УДК 519.7 DOI 10.17223/2226308X/8/22

СЛОЖЕНИЕ ПО МОДУЛЮ 2^n В БЛОЧНОМ ШИФРОВАНИИ

А. М. Карондеев

Произведён анализ криптографических свойств операции сложения по модулю 2^n. Предложены линейные и нелинейные аппроксимации данной операции, а также изучены особенности их использования при проведении криптоанализа. Приведены примеры использования аппроксимаций сложения по модулю 2^n для проведения атак с известным открытым текстом на шифры, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n. Показано, что замена операции сложения по модулю 2 на сложение по модулю 2^n приводит к увеличению стойкости блочных шифров.

Ключевые слова: *сложение по модулю 2^n, блочные шифры, криптоанализ.*

Составной частью любого блочного шифра является процедура смешения с ключом. Обычно данная процедура представляет собой сложение по модулю 2 (XOR) промежуточного информационного блока с раундовым ключом (как в алгоритмах DES, AES и др.), однако ничто не мешает использовать любую другую операцию, например сложение по модулю 2^n (как в алгоритме ГОСТ 28147-89). С учётом современной элементной базы и структуры большинства блочных шифров замена операции XOR на сложение по модулю 2^n не приведёт к существенному возрастанию сложности как программной, так и аппаратной реализации шифра. Работа посвящена анализу стойкости алгоритмов блочного шифрования, в которых операция смешения с ключом реализована как операция сложения по модулю 2^n.

Произведён анализ криптографических свойств операции $A + B = D \bmod 2^n$, где $A = (a_{n-1}, \ldots, a_0)$, $B = (b_{n-1}, \ldots, b_0)$, $D = (d_{n-1}, \ldots, d_0)$. В частности, рассмотрены линейные и нелинейные аппроксимации для выходных битов d_i и доказано, что для любого $i > 0$ функции $a_i \oplus b_i \oplus a_{i-1}$ и $a_i \oplus b_i \oplus b_{i-1}$ являются наилучшими линейными аппроксимациями для d_i, а именно: если a_j, b_j, $j = 0, \ldots, n-1$, являются независимыми случайными величинами, принимающими все свои значения с равной вероятностью, то линейные соотношения

$$d_i = a_i \oplus b_i \oplus a_{i-1}, \tag{1}$$

$$d_i = a_i \oplus b_i \oplus b_{i-1} \tag{2}$$

выполняются с вероятностью 0,75.

Рассмотрим особенности использования данных линейных аппроксимаций при проведении линейного криптоанализа блочных шифров, в которых для смешения с ключом используется операция $Y = X + K \bmod 2^n$. При проведении линейного криптоанализа [1] считается, что ключ фиксирован и аналитик располагает некоторым количеством пар открытый текст/шифртекст (материалом), полученных на этом ключе. Показано, что при фиксированном ключе вероятность выполнения соотношений (1), (2) может сильно отличаться от 0,75, а именно она колеблется в интервале от 0,5 до 1, причём границы достижимы. Таким образом, если при проведении линейного криптоанализа использовать аппроксимации (1), (2) для конкретного ключа, вероятность их выполнения может оказаться равной 0,5, и анализ будет невозможен.

Предложено новое решение — нелинейные соотношения, выполняющиеся с преобладанием не меньше 0,25 для любого фиксированного ключа. Точнее, доказано:

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4; \tag{3}$$

$$\forall i > 0\ \forall K\ \exists z\ (\mathbf{P}\{y_i \oplus y_{i-1} = x_i \oplus z x_{i-1}\} = 1/2 + \varepsilon,\ |\varepsilon| \geqslant 1/4. \tag{4}$$

Изучена возможность применения соотношений (3), (4) для анализа блочных шифров, использующих операцию $+ \bmod 2^n$. Предложена модификация линейного метода криптоанализа, которая в ряде случаев позволяет провести более эффективные атаки.

В частности, аппроксимации (3), (4) использованы для проведения атаки с известным открытым текстом на конкретный шифр, имеющий структуру SP-сети, в котором для смешения с ключом используется операция $+ \bmod 2^n$. Эта атака позволяет восстановить ключ быстрее полного перебора, что подтверждено моделированием на ЭВМ. Далее был проанализирован шифр, имеющий аналогичное строение, но использующий для смешения с ключом операцию XOR. Сравнительный анализ показал, что замена операции XOR на $+ \bmod 2^n$ приводит к существенному увеличению стойкости шифра. При проведении атаки на шифр, использующий $+ \bmod 2^n$ вместо XOR, помимо S-блоков необходимо аппроксимировать блок смешения с ключом, поэтому в большинстве случаев абсолютная величина преобладания итогового соотношения, связывающего некоторые биты открытого текста, шифртекста и ключа, становится гораздо ниже, из-за чего для проведения атаки требуется существенно больше материала.

Проведена атака с известным открытым текстом на алгоритм ГОСТ 28147-89 с сокращённым числом раундов и S-блоками специального вида. В [2] доказана стойкость алгоритма ГОСТ 28147-89 с не менее чем пятью раундами шифрования относительно линейного метода криптоанализа. Предложенный метод позволил провести атаку на алгоритм ГОСТ 28147-89 с восемью раундами шифрования.

ЛИТЕРАТУРА

1. *Matsui M.* Linear cryptanalysis method for DES cipher // LNCS. 1993. V. 765. P. 386–397.
2. *Shorin V. V., Jelezniakov V. V., and Gabidulin E. M.* Linear and differential cryptanalysis of Russian GOST // Proc. Int. Workshop Coding and Cryptography (Paris, France, January 8–12, 2001). P. 467–476.

УДК 519.723 DOI 10.17223/2226308X/8/23

НЕЭНДОМОРФНЫЕ СОВЕРШЕННЫЕ ШИФРЫ С ДВУМЯ ШИФРВЕЛИЧИНАМИ

Н. В. Медведева, С. С. Титов

Исследуются неэндоморфные совершенные по Шеннону (абсолютно стойкие к атаке по шифртексту) шифры в случае, когда мощность множества шифрвеличин равна двум. В терминах линейной алгебры на основе теоремы Биркгофа о классификации дважды стохастических матриц описаны матрицы вероятностей ключей данных шифров. Построено множество возможных значений априорных вероятностей шифробозначений совершенного шифра.

Ключевые слова: *совершенные шифры, неэндоморфные шифры, максимальные шифры, дважды стохастические матрицы.*

Впервые вероятностная модель шифра рассмотрена в фундаментальной работе К. Шеннона [1]. Пусть X, Y — конечные множества соответственно шифрвеличин и