $D(\eta)\rightarrow 0.5$. Данные о полученных значениях математического ожидания и дисперсии для 10 значений входных блоков сведены в таблицу 1.

Таблица 1.

Номер входного блока	Математическое ожидание $\mu(\eta)$	Дисперсия $D(\eta)$
1	32.04	0.56
2	32.11	0.48
3	31.89	0.49
4	31.91	0.54
5	32.12	0.61
6	32.03	0.47
7	31.96	0.52
8	31.92	0.43
9	32.07	0.59
10	32.03	0.61

Приведенные в таблице данные свидетельствуют о том, что булевы функции, эквивалентные DES, практически соответствуют критерию строго лавинного эффекта, в отличие от булевых функций, эквивалентных алгоритму ГОСТ 28147-89.

IV Выводы

Основным результатом проведенных исследований является обоснование и разработка достаточно общего для широкого класса алгоритмов защиты информации подхода к оценки их эффективности через определение специфических критериев выполняемых в алгоритмах битовых преобразований. Разработана и практически опробована методика статистического исследования эквивалентных алгоритмам булевых преобразований. Анализ экспериментально полученных результатов для алгоритмов DES, ГОСТ 28147-89, SHA-1 показывает, что они достаточно хорошо согласуются с результатами ранее проведенных исследований криптостойкости этих алгоритмов,

Следует специально отметить, что предложенный подход в полной мере применим к оценке устойчивости к вскрытиям достаточно широкого класса криптографических алгоритмов, который включает симметричные обратимые алгоритмы и необратимые алгоритмы формирования хеш-сигнатур. Что касается большинства несимметричных криптографических алгоритмов, то в их основе лежат иные трудно решаемые математические задачи и к ним предложенный метод неприменим.

Предложенный подход и методики могут быть использованы при сертификации создаваемых и вводимых алгоритмов криптографической защиты информации, в основе которых лежат битовые преобразования.

Литература: 1. Coppersmith D. The Data Encryption Standard (DES) and its Strength against attacks. IBM Jornal of Research and Development, Vol.38, No.3, pp.243-246, 1994. 2. Matsui M., Linear Cryptanalysis Method for DES Cipher, Proceedings of EUROCRYPT '93, Spriger-Varlag, Vol.765, pp.386-397 , 1994. 3. Pippenger N. Entropy and Enumeration of Boolean function. IEEE Transactions and information theory, vol.45, no.6, pp. 2096-2100, 1999. 4. Saberry J, Zhang X.M., Zheng Y. Nonlinearity and propagation characteristics of balanced Boolean functions. Inform.Comput., vol.119, no.1, pp.1-13, 1995. 5. Schneier B. Applied Cryptography. Protocols. Algorithms and Source codes in C. Ed.John Wiley, p.758. 1996.