МАТЕМАТИЧЕСКИЕ МЕТОДЫ КРИПТОГРАФИИ

DOI 10.17223/20710410/1/7

УДК 519.7

ЭЛЕМЕНТЫ ТЕОРИИ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ С АДДИТИВНЫМ РАУНДОВЫМ КЛЮЧОМ

Г.П. Агибалов

Томский государственный университет

E-mail: agibalov@isc.tsu.ru

Метод дифференциального криптоанализа излагается в общем виде применительно к произвольным итеративным блочным шифрам, в которых блок открытого текста преобразуется в блок шифртекста за несколько раундов с использованием на каждом раунде одной и той же операции преобразования, осуществляемой в зависимости от аддитивного раундового ключа. Для этого вводятся необходимые элементы теории функций на конечных абелевых группах, определяется класс рассматриваемых шифров, устанавливаются необходимые вспомогательные предложения и формулируется алгоритм метода, сочетающий применение дифференциальной характеристики и решение системы полиномиальных уравнений над конечным полем. Все построения иллюстрируются на примере DES.

Ключевые слова: *дифференциальный криптоанализ*, *итеративные блочные шифры*, *функции на конечных абелевых группах*, *полиномиальные уравнения над конечным полем.*

Применительно к шифрам, а здесь мы говорим только о них, дифференциальный криптоанализ используется для построения атак с выбором открытого текста, имеющих целью (полное или частичное) раскрытие ключа шифра. Его название происходит от английского difference – разность и связано с тем, что в нем рассматриваются зависимости не между открытыми и шифртекстами, а между разностями пар открытых текстов и разностями пар соответствующих шифртекстов при фиксированном неизвестном ключе. Со времени выхода в свет первых работ по дифференциальному криптоанализу [1 – 3] появились десятки, если не сотни, публикаций, в которых предлагаются конкретные атаки на конкретные шифры (или другие криптосистемы), разработанные на основе этой его идеи. К сожалению, автору не известно ни одной работы, которая содержала бы изложение дифференциального криптоанализа как метода в общем виде, а именно так, как это принято в вычислительной математике – с определением основных его понятий, с формулировкой и доказательством его базовых теорем, с определением классов шифров, к которым он применим, с формулировкой его алгоритма для какого-либо из этих классов или, хотя бы, четких правил (технологии) разработки такого алгоритма. Ничего подобного, к сожалению, на данный момент в криптографии нет. Известные атаки дифференциального криптоанализа на конкретные шифры носят совершенно частный характер и неприменимы к другим шифрам, даже близким по классу.

В данной работе предпринимается попытка хотя бы частично восполнить этот пробел. Здесь мы рассматриваем дифференциальный криптоанализ применительно к произвольным итеративным блочным шифрам, в которых блок открытого текста преобразуется в блок шифртекста за несколько раундов с применением на каждом раунде одной и той же операции преобразования, осуществляемой в зависимости от аддитивного раундового ключа. Изложению метода в общем виде предшествуют введение необходимых элементов теории функций на конечных абелевых группах, определение класса рассматриваемых шифров, их классификация по свойствам раундовой функции, установление необходимых вспомогательных предложений, а также формулировка альтернативного метода для одного частного случая, а именно для шифров с функцией раунда, разделимой по Фейстелю. Этот частный метод основан на теореме об аддитивном раундовом ключе и фактически повторяет классический подход дифференциального криптоанализа к DES с присущими ему недостатками. Общий же метод дифференциального криптоанализа, сформулированный здесь как алгоритм для всех итеративных блочных шифров с аддитивным раундовым ключом, в своей основе сводится к решению системы полиномиальных уравнений над конечным полем для последнего раунда шифра с известными значениями на его выходе, с известной с ненулевой вероятностью разностью значений на его входе, с неизвестными компонентами раундового ключа и с неизвестными значениями на его входе. Для r-раундового шифра разность на входе r-го раунда берется из $(r-1)$-раундовой характеристики этого шифра. Все построения общего характера иллюстрируются на примере DES, взятого без операций начальной и заключи-

тельной перестановок и без расписания раундовых ключей. Решение систем полиномиальных уравнений над конечным полем и построение многораундовых вероятностных характеристик шифров составляют предмет самостоятельных исследований и в работе не рассматриваются.

Справедливости ради следует заметить, что попытки построения теории дифференциального криптоанализа предпринимались и ранее его авторами в [1, 2] и Д.Р. Стинсоном в его замечательной монографии [4], однако эти попытки ограничились рассмотрением только класса DES-подобных шифров и не привели к созданию единого алгоритма их дифференциального криптоанализа.

1. Функции на конечных абелевых группах

Будем рассматривать функции, которые, как и их аргументы, принимают значения в конечных абелевых группах. Некоторые из независимых переменных, от которых могут зависеть рассматриваемые функции, играют особую роль и называются параметрами. Их особая роль заключается в выборе подфункций заданной функции путем фиксации их значений под знаком функции. Для функций шифрования, например, в роли параметров выступают компоненты ключа. Функция, среди аргументов которой имеются или отсутствуют параметры, называется функцией с параметром или без соответственно. Впредь, в отсутствие специальных оговорок, под функцией подразумевается функция без параметров. Условимся также значения переменных функции, не являющихся параметрами, и значения самой функции называть значениями соответственно на ее входе и на ее выходе. Для простоты записи во всех рассматриваемых группах операция сложения в отсутствие дополнительных оговорок обозначается одинаково – символом +.

Пусть далее A, B и I суть конечные абелевы группы, $t = |A|$, $h: A \to B$ есть функция без параметра и $\eta: A \times I \to B$ есть функция с параметром, принимающим значения в I. Будем представлять последнюю системой функций без параметра – ее подфункций $\eta_i: A \to B$, $i \in I$, где $\eta_i(u) = \eta(u, i)$ для всех $u \in A$ и $i \in I$.

Назовем *разностным множеством* функции h любое множество $D_h(a, b) = \{u \in A: h(u) - h(u - a) = b\}$ для $a \in A$ и $b \in B$. Это название обязано тому, что здесь a есть разность $u - u^*$ элементов u и $u^* = u - a$ на входе h, а b – разность $h(u) - h(u^*)$ соответствующих значений на выходе h. По определению, $D_h(a, b)$ есть множество всех тех значений u аргумента функции h, изменение которых на величину a (т.е. с u на $u^* = u - a$) вызывает изменение значения h на величину b (с $h(u)$ на $h(u^*) = h(u) - b$).

Назовем *тестовым множеством* функции $h: A \to B$ любое множество $T_h(v, v^*, b) = \{d - v: d \in D_h(a, b)\}$ для v, v^* в A, b в B и $a = v - v^*$.

Теорема 1. Для любых v, v^*, k в A и $b \in B$ если $b = h(v + k) - h(v^* + k)$, то $k \in T_h(v, v^*, b)$.

Доказательство. Пусть $a = v - v^*$. Тогда $b = h(v + k) - h(v^* + k) = h(v + k) - h(v + k - a)$, $v + k \in D_h(a, b)$ и $k = (v + k) - v \in T_h(v, v^*, b)$. ■

Ввиду $b \neq b' \Rightarrow D_h(a, b) \cap D_h(a, b') = \varnothing$, при любом $a \in A$ все непустые разностные множества $D_h(a, b)$, $b \in B$, образуют разбиение множества A, и функция $p_h(b|a)$ от b, задаваемая равенством $p_h(b|a) = t^{-1}|D_h(a, b)|$, является распределением вероятностей на B. Ее значение для конкретного $b \in B$ есть вероятность того, что для случайного (т.е. выбранного с вероятностью t^{-1}) u в A и для $u^* = u - a$ будет $h(u) - h(u^*) = b$. Будем называть $p_h(b|a)$ *вероятностью разности b на выходе функции h при условии, что разность на ее входе равна a*.

Если ввести $Q(a) = \{(u, u^*) \in A^2: u - u^* = a\}$ и $Q_h(a, b) = \{(u, u^*) \in A^2: u - u^* = a, h(u) - h(u^*) = b\}$, то легко заметить, что $|Q(a)| = t$, $|Q_h(a, b)| = |D_h(a, b)|$ и, следовательно, $p_h(b|a) = |Q_h(a, b)| / |Q(a)|$, т.е. $p_h(b|a)$ – это доля упорядоченных пар наборов на входе h с фиксированной разностью a, соответствующие которым наборы на выходе h имеют разность b.

Для функции с параметром $\eta: A \times I \to B$, для каждого значения ее параметра $i \in I$, имея $a \in A$ и $b \in B$, можно вычислить $D_{\eta_i}(a, b) = \{u \in A: \eta_i(u) - \eta_i(u - a) = b\}$ и $p_{\eta_i}(b \mid a) = t^{-1} | D_{\eta_i}(a, b)|$. Величину $p_{\eta_i}(b \mid a)$ естественно обозначать $p_\eta(b \mid a, i)$ и называть вероятностью разности b на выходе функции η при условии, что разность на ее входе равна a и ее параметр имеет значение i.

Будем называть η *функцией с аддитивным параметром* (в I), если существуют функции $\varphi: A \to I$ и $\psi: A \times I \to B$, такие, что φ – гомоморфизм групп и $\eta(u, i) = \psi(u, \varphi(u) + i)$ для любых $u \in A$ и $i \in I$; в этом случае пишем $\eta = [\psi, \varphi]$.

Функцию $\eta = [\psi, \varphi]$ называем функцией *с ветвлением* или *без ветвления входа*, если в ней $\psi(u, i)$ зависит от аргумента u существенно или фиктивно соответственно; в последнем случае вместо $\psi(u, i)$ пишем $\psi(i)$ и имеем $\eta(u, i) = \psi(\varphi(u) + i)$ для всех $u \in A$ и $i \in I$. Функция $\eta = [\psi, \varphi]$ называется *разделимой*, если $A = A' \times A''$, $B = B' \times B''$ для некоторых абелевых групп A', A'', B', B'', $\varphi(u) = \varepsilon(R)$, $\psi(u, j) = (\lambda(R), \rho(L, j))$ для некоторых функций $\varepsilon: A'' \to I$, $\lambda: A'' \to B'$, $\rho: A' \times I \to B''$ и любых $u = LR \in A' \times A''$ и $j \in I$; в этом случае для всех $u = LR \in A' \times A''$ имеем $\eta(u, i) = [\psi, \varphi](LR, i) = \psi(LR, \varphi(LR) + i) = (\lambda(R), \rho(L, \varepsilon(R) + i))$ и пишем $\eta = [\lambda, \rho, \varepsilon]$. По определению, здесь ε – гомоморфизм групп. Функция $\eta = [\lambda, \rho, \varepsilon]$ называется *разделимой по Фейстелю*, если $A'' = B'$, λ – тождественная функция, $A' = B''$ и $\rho(L, j) = L + \delta(j)$ для некоторой функции $\delta: I \to A'$ и любых $L \in A'$ и $j \in I$; в этом случае имеем $\eta(LR, i) = (R, L + \delta(\varepsilon(R) + i))$ и пишем $\eta = \langle \delta, \varepsilon \rangle$.

Теорема 2. Если $\eta = [\psi, \varphi]$, то $\forall i \in I(p_\eta(b \mid a, i) = p_\psi(b \mid a\varphi(a))$.

Доказательство. Имеем $\eta_i(u) = \eta(u, i) = \psi(u, \varphi(u) + i)$. Пусть $a = u - u^*$. Тогда ввиду гомоморфности φ можно записать $p_{\eta_i}(b \mid a) = p_{\eta_i}(b \mid u - u^*) = p_\psi(b \mid (u, \varphi(u)+i) - (u^*, \varphi(u^*)+i) = p_\psi(b \mid a\varphi(u - u^*)) = p_\psi(b \mid a\varphi(a))$. ■

Таким образом, для функции с аддитивным параметром вероятность разности на ее выходе определяется однозначно разностью на ее входе и не зависит от значения ее параметра.

Следствие 1. Для функции $\eta = [\psi, \varphi]$ без ветвления входа $\forall i \in I(p_\eta(b \mid a, i) = p_\psi(b \mid \varphi(a))$.

Следствие 2. Для функции $\eta = [\lambda, \rho, \varepsilon]$ с тождественной компонентой λ если $a = a'a'' \in A' \times A''$ и $b = b'b'' \in B' \times B''$, то $\forall i \in I(p_\eta(b \mid a, i) = p_\rho(b'' \mid a''\varepsilon(a''))$. В частности, для функции η, разделимой по Фейстелю, т.е. для $\eta = \langle\delta, \varepsilon\rangle$ будет $\forall i \in I(p_\eta(b \mid a, i) = p_\delta(b'' - a' \mid \varepsilon(a''))$.

2. Итеративные блочные шифры

Пусть далее m, n и r суть натуральные числа, обозначающие соответственно длину раундового ключа, длину блока шифра и количество раундов, $K = \{0, 1\}^m$, $X = \{0, 1\}^n$ и $Y = \{0, 1\}^n$ – множества соответственно раундовых ключей, блоков открытых текстов и блоков шифртекстов. Пусть также $U = \{0, 1\}^n$ и g: $U \times K \to U$ – произвольная функция со свойством *обратимости*: для любых u, v в U и k в K если $u \neq v$, то $g(u, k) \neq g(v, k)$. Это свойство позволяет ввести функцию g^{-1}: $U \times K \to U$ как $g^{-1}(u, k) = v$, если $g(v, k) = u$. Определим также функцию G: $X \times K^r \to Y$, положив $G(x, k_1 \ldots k_r) = y$, где y вычисляется итеративно как $y = u_r$, $u_i = g(u_{i-1}, k_i)$, $i = 1, 2, \ldots, r$ и $u_0 = x$. Назовем ее функцией *r-раундового шифрования*. Под ее знаком k_i называется (*раундовым*) *ключом i-го раунда*. Она обратима: $G(x, k_1 \ldots k_r) = y \Rightarrow x = G^{-1}(y, k_1 \ldots k_r)$, где $G^{-1}(y, k_1 \ldots k_r) = u_0$, $u_{i-1} = g^{-1}(u_i, k_i)$, $i = r, r-1, \ldots, 1$ и $u_r = y$. Вместе с множествами K, X, Y и *обращением* G^{-1} она образует *r-раундовый итеративный блочный шифр* $C = (X, Y, K^r, G, G^{-1})$. Функция g называется функцией *раундового шифрования*, или, для краткости, *раундом* этого шифра.

Пример 1. Классическим примером итеративного блочного шифра является DES (без операций начальной и заключительной перестановок и без расписания раундовых ключей). В нем $n = 64$, $m = 48$, $r = 16$, $U = \{0, 1\}^{32} \times \{0, 1\}^{32}$, $g = (g', g'')$, g': $U \times K \to \{0, 1\}^{32}$, $g'(LR, k) = R$, g'': $U \times K \to \{0, 1\}^{32}$, $g''(LR, k) = L \oplus f(R, k)$, f: $\{0, 1\}^{32} \times K \to \{0, 1\}^{32}$, $f(R, k) = P(S(E(R) \oplus k))$, E: $\{0, 1\}^{32} \to \{0, 1\}^{48}$, S: $\{0, 1\}^{48} \to \{0, 1\}^{32}$, P: $\{0, 1\}^{32} \to \{0, 1\}^{32}$, $\oplus$ – покомпонентное сложение булевых векторов по модулю 2 и E, S, P – операции соответственно расширения, замены и перестановки в раунде DES.

3. Шифры с аддитивным раундовым ключом

Обратим внимание на следующее существенное свойство функции раундового шифрования DES: в ее выражение раундовый ключ входит аддитивно с инъективным образом шифруемого блока, вследствие чего ее значение определяется фактически не блоком и раундовым ключом, взятыми отдельно, но их суммой с операцией сложения ($\oplus$), которая на множестве раундовых ключей определяет структуру аддитивной абелевой группы. Это свойство присуще функциям раундового шифрования большинства современных итеративных блочных шифров, с той лишь разницей, что групповая операция сложения на множестве раундовых ключей в них может отличаться от $\oplus$. Например, в российском шифре ГОСТ 28147-89 в качестве таковой выступает сложение раундовых ключей как целых чисел по модулю 2^{32}. Впредь итеративные блочные шифры, в которых функция раундового шифрования обладает указанным свойством, мы называем шифрами с аддитивным раундовым ключом. Ниже следует их строгое определение.

Предполагая множества U и K аддитивными абелевыми группами, назовем функцию g: $U \times K \to U$ и итеративный блочный шифр C с функцией раундового шифрования g соответственно *функцией* и *шифром с аддитивным раундовым ключом*, если g есть функция с аддитивным параметром в K, т.е. если $g = [\psi, \varphi]$ для некоторых φ: $U \to K$ и ψ: $U \times K \to U$ и, следовательно, $g(u, k) = \psi(u, \varphi(u) + k)$.

Пример. Функция g раундового шифрования в DES является функцией с аддитивным раундовым ключом, разделимой по Фейстелю. Действительно, для нее $g(LR, k) = (R, (L + P(S(E(R) + k))))$, поэтому $g = [\psi, \varphi]$, где $\varphi(LR) = E(R)$, $\psi(LR, j) = (R, P(S(j)))$ для всех $LR \in U$ и $j \in K$, и, кроме того, $g = \langle\delta, \varepsilon\rangle$, где $\delta(j) = P(S(j))$ и $\varepsilon(R) = E(R)$ для всех $j \in K$ и $R \in \{0, 1\}^{32}$.

Следующая теорема является одной из основ для дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом.

Теорема 3 (об аддитивном раундовом ключе). Для функции раундового шифрования $g = [\psi, \varphi]$: $U \times K \to U$ с аддитивным ключом в K, для любых u, u^* в U, $k \in K$ и $b \in U$ если $b = g(u,k) - g(u^*,k)$, то $0k \in T_\psi(u\varphi(u), u^*\varphi(u^*), b)$.

Доказательство. Имеем $b = \psi(u\varphi(u) + 0k) - \psi(u^*\varphi(u^*) + 0k)$, и требуемое утверждение получаем по теореме 1 при $A = U \times K$, $B = U$, $h = \psi$, $v = u\varphi(u)$, $v^* = u^*\varphi(u^*)$. ■

В случае, если функция $[\psi, \varphi]$ не имеет ветвления входа, это утверждение принимает следующий вид.

Следствие 1 (теорема об аддитивном ключе раунда без ветвления входа). Для функции раундового шифрования $g = [\psi, \varphi]$: $U \times K \to U$ с аддитивным ключом в K и без ветвления входа, для любых u, u^* в U, $k \in K$ и $b \in U$ если $b = g(u, k) - g(u^*, k)$, то $k \in T_\psi(\varphi(u), \varphi(u^*), b)$. ■

Следствие 2 (теорема об аддитивном ключе раунда с разделимой функцией). Для разделимой функции раундового шифрования $g = [\lambda, \rho, \varepsilon]$: $U \times K \to U$, где $U = U' \times U''$, ε: $U'' \to K$, λ: $U'' \to U'$, ρ: $U' \times K \to U''$, для любых L, L^* в U', R, R^* в U'', $u = LR$, $u^* = L^*R^*$, $k \in K$, $b' \in U'$, $b'' \in U''$ и $b = b'b''$ если $b = g(u, k) - g(u^*, k)$, то $0k \in T_\rho(L\varepsilon(R), L^*\varepsilon(R^*), b'')$. ■

Назовем раундом Фейстеля раунд с аддитивной функцией шифрования, разделимой по Фейстелю.

Следствие 3 (теорема об аддитивном ключе раунда Фейстеля). Для разделимой по Фейстелю функции раундового шифрования $g = \langle\delta, \varepsilon\rangle$: $U \times K \to U$, где $U = U' \times U'$, ε: $U' \to K$, δ: $K \to U'$, для любых L, L^*, R, R^* в U', $L' = L - L^*$, $u = LR$, $u^* = L^*R^*$, $k \in K$, $b' \in U'$, $b'' \in U'$, $b = b'b''$ и $b_1 \in U'$ если $b = g(u, k) - g(u^*, k)$ и $b_1 = b'' - L'$, то $k \in T_\delta(\varepsilon(R), \varepsilon(R^*), b_1)$. ■

Следствие 4 (теорема об аддитивном ключе раунда DES). Для функции g раундового шифрования DES в обозначениях из следствия 3 если $b = g(u, k) - g(u^*, k)$ и $b_1 = P^{-1}(b'' - L')$, то $k \in T_S(\varepsilon(R), \varepsilon(R^*), b_1)$. ■

Положим $\psi_w(j) = \psi(w, j)$ для всех $w \in U$ и $j \in K$.

Теорема 4. Для функции раундового шифрования $[\psi, \varphi]$: $U \times K \to U$ с аддитивным ключом в K, для любых w, u, u^* в U, k в K и $b \in U$ если $b = \psi_w(\varphi(u) + k) - \psi_w(\varphi(u^*) + k)$, то $k \in T_{\psi_w}(\varphi(u), \varphi(u^*), b)$.

Доказательство. Утверждение следует непосредственно из теоремы 1 при $A = K$, $B = U$, $h = \psi_w$, $v = \varphi(u)$, $v^* = \varphi(u^*)$. ■

Обратим внимание на то, что в теореме 4, в отличие от теоремы 3 и ее следствий, величина b не обязана быть разностью $g(u, k) - g(u^*, k)$ на выходе раунда, что открывает дополнительные возможности для дифференциального криптоанализа. Изучение этих возможностей, однако, выходит за пределы настоящей работы.

4. Дифференциальный криптоанализ одного раунда с аддитивным ключом

Согласно теореме 3, если раундом $g = [\psi, \varphi]$ с аддитивным раундовым ключом k некоторые блоки u, u^* на входе раунда зашифровываются в блоки на его выходе, разность которых равна b, то вектор $0k$ с искомым ключом k принадлежит тестовому множеству $T_\psi(u\varphi(u), u^*\varphi(u^*), b)$ и может быть найден в результате пересечения нескольких таких множеств, построенных для различных пар блоков на входе раунда. В этом, собственно, и состоит дифференциальный криптоанализ любого 1-раундового блочного шифра подобного рода. Более детально алгоритм такого криптоанализа с целью нахождения раундового ключа выглядит следующим образом.

Алгоритм A_1. Последовательно выбираются пары блоков открытого текста и для каждой выбранной пары (u_t, u_t^*), $t = 1, 2, \ldots$, и соответствующей пары $(g(u_t, k), g(u_t^*, k))$ блоков шифртекста на выходе раунда вычисляются образы $\varphi(u_t)$, $\varphi(u_t^*)$, разности $a_t = u_t\varphi(u_t) - u_t^*\varphi(u_t^*)$ и $b_t = g(u_t, k) - g(u_t^*, k)$, разностное множество $D_\psi(a_t, b_t) = \{0v: v \in K, \psi(0v) - \psi(0v - a_t) = b_t\}$ и тестовое множество $T_t = T_\psi(u_t\varphi(u_t), u_t^*\varphi(u_t^*), b_t) = \{d - u_t\varphi(u_t): d \in D_\psi(a_t, b_t)\}$. Строится пересечение Q тестовых множеств T_t для всех рассматриваемых t. С получением одноэлементного Q процесс заканчивается с результатом k, где $\{0k\} = Q$. Процесс может быть остановлен и при несколько более слабом условии, а именно с получением тестовых множеств, в которых некоторый один элемент $0k$ встречается много чаще других. Часть k в нем и выдается за результат криптоанализа – искомый раундовый ключ.

Очевидным образом данный алгоритм переформулируется на любой из частных случаев раунда, представленных следствиями 1 – 4 из теоремы 3.

В реальных шифрах компоненты ψ и φ функции раундового шифрования $g = [\psi, \varphi]$ строятся обычно в виде суперпозиции некоторых более простых функций, допуская, в частности, возможность эффективного вычисления требуемых для алгоритма разностных и тестовых множеств. Ниже эта возможность демонстрируется на примере DES.

5. Пример: дифференциальный криптоанализ 1- и 3-раундовых DES

Пусть далее L_0R_0, $L_0^*R_0^*$ – два блока открытого текста на входе 1-го раунда DES и для i-го раунда DES с $i \geq 1$:

k_i – фиксированный раундовый ключ,

L_iR_i, $L_i^*R_i^*$ – два блока шифртекста на выходе раунда,

$e_i = E(R_{i-1})$, $e_i^* = E(R_{i-1}^*)$, $x_i = e_i \oplus k_i$, $x_i^* = e_i^* \oplus k_i$, $c_i = S(x_i)$, $c_i^* = S(x_i^*)$, $e_{i1}e_{i2}\ldots e_{i8} = e_i$, $e_{i1}^* e_{i2}^* \ldots e_{i8}^* = e_i^*$, $k_{i1}k_{i2}\ldots k_{i8} = k_i$, $(S_1, S_2, \ldots, S_8) = S$, S_j: $\{0, 1\}^6 \to \{0,1\}^4$, $|e_{ij}| = |e_{ij}^*| = |k_{ij}| = 6$, $e_{ij}' = e_{ij} \oplus e_{ij}^*$, $j = 1, 2, \ldots, 8$.

Таким образом, по определению DES, $L_i = R_{i-1}$, $L_i^* = R_{i-1}^*$, $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$, $R_i^* = L_{i-1}^* \oplus f(R_{i-1}^*, k_i)$, $P(c_i) = f(R_{i-1}, k_i)$ и $P(c_i^*) = f(R_{i-1}^*, k_i)$ для $i = 1, 2, \ldots, 16$.

Пусть также $L_i'R_i' = L_iR_i \oplus L_i^*R_i^*$ для $i = 0, 1, \ldots, 16$. Очевидно, здесь $L_i' = R_{i-1}'$ для $i \geq 1$.

Криптоанализ 1-раундового DES

Имеем: $R_1 = L_0 \oplus f(R_0, k_1)$, $R_1^* = L_0^* \oplus f(R_0^*, k_1)$, $R_1' = R_1 \oplus R_1^* = L_0 \oplus L_0^* \oplus f(R_0, k_1) \oplus f(R_0^*, k_1) = L_0' \oplus f(R_0, k_1) \oplus f(R_0^*, k_1) = L_0' \oplus P(c_1) \oplus P(c_1^*) = L_0' \oplus P(c_1 \oplus c_1^*)$, $L_0' \oplus R_1' = P(c_1 \oplus c_1^*)$. Положим $b = P^{-1}(L_0' \oplus R_1')$. Тогда $b = c_1 \oplus c_1^* = S(x_1) \oplus S(x_1^*)$ и по следствию 4 из теоремы 3 $k_1 \in T_S(e_1, e_1^*, b)$ для $e_1 = E(R_0)$, $e_1^* = E(R_0^*)$.

Отсюда – следующий алгоритм криптоанализа 1-раундового DES. Последовательно выбираются пары блоков открытого текста и для каждой такой пары $(L_0R_0, L_0^*R_0^*)$ и соответствующей пары блоков шифртекста $(L_1R_1, L_1^*R_1^*)$ вычисляются $e_1 = E(R_0)$, $e_1^* = E(R_0^*)$, $L_0' = L_0 \oplus L_0^*$, $R_1' = R_1 \oplus R_1^*$, $b = P^{-1}(L_0' \oplus R_1')$, $b_1b_2\ldots b_8 = b$, где $|b_1| = \ldots = |b_8| = 4$, разностные множества $D_{S_j}(e_{1j}', b_j)$ и тестовые множества $T_j = T_{S_j}(e_{1j}, e_{1j}^*, b_j) = \{d - e_{1j} : d \in D_{S_j}(e_{1j}', b_j)\}$ для $j = 1, 2, \ldots, 8$. Для каждого такого j строится пересечение Q_j тестовых множеств T_j, вычисленных так для всех выбранных пар блоков открытого текста. С получением одноэлементных Q_j для всех j процесс заканчивается с результатом $k_1 = k_{11}k_{12}\ldots k_{18}$, где $\{k_{1j}\} = Q_j$, $j = 1, 2, \ldots, 8$.

Криптоанализ 3-раундового DES [4]

Цель атаки – найти раундовый ключ k_3.

Имеем: $R_3 = L_2 \oplus f(R_2, k_3) = R_1 \oplus f(R_2, k_3) = L_0 \oplus f(R_0, k_1) \oplus f(R_2, k_3)$ и, аналогично, $R_1^* = L_0^* \oplus f(R_0^*, k_1) \oplus f(R_2^*, k_3)$, поэтому $R_3' = L_0' \oplus f(R_0, k_1) \oplus f(R_2, k_3) \oplus f(R_0^*, k_1) \oplus f(R_2^*, k_3)$. Выберем $R_0 = R_0^*$. Тогда $R_3' = L_0' \oplus f(R_2, k_3) \oplus f(R_2^*, k_3)$, $R_3' \oplus L_0' = f(R_2, k_3) \oplus f(R_2^*, k_3) = P(c_3) \oplus P(c_3^*) = P(c_3 \oplus c_3^*)$. Пусть $b = P^{-1}(L_0' \oplus R_3')$. Тогда $b = c_3 \oplus c_3^* = S(x_3) \oplus S(x_3^*)$ и по теореме 1 $k_3 \in T_S(e_3, e_3^*, b)$. Здесь $R_2 = L_3$, $R_2^* = L_3^*$, поэтому $e_3 = E(L_3)$, $e_3^* = E(L_3^*)$.

Отсюда – следующий алгоритм криптоанализа 3-раундового DES. Последовательно выбираются пары блоков открытого текста $(L_0R_0, L_0^*R_0^*)$, где $R_0 = R_0^*$, и для каждой такой пары и соответствующей пары блоков шифртекста $(L_3R_3, L_3^*R_3^*)$ вычисляются $e_3 = E(L_3)$, $e_3^* = E(L_3^*)$, $L_0' = L_0 \oplus L_0^*$, $R_3' = R_3 \oplus R_3^*$, $b = P^{-1}(L_0' \oplus R_3')$, $b_1b_2\ldots b_8 = b$, где $|b_1| = \ldots = |b_8| = 4$, разностные множества $D_{S_j}(e_{3j}', b_j)$ и тестовые множества $T_j = T_{S_j}(e_{3j}, e_{3j}^*, b_j) = \{d - e_{3j} : d \in D_{S_j}(e_{3j}', b_j)\}$ для $j = 1, 2, \ldots, 8$. Для каждого такого j строится пересечение Q_j тестовых множеств T_j, вычисленных так для всех выбранных пар блоков открытого текста. С получением одноэлементных Q_j для всех j процесс заканчивается с результатом $k_3 = k_{31}k_{32}\ldots k_{38}$, где $\{k_{3j}\} = Q_j$, $j = 1, 2, \ldots, 8$.

6. Вероятность разности на выходе раунда с аддитивным ключом

В соответствии с теоремой 2 вероятность $p_g(b \mid a, k)$ разности b на выходе раунда $g = [\psi, \varphi]$ с фиксированными разностью a на его входе и аддитивным раундовым ключом k не зависит от последнего и равна $p_\psi(b \mid a\varphi(a))$. Мы обозначаем ее $p_g(b \mid a)$. Это есть вероятность разности b на выходе раунда g с аддитивным ключом при заданной разности a на его входе и любом фиксированном значении раундового ключа.

Как уже говорилось, в реальных итеративных блочных шифрах функция раундового шифрования g строится обычно в виде суперпозиции некоторых более простых функций, допуская возможность эффективного вычисления вероятности $p_g(b|a)$ для любых заданных a и b. Ниже эта возможность демонстрируется на примере раунда DES.

Пример [4]. В раунде DES операция замены S является набором функций S_i: $\{0, 1\}^6 \to \{0, 1\}^4$, $i = 1,\ldots,8$, для нее $p_S(b|a) = \prod_{i=1}^{8} p_{S_i}(b_i \mid a_i)$ для $a = a_1a_2\ldots a_8$ и $b = b_1b_2\ldots b_8$ и $p_{S_i}(b_i \mid a_i) = |D_{S_i}(a_i, b_i)| / 64$ для $i = 1,\ldots,8$. Функция $S_1(x_1x_2x_3x_4x_5x_6)$ задается табл. 1.

Таблица 1

x_1x_6	$x_2x_3x_4x_5$							
	0000	0001	0010	0011	0100	0101	0110	0111
00	1110	0100	1101	0001	0010	1111	1011	1000
01	0000	1111	0111	0100	1110	0010	1101	0001
10	0100	0001	1110	1000	1101	0110	0010	1011
11	1111	1100	1000	0010	0100	1001	0001	0111

x_1x_6	$x_2x_3x_4x_5$							
	1000	1001	1010	1011	1100	1101	1110	1111
00	0011	1010	0110	1100	0101	1001	0000	0111
01	1010	0110	1100	1011	1001	0101	0011	1000
10	1111	1100	1001	0111	0011	1010	0101	0000
11	0101	1011	0011	1110	1010	0000	0110	1101

Ее разностные множества $D_{S_1}(a,b)$ для $a = 110100$ и всевозможных $b \in \{0, 1\}^4$ перечислены в табл. 2.

Таблица 2

b	$D_{S_1}(110100,b)$
0000	
0001	000011, 001111, 011110, 011111, 101010, 101011, 110111, 111011
0010	000100, 000101, 001110, 010001, 010010, 010100, 011010, 011011, 100000, 100101, 010110, 101110, 101111, 110000, 110001, 111010
0011	000001, 000010, 010101, 100001, 110101, 110110
0100	010011, 100111
0101	
0110	
0111	000000, 001000, 001101, 010111, 011000, 011101, 100011, 101001, 101100, 110100, 111001, 111100
1000	001001, 001100, 011001, 101101, 111000, 111101
1001	
1010	
1011	
1100	
1101	000110, 010000, 010110, 011100, 100010, 100100. 101000, 110010
1110	
1111	000111, 001010, 001011, 110011, 111110, 111111

Таким образом, $p_{S_1}(0000 \mid 110100) = 0$, $p_{S_1}(0001 \mid 110100) = 1/8$, $p_{S_1}(0010 \mid 110100) = 1/4$ и т.д. Аналогично вычисляются все другие вероятности $p_{S_i}(b_i \mid a_i)$ в выражении для $p_S(b \mid a)$. Например, $D_{S_1}(001100, 1110) = \{000011, 000110, 001010, 001111, 010011, 010111, 011011, 011111, 100001, 100110, 101010, 101101, 110111, 111011\}$ и $p_{S_1}(1110 \mid 001100) = 14/64$.

По определению функции f в DES (пример 1), для любых $a = u \oplus u^*$, b в $\{0, 1\}^{32}$ и $k \in \{0, 1\}^{48}$ ввиду теоремы 2 $p_f(b \mid a) = p_f(b \mid a, k) = p_S(P^{-1}(b) \mid E(u) \oplus k \oplus E(u^*) \oplus k) = p_S(P^{-1}(b) \mid E(a))$. По определению функции $g = (g', g'')$ раундового шифрования в DES (пример 1), для любых разностей $L_{i-1}'R_{i-1}'$ и $L_i'R_i'$ соответственно на входе и на выходе i-го раунда DES ввиду следствия 2 из теоремы 2 получаем $p_g(L_i'R_i' \mid L_{i-1}'R_{i-1}') = p_{g''}(R_i' \mid L_{i-1}'R_{i-1}') = p_f(R_i' \oplus L_{i-1}' \mid R_{i-1}') = p_S(P^{-1}(R_i' \oplus L_{i-1}') \mid E(R_{i-1}'))$.

Обратим внимание на неравномерность в DES распределения $p_{S_1}(b \mid 110100)$, обязанную неравномощности множеств $D_{S_1}(110100,b)$. Следствием неравномерности некоторых распределений вероятностей $p_{S_i}(b_i \mid a_i)$ является неравномерность распределений $p_g(b|a)$ для некоторых разностей a на входе раунда DES.

Именно неравномерность распределений вероятностей некоторых разностей на выходе раунда, возможная при некоторых разностях на его входе (вследствие неравномощности соответствующих разностных множеств функции ψ), служит еще одной основой для дифференциального криптоанализа любого итеративного блочного шифра с аддитивным раундовым ключом и парой $[\psi, \varphi]$ в качестве функции раундового шифрования g.

7. Дифференциальная вероятностная характеристика итеративного блочного шифра с аддитивным раундовым ключом

Пусть далее C есть r-раундовый итеративный блочный шифр с функцией раундового шифрования g: $U \times K \to U$ и с аддитивными раундовыми ключами $k_1, \ldots, k_r$ в K, где k_i – ключ i-го раунда, $i = 1, \ldots, r$. Для любого натурального $t \le r$ последовательность $\chi_t = (a_0', a_1', p_1, a_2', p_2, \ldots, a_t', p_t)$, где все $a_0', a_1', \ldots, a_t'$ принадлежат U, называется *t-раундовой дифференциальной вероятностной характеристикой* шифра C, если для любого $i \ge 1$ в ней $p_i = p_g(a_i' | a_{i-1}')$, т.е. если a_{i-1} и a_{i-1}^* выбраны в U так, что $a_{i-1} - a_{i-1}^* = a_{i-1}'$, и вычислены $a_i = g(a_{i-1}, k_i)$ и $a_i^* = g(a_{i-1}^*, k_i)$, то $a_i - a_i^* = a_i'$ с вероятностью p_i. Произведение $p = p_1 \ldots p_t$ называется *вероятностью характеристики* χ_t.

Смысл данного понятия следующий: если зафиксировать раундовые ключи шифра C и на его вход подать поочередно два блока открытого текста, разность которых равна a_0', то на выходе t-го раунда будут получены два блока шифртекста, разность которых совпадет с a_t' с вероятностью не меньше p. Таким образом, имея характеристику χ_t для $t < r$, криптоаналитик может проводить на шифр C атаку с выбором открытого текста (выбирая пары блоков с разностью a_0'), в которой, не имея доступа к выходу промежуточного (t-го)

раунда, он с вероятностью p знает разности (соответствующих) блоков на нем и это знание может использовать для достижения цели криптоанализа.

Имея две характеристики шифра $\chi_t = (a_0', a_1', p_1, a_2', p_2, \ldots, a_t', p_t)$ и $\chi_s^* = (b_0', b_1', q_1, b_2', q_2, \ldots, b_s', q_s)$, где $a_t' = b_0'$, можно построить третью – $\chi_{t+s} = (a_0', a_1', p_1, a_2', p_2, \ldots, a_{t+s}', p_{t+s}) = (a_0', a_1', p_1, a_2', p_2, \ldots, a_t', p_t, b_1', q_1, b_2', q_2, \ldots, b_s', q_s)$, которая называется *конкатенацией* первых двух и обозначается $\chi_t \circ \chi_s^*$. Таким образом из 1-раундовых характеристик строятся многораундовые, в том числе *оптимальные* – с наибольшей вероятностью.

Примеры. Всякая t-раундовая вероятностная характеристика DES имеет вид $(L_0'R_0', L_1'R_1', p_1, L_2'R_2', p_2, \ldots, L_t'R_t', p_t)$. В ней для любого $i \geq 0$: $L_i' \in \{0, 1\}^{32}$, $R_i' \in \{0, 1\}^{32}$ и $L_{i+1}' = R_i'$. Приведем несколько примеров характеристик DES, представляя элементы в $\{0, 1\}^{32}$ целыми числами в 16-ричной системе.

1. Последовательность $\alpha = (L_0'R_0', L_1'R_1', p_1)$, где L_0' – любое, $R_0' = 00000000_{16} = L_1'$, $R_1' = L_0'$, $p_1 = 1$, является 1-раундовой характеристикой DES, ибо если $R_0 \oplus R_0^* = R_0'$, то $R_0 = R_0^*$, $R_1' = R_1 \oplus R_1^* = L_0 \oplus f(R_0, k_1) \oplus L_0^* \oplus f(R_0^*, k_1) = L_0 \oplus L_0^* = L_0'$ и $p_g(L_1'R_1' \mid L_0'R_0') = p_f(R_1' \oplus L_0' \mid R_0') = p_S(P^{-1}(R_1' \oplus L_0') \mid E(R_0')) = p_S(P^{-1}(00000000_{16}) \mid E(00000000_{16})) = p_S(00000000_{16} \mid 000000000000_{16}) = 1 = p_1$.

2. Последовательность $\beta = (L_0'R_0', L_1'R_1', p_1)$, где $L_0' = 00000000_{16}$, $R_0' = 60000000_{16} = L_1'$, $R_1' = 00808200_{16}$, $p_1 = 14/64$, является также 1-раундовой характеристикой DES, ибо $P_g(L_1'R_1' \mid L_0'R_0') = p_S(P^{-1}(R_1' \oplus L_0') \mid E(R_0')) = p_S(P^{-1}(00808200_{16}) \mid E(60000000_{16})) = p_S(\mathrm{E}0000000_{16} \mid 300000000000_{16}) = p_{S_1}(1110 \mid 001100) = 14/64 = p_1$.

3. Конкатенация $\alpha \circ \beta$ предыдущих двух характеристик с $L_0' = 60000000_{16}$ в первой является 2-раундовой характеристикой DES $(L_0'R_0', L_1'R_1', p_1, L_2'R_2', p_2)$, в которой $L_0' = 60000000_{16}$, $R_0' = 00000000_{16} = L_1'$, $R_1' = 60000000_{16}$, $p_1 = 1$, $L_2' = R_1'$, $R_2' = 00808200_{16}$, $p_2 = 14/64$. Ее вероятность есть $p = p_1 p_2 = 14/64$.

8. Шифры над конечным полем

Пусть далее s есть натуральное число, $s \geq 2$ и $F = \{0, 1\}^s$ – конечное поле с числом элементов $q = 2^s$. Для любого натурального t, кратного s, т.е. такого, что $t = sl$ для некоторого целого $l > 1$, элементы множества $\{0, 1\}^t = \{0, 1\}^{sl}$ можно рассматривать как векторы длиной l с компонентами в F, а само это множество как векторное пространство F^l. Таким образом, в случае n и m, кратных s, множества $X = Y = U = \{0, 1\}^n$ и $K = \{0, 1\}^m$ можно представлять как векторные пространства F^ν и F^μ соответственно, где $\nu = n/s$ и $\mu = m/s$, а шифр $C = (X, Y, K^r, G, G^{-1})$ и его функцию раундового шифрования g: $U \times K \to U$ – как соответственно шифр и функцию над полем F, а именно: $C = (F^\nu, F^\nu, (F^\mu)^r, G, G^{-1})$ и g: $F^\nu \times F^\mu \to F^\nu$.

В дальнейшем мы пользуемся этой возможностью без дополнительных оговорок, предполагая, что для шифра с аддитивным раундовым ключом групповая операция сложения векторов в F^ν и F^μ совпадает с их покомпонентным сложением в поле F. Кроме того, мы допускаем возможность задания функции g системой Ω функций g_i: $F^\nu \times F^\mu \to F$, $i = 1, 2, \ldots, \nu$, определяемых для произвольных $u = (u_1 \ldots u_\nu) \in F^\nu$ и $k = (k_1 \ldots k_\mu) \in F^\mu$ как $(g_1(u_1, \ldots, u_\nu, k_1, \ldots, k_\mu) \ldots g_\nu(u_1, \ldots, u_\nu, k_1, \ldots, k_\mu)) = g(u_1, \ldots, u_\nu, k_1, \ldots, k_\mu)$ и задаваемых полиномами над F. Для большинства известных итеративных блочных шифров, в том числе для DES, AES, IDEA, SAFER, LOKI91, Serpent, Redoc и др., реализация этой возможности не представляет сколь-либо заметных трудностей.

9. Уравнения раунда с вероятностной разностью на входе

Рассмотрим ситуацию, когда пары (u, u^*) блоков открытого текста на входе раунда криптоаналитику не доступны ни для выбора, ни для наблюдения, но он знает, что их разность $u - u^*$ с вероятностью $p > 0$ совпадает с блоком u', и может наблюдать на выходе раунда его реакции на них $v = g(u, k)$ и $v^* = g(u^*, k)$. Данная ситуация возникает в дифференциальном криптоанализе многораундового шифра на основе вероятностной характеристики. Для определения ключа раунда в этом случае алгоритм A_1 не годится, так как он предполагает построение тестовых множеств, что невозможно сделать без знания u. Кроме того, останов алгоритма по условию одноэлементности пересечения Q тестовых множеств теперь бессмыслен, потому что если на самом деле $u - u^* \neq u'$, то соответствующее тестовое множество не обязано ни содержать раундовый ключ, ни даже быть непустым.

Вместе с тем описание раунда g системой функций Ω позволяет связать неизвестные компоненты $k_1, \ldots, k_\mu$ его ключа k и неизвестные значения на его входе $u(t) = (u_1(t), \ldots, u_\nu(t))$ и $u^*(t) = (u^*_1(t), \ldots, u^*_\nu(t))$ для любого $t = 1, 2, \ldots, \tau$ с соответствующими известными значениями на его выходе $v(t) = (v_1(t), \ldots, v_\nu(t))$ и $v^*(t) = (v^*_1(t), \ldots, v^*_\nu(t))$ и с известными разностями $u' = (u'_1, \ldots, u'_\nu)$ на его входе следующей системой полиномиальных уравнений над полем F:

$$\begin{gathered} g_i(u_1(t), \ldots, u_\nu(t), k_1, \ldots, k_\mu) = v_i(t), \\ g_i(u^*_1(t), \ldots, u^*_\nu(t), k_1, \ldots, k_\mu) = v^*_i(t), \\ u_i(t) - u^*_i(t) = u'_i,\ i = 1, 2, \ldots, \nu; \\ t = 1, 2, \ldots, \tau. \end{gathered} \tag{1}$$

При $\tau \geq \mu/\nu$ эта система переопределенная: количество уравнений в ней не меньше числа неизвестных. Например, для раунда DES, где $\nu = 32$ и $\mu = 48$, это выполняется уже при $\tau \geq 2$. Условие переопределенности, как известно, является необходимым для единственности решения совместной системы. Данная система, кроме того, вероятностная: уравнения в первых двух строчках выполняются с вероятностью 1, а в третьей – с вероятностью p. Таким образом, p^τ есть вероятность совместности всей системы. Это значит, что только для части $p^\tau \cdot q^\nu$ пар из числа q^ν всех пар $(u(t), u^*(t))$ с заданной разностью $u(t) - u^*(t) = u'$ данная система имеет решение. Для того чтобы это число было не меньше 1, надо иметь $p \geq q^{-\nu/\tau} \geq q^{-\nu^2/\mu}$. Так, в случае DES должно быть $p \geq 2^{-21}$.

10. Дифференциальный криптоанализ многораундового шифра

Постановка задачи. Пусть имеются: r-раундовый шифр C с фиксированными аддитивными раундовыми ключами и его $(r-1)$-раундовая дифференциальная вероятностная характеристика $\chi_{r-1} = (a_0', a_1', p_1, \ldots, a'_{r-1}, p_{r-1})$ с вероятностью $p > 0$. Требуется найти ключ $k = (k_1, \ldots, k_\mu)$ последнего раунда шифра C или его непустую часть.

Рассмотрим два подхода к решению этой задачи: 1 – на основе теоремы об аддитивном раундовом ключе и 2 – на основе решения системы уравнений последнего раунда. Первый применяется в случае, если раундовая функция шифрования в C разделима по Фейстелю, второй – в случае произвольного C.

Алгоритм криптоанализа на основе теоремы об аддитивном раундовом ключе

Итак, пусть функция g раунда в C разделима по Фейстелю, т.е. $g = \langle\delta, \varepsilon\rangle$: $U \times K \to U$, где $U = U' \times U''$, ε: $U' \to K$, δ: $K \to U''$ и $g(LR, k) = R\delta(L + (\varepsilon(R) + k))$ для любых L, R в U' и $k \in K$. В этом случае заданная вероятностная характеристика имеет вид $\chi_{r-1} = (L_0'R_0', L_1'R_1', p_1, \ldots, L'_{r-1}R'_{r-1}, p_{r-1})$.

Алгоритм B_1. Его параметром является натуральное число N.

1. Для каждого $t = 1, 2, \ldots, N$ выполним следующую последовательность действий:

1) выбирается пара блоков $(x(t), x^*(t))$ открытого текста на входе C, таких, что $x(t) - x^*(t) = L_0'R_0'$;

2) на выходе C получается пара соответствующих блоков шифртекста $(y(t), y^*(t)) = (G(x(t), z), (G(x^*(t), z))$, где $z \in K^r$ – неизвестный ключ шифра, и находятся такие $L(t)$, $L^*(t)$, $R(t)$, $R^*(t)$ в U', что $L(t)R(t) = y(t)$ и $L^*(t)R^*(t) = y^*(t)$;

3) вычисляются разности $b(t) = b'(t)b''(t) = y(t) - y(t)^*$ с $b'(t)$, $b''(t)$ в U'' и $b_1(t) = b''(t) - L'_{r-1}$, а также разностное множество $D_\delta(\varepsilon(b'(t)), b_1(t)) = \{j \in K: \delta(j) - \delta(j - \varepsilon(b'(t))) = b_1(t)\}$ и тестовое множество $T_t = T_\delta(\varepsilon(L(t)), \varepsilon(L^*(t)), b_1(t)) = \{j - \varepsilon(L(t)): j \in D_\psi(\varepsilon(b'(t)), b_1(t))\}$.

2. Находится такой элемент $k \in K$, который наиболее часто встречается в тестовых множествах T_t для $t = 1, 2, \ldots, N$. Этот элемент и выдается за результат криптоанализа – искомый раундовый ключ.

Сделаем несколько замечаний к данному алгоритму. В п. 1.3 используется L'_{r-1} – часть разности на входе r-го раунда, известная с вероятностью p, отчего результат криптоанализа будет совпадать с истинным раундовым ключом лишь с некоторой вероятностью, которая тем больше, чем больше вероятность p и число N используемых пар блоков открытого текста. Реализация п. 2 требует применения счетчиков ключей из K в тестовых множествах, что предполагает большие затраты памяти. Алгоритм, подобный данному, невозможен для шифра с произвольной разделимой функцией раунда, с произвольной функцией раунда без ветвления входа и, тем более, с произвольной функцией раунда с аддитивным ключом, так как вычисление тестового множества требует знания блока (или, как в разделимом случае, его части) на входе последнего раунда, который в этих случаях недоступен криптоаналитику.

Алгоритм криптоанализа на основе решения системы уравнений

В отличие от предыдущего, этот алгоритм решает поставленную задачу для любого шифра C с аддитивным раундовым ключом, не требуя больших затрат памяти. В нем предполагается, что заданный шифр C представлен как шифр над полем F и его функция раундового шифрования g: $F^\nu \times F^\mu \to F^\nu$ задана системой функций $\Omega = \{g_i: F^\nu \times F^\mu \to F, i = 1, 2, \ldots, \nu\}$.

Алгоритм B. Пусть $\tau = \lceil \mu/\nu \rceil$.

1. Выбираются пары блоков $(a(1), a^*(1)), (a(2), a^*(2)), \ldots, (a(\tau), a^*(\tau))$ открытого текста на входе C, такие, что $a(t) - a^*(t) = a_0'$ для каждого $t = 1, 2, \ldots, \tau$.

2. На выходе C получаются пары соответствующих блоков шифртекста $(v(1), v^*(1)), (v(2), v^*(2)), \ldots, (v(\tau), v^*(\tau))$.

3. Записывается система уравнений (1) с переменными в F, где $(v_1(t),\ldots,v_\nu(t)) = v(t)$, $(v^*_1(t),\ldots,v^*_\nu(t)) = v^*(t)$, $t = 1, 2, \ldots, \tau$, и $(u'_1, \ldots, u'_\nu) = a'_{r-1}$.

4. Если эта система несовместна, то пп.1 – 3 повторяются с выбором в п. 1 другого набора пар блоков открытого текста; в противном случае

5. Находится решение полученной системы уравнений – возможно, частичное: только для переменных в k. Найденные значения последних и есть результат.

Сделаем несколько замечаний к данному алгоритму. Прежде всего, заметим, что если в последнем пункте алгоритма находится полное решение системы уравнений, то становятся известными пары блоков шифртекста на выходе (r–1)-го раунда, и алгоритм может быть повторен с укороченной характеристикой (a_0', a_1', p_1, …, a'_{r-2}, p_{r-2}) для нахождения ключа предпоследнего раунда. Таким путем можно последовательно найти ключи всех раундов шифра.

Количество циклов из пп. 1 – 3, а следовательно, и количество блоков открытого текста, необходимых алгоритму для достижения результата, зависят от вероятности p используемой характеристики χ_{r-1}: чем она выше, тем меньше это число.

Свойство аддитивности раундового ключа собственно алгоритмом непосредственно не используется, оно нужно только для построения необходимой многораундовой характеристики шифра.

Алгоритм можно применять, очевидно, и тогда, когда системой уравнений (1) описывается не один раунд, но ряд из $l \geq 1$ последних раундов шифра, а вместо χ_{r-1} используется характеристика χ_{r-l} и $\tau = \lceil \mu \cdot l / \nu \rceil$. В этом случае результатом криптоанализа будут ключи этих раундов.

В алгоритме можно использовать одновременно не одну, а несколько дифференциальных характеристик. В этом случае в его п. 3 в качестве (1) берется объединение систем уравнений, записанных для разных характеристик, что повышает результативность алгоритма.

В последнее время методы решения систем уравнений над конечным полем развиваются интенсивно [5]; есть многочисленные примеры их успешного применения в криптоанализе (см., например, [5 – 7]). Какой из методов наиболее эффективен в применении к той или иной конкретной системе уравнений, определяется параметрами последней и соотношениями между ними, такими, как число переменных, уравнений и мономов в системе, ее степень, мощность линеаризационного множества и т.п.

Например, для раунда DES система уравнений (1) с $\tau = 2$ содержит в совокупности 192 уравнения и 176 переменных. Каждое уравнение в ней зависит от 7 переменных, и его степень равна 5. Система состоит из 8 подсистем с 24 уравнениями и 22 переменными в каждой, где 8 уравнений линейные вида $x \oplus y = c$. После исключения переменных по правилу $y = x \oplus c$ в каждой подсистеме остается 16 уравнений и 14 переменных. Множества переменных в различных подсистемах не пересекаются, и решение всей системы сводится к решению каждой ее подсистемы в отдельности, что реально осуществимо даже методом исчерпывающего поиска – перебором всех возможных комбинаций значений переменных в подсистеме.

Выражаю благодарность И.А. Панкратовой, указавшей на некоторые опечатки и ошибки в тексте статьи и исследовавшей алгоритм *B* на примере DES в компьютерном эксперименте [8].

ЛИТЕРАТУРА

1. *Biham E.*, *Shamir A*. Differential cryptanalysis of DES-like cryptosystems / Technical Report. The Weizmann Institute of Science. Department of Applied Mathematics: 1990. 105 p. // J. Cryptology. 1991. V. 4. No. 1. P. 3 – 72.
2. *Biham E.*, *Shamir A*. Differential cryptanalysis of the Data Encryption Standard. Springer Verlag, 1993. 188 p.
3. *Biham E.*, *Shamir A*. Differential cryptanalysis of the full 16-round DES // Lect. Not. Comp. Science. 1993. No. 740. P. 494 – 502.
4. *Stinson D.R.* Cryptography. Theory and Practice. CRC Press, 1995. 434 p.
5. *Агибалов Г.П.* Методы решения систем полиномиальных уравнений над конечным полем // Вестник ТГУ. Приложение. 2006. № 17. С. 4 – 9.
6. *Агибалов Г.П.* Логические уравнения в криптоанализе генераторов ключевого потока // Вестник ТГУ. Приложение. 2003. № 6. С. 31 – 41.
7. *Courtois N.*, *Pieprzyk J.* Cryptanalysis of Block Ciphers with Overdefined Systems of Equations // ASIACRYPT 2002, LNCS 2501. 2002. P. 267 – 287.
8. *Панкратова И.А.* Экспериментальное исследование одного алгоритма дифференциального криптоанализа на примере DES // Прикладная дискретная математика (в печати).