А. И. Пестунов

ДИФФЕРЕНЦИАЛЬНЫЙ КРИПТОАНАЛИЗ БЛОЧНОГО ШИФРА CAST-256

Введение

Общие сведения о блочных шифрах. Блочные шифры являются важнейшим элементом в современных системах защиты информации, поэтому большое внимание уделяется их исследованию, и в последние годы были реализованы несколько проектов, на это направленных [1—3]. Серьезное влияние имел проект Advanced Encryption Standard (AES) [1], шифр-победитель которого стал стандартом шифрования в США. Типичный блочный шифр преобразует открытый текст, представленный в виде последовательности битов (нулей и единиц), по блокам фиксированной длины, чаще всего равной 64 или 128 бит. Секретный ключ также представляет собой битовую последовательность (обычно длиной 128 или 256), из которой по определенному для каждого шифра механизму получается набор из R *подключей*. Процедура шифрования носит итеративный характер и заключается в R-кратном выполнении некоторого относительно «слабого» преобразования, которое зависит от своего подключа и называется *раундом* шифрования. Раунды могут быть как одинаковыми, так и различными. Чем больше их выполнено, тем надежнее, но медленнее становится шифр, поэтому его создатель определяет такое количество раундов, которое обеспечивает и безопасность, и быстродействие алгоритма.

Криптоанализ блочных шифров. Исследовать безопасность криптоалгоритмов призван раздел криптологии, называемый *криптоанализом*. Криптоанализ блочных шифров подобен соревнованию между криптоаналитиками, которые стараются найти неизвестный секретный ключ для упрощенных версий шифра, по возможности более близких к исходному варианту. Например, для шифра, состоящего из 20 раундов, криптоанализ 12 раундов считается продвижением в анализе шифра, если ранее удавалось найти ключ только для версии шифра, состоящей из 10 раундов. Заметим, что знание всех подключей блочного шифра эквивалентно знанию секретного ключа, поскольку в шифровании участвуют подключи, а секретный ключ используется только для их вычисления. Алгоритм, позволяющий найти секретный ключ или массив подключей быстрее, чем полный перебор ключей, называется *атакой* на шифр. Даже если атака нереализуема на практике (например, ее сложность составляет 2^{200}, а метод полного перебора ключей требует 2^{256}), это является важным сертификационным недостатком шифра [4].

На сегодняшний день не существует цельной теории, в рамках которой можно было бы гарантировать безопасность того или иного блочного шифра, поэтому надежность шифра можно оценить только на основе предложенных атак на него. Например, 20-раундовый шифр, имеющий атаку на 5 раундов, может быть признан безопасным, а имеющий атаку на 19 раундов вряд ли выдержит атаки криптоаналитиков в ближайшие годы.

Результаты данной статьи. Шифр CAST-256 [5] участвовал в конкурсе AES, и на этот 48-раундовый шифр опубликованы две атаки. Первая из них позволяет найти подключи шифра, состоящего из 16 раундов [6]. Вторая атака [7] позволяет сделать это для шифра, имеющего до 36 раундов, но только для некоторого класса *слабых* ключей. В частности, 24-раундовая версия шифра может быть атакована только для 2^{-30} части ключей. Атака, предложенная в данной статье, позволяет найти подключи шифра CAST-256, состоящего из 24 раундов, но не только для слабых ключей, а для всех.

Таблица 1. Обозначения, используемые в статье

$+$	Сложение по модулю 2^{32}	(a_0, a_1, a_2, a_3)	128-битовый блок, разбитый на четыре 32-битовых слова
$-$	Вычитание по модулю 2^{32}	δ_i	2^i , т. е. 32-битовое слово, у которого i -й бит равен 1, а остальные — 0.
$\oplus$	Побитовое сложение (xor)	$v^{[n,\ldots,m]}$	с m -го по n -й биты слова v
$\lll K_r$	Поворот влево на K_r бит	$60\,A40_x$	Число, записанное в шестнадцатеричной системе исчисления

Краткое описание дифференциального криптоанализа

Основные понятия. Основной объект, который исследуется в дифференциальном криптоанализе, — это пары блоков текста A и B с определенной разностью [8]. Эта разность представляет собой побитовое сложение по модулю 2 (xor) — $A \oplus B$. Если информация о том, как связаны входная разность (между блоками открытого текста) и выходная разность (между блоками шифртекста), отсутствует, то все выходные разности равновероятны. Однако если (каким-то образом) удается установить, что некоторая входная разность Δ_{inp} приводит к некоторой выходной разности Δ_{out} с вероятностью p , большей, чем остальные, то это может быть использовано для отыскания подключей шифра. Пара $(\Delta_{inp}, \Delta_{out})$ называется *дифференциалом*, а совокупность дифференциалов на различных раундах называется *характеристикой*. Если выходная разность включает в себя неизвестные биты, то дифференциал называется *усеченным* [9]. В дальнейшем дифференциал обозначается следующим образом:

$$\Delta_{inp} \xrightarrow{\text{количество раундов (с вероятность ю p)}} \Delta_{out}.$$

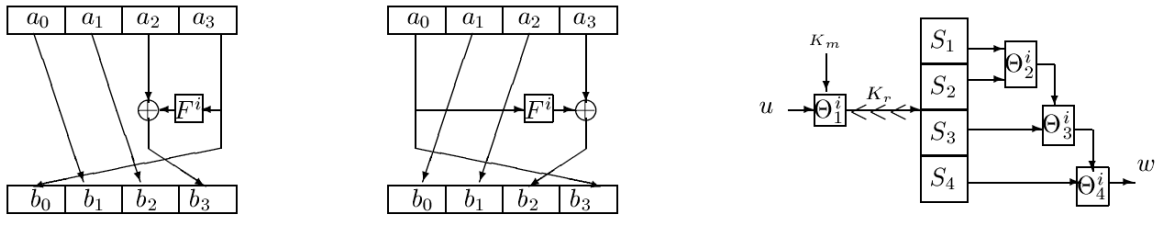
Например, для совершенного шифра со 128-битовым блоком при любой входной разности выходная разность принимает некоторое фиксированное значение с вероятностью 2^{-128}. Таким образом, если в процессе анализа шифра обнаружится, что определенная входная разность приводит к определенной выходной разности с вероятностью большей, чем 2^{-128} (например, 2^{-100}), то эта информация может быть использована с целью отыскания его подключей. Количество текстов, требующееся для реализации атаки, пропорционально $1/p$.

Описание шифра CAST-256

В данном разделе приводится краткое описание шифра CAST-256. Полное описание может быть найдено в [5].

Общая структура шифра CAST-256. Шифр CAST-256 состоит из 48 раундов двух типов: **A** и **B**, а также трех типов раундовой функции: F^1, F^2 и F^3. Если раунд использует функцию F^i, то он обозначается $\mathbf{A}^i$ или $\mathbf{B}^i$, если тип функции F не важен, то индекс i опускается. Вначале открытый текст преобразуется 24 раундами типа **A**, а затем 24 раундами типа **B**, точная последовательность раундов следующая:

$\mathbf{A}^1, \mathbf{A}^2, \mathbf{A}^3, \mathbf{A}^1, \quad \mathbf{A}^1, \mathbf{A}^2, \mathbf{A}^3, \mathbf{A}^1, \quad \mathbf{A}^1, \mathbf{A}^2, \mathbf{A}^3, \mathbf{A}^1, \ldots$
$\mathbf{B}^1, \mathbf{B}^2, \mathbf{B}^3, \mathbf{B}^1, \quad \mathbf{B}^1, \mathbf{B}^2, \mathbf{B}^3, \mathbf{B}^1, \quad \mathbf{B}^1, \mathbf{B}^2, \mathbf{B}^3, \mathbf{B}^1, \ldots$



$\oplus$	побитовое сложение (xor)	$\boxed{S_i}$	S-бокс — отображение 8 бит в 32,
Θ_j^i	бинарные операции (см. табл 2)	$\lll_{K_r}$	поворот влево на K_r бит,
K_r	5-битовый подключ поворота	$a_i,\ b_i,\ u,\ w$	32-битовые слова
$\boxed{F^i}$	функция F^i,	K_m	32-битовый подключ маскировки

Рис. 1. Структура раундов шифра CAST-256

Функции F^i. Три типа функции F (Рис. 1) имеют схожую структуру и отличаются только порядком операций в них (таблица 2).

Таблица 2. Три типа функции F

i	Θ_1^i	Θ_2^i	Θ_3^i	Θ_4^i
1	+	$\oplus$	–	+
2	$\oplus$	–	+	$\oplus$
3	–	+	$\oplus$	–

Рассмотрим, например, функцию F^2. Она снабжается 5-битовым подключом «поворота» K_r и 32-битовым подключом «маскировки» K_m, имеет одно 32-битовое слово u на входе и одно 32-битовое слово w на выходе. Преобразование этих слов в процессе исполнения функции приведено ниже:

$$v := (u \oplus K_m)^{\lll K_r};$$

$$w := ((S_1(v^{[31,\ldots,24]}) - S_2(v^{[23,\ldots,16]})) + S_3(v^{[15,\ldots,8]})) \oplus S_4(v^{[7,\ldots,0]})).$$

Раунды шифра CAST-256. Если блок B является результатом одноraундового шифрования блока A, тогда $(b_0, b_1, b_2, b_3) = (a_3, a_0, a_1, a_2 \oplus F(a_3))$, когда используется раунд типа **A**, и $(b_0, b_1, b_2, b_3) = (a_1, a_2, a_3 \oplus F(a_0), a_0)$, когда используется раунд типа **B**.

18-раундовая характеристика шифра CAST-256

Данный параграф посвящен построению характеристики

$$(\beta,\alpha,0,0) \xrightarrow{\text{2 раунда A (p=1)}} (0,0,\beta,\alpha) \xrightarrow{\text{1 раунд A}^2\ (p=2^{-17})} (\alpha,0,0,0) \xrightarrow{\text{15 раундов (p=1)}} (?,\ ?,\ ?,\ \alpha),$$

которая покрывает 18 раундов шифра CAST-256 — с 4-го по 9-й раунд типа **A** (т. е. с 4-го по 9-й раунд шифра CAST-256) плюс с 1-го по 12-й раунд типа **B** (т. е. с 21-го по 32-й раунд шифра CAST-256).

Здесь $\beta = 60A40_x$, $\alpha = 29_x^{\lll n}$, (1)

величина n выбрана случайно из множества $\{0, 1, 2, \ldots, 2^5 - 1\}$.

Замечание. В работе [10] использовалась идея о том, что разность между двумя словами в 1 бит сохраняется после сложения этих слов с третьим с вероятностью 1/2 или 1.

Более формально эта идея выглядит следующим образом. Пусть a и z — случайные величины, $a \oplus b = d$ и $d = \delta_i$. Тогда вероятность того, что $a \oplus b = (a + z) \oplus (b + z)$, равна 1/2 (или 1, если i = 31). Эта идея может быть расширена на случай произвольной разности d следующим образом. Если разность двух слов равна d и величина d имеет вес Хэмминга h, то после сложения этих слов с третьим эта разность сохраняется с вероятностью 2^{-h} (или $2^{-(h-1)}$, если одна из «1» находится на месте старшего бита).

1-раундовая характеристика. Опишем построение характеристики

$$(0,0,\beta,\alpha) \xrightarrow{\text{1 раунд A}^2\ (p=2^{-17})} (\alpha,0,0,0).$$

Рассмотрим функцию F^2 и предположим, что K_r известно. Пусть $u_1 \oplus u_2 = 29_x^{<<<24\text{-}K_r}$. Разность этой пары после побитового сложения с K_m сохраняется, т. е. $v_1 \oplus v_2 = 29_x^{<<<24\text{-}K_r}$. После поворота на K_r бит разность становится равной $29_x^{<<<24}$. Значит, входная разность в S_1 равна 29_x, а все остальные S-боксы имеют нулевую входную (а значит, и выходную) разность, т. е. $v_1^{[23,\ldots,0]} = v_2^{[23,\ldots,0]}$. Поэтому положим

$z := S_3(v_1^{[15,\ldots,8]}) - S_2(v_1^{[23,\ldots,16]}) = S_3(v_2^{[15,\ldots,8]}) - S_2(v_2^{[23,\ldots,16]})$,

тогда можно записать

$w_i := (S_1(v_i^{[31,\ldots,24]}) + z) \oplus S_4(v_1^{[7,\ldots,0]})$, $i = 1,2$

Перебор всех возможных 256 входных пар в S_1 показал, что две из них с разностью 29_x: $(17_x, 3E_x)$ и $(3E_x, 17_x)$ обеспечивают выходную разность β. Рассматривая этот случай, т. е. когда $S_1(v_1^{[31,\ldots,24]}) + z) \oplus S_1(v_2^{[31,\ldots,24]}) = \beta$ получаем, что

$(S_1(v_1^{[31,\ldots,24]}) + z) \oplus S_1(v_2^{[31,\ldots,24]}) + z) = \beta$

с вероятностью 2^{-5}, поскольку вес Хэмминга β равен 5. Побитовое сложение с выходом S_4 не меняет разность.

Таким образом, предположив, что значение K_r известно, входная разность $29_x^{<<24\text{-}Kr}$ приводит к выходной разности β с вероятностью 2^{-12}. Но поскольку K_r не известно, то его можно угадать, заметив, что α равняется $29_x^{<<24\text{-}Kr}$ с вероятностью 2^{-5} и выходная разность функции F^2 равна β с вероятностью 2^{-17}.

Обратимся к раунду типа $\mathbf{A}^2$ с входной разностью (0, 0, β, α). Выходная разность функции F^2, равная β, побитово складывается с третьим словом входной разности в раунд $\mathbf{A}^2$, и получается ноль.

2-раундовая и 15-раундовая характеристики. Характеристика

$$(\beta,\alpha,0,0) \xrightarrow{\text{2 раунда A (p=1)}} (0,0,\beta,\alpha)$$

и характеристика, представленная в таблице 3, очевидным образом вытекают из структуры раундов шифра CAST-256.

Таблица 2. 15-раундовая характеристика с вероятностью 1

	3 раунда **A**			12 раундов **B**											
α	0	0	0	0	0	α	0	0	?	α	0	?	?	α	?
0	α	0	0	0	α	0	0	?	α	0	?	?	α	?	?
0	0	α	0	α	0	0	?	α	0	?	?	α	?	?	?
0	0	0	α	0	0	0	α	0	0	?	α	?	?	?	α

Атака на CAST-256

В данном параграфе описывается атака на 24 раунда шифра CAST-256. Первые 18 раундов покрываются построенной в предыдущем параграфе характеристикой, а для заключительных 6 раундов производится перебор 37-битовых подключей.

Замечание. Для удобства рассмотрим шесть перебираемых 37-битовых подключей раундов как один 222-битовый, и основная часть атаки направлена на поиск этого подключа. Пусть $X = CAST(A)$ означает шифрование 24 раундами шифра CAST-256.

Основная часть атаки на CAST-256. Атака работает подобно фильтру, имеющему 19 слоев. Перебираются все возможные 2^{222} подключи, каждый из которых пропускается через этот фильтр. Решающее свойство фильтра заключается в том, что правильный подключ успешно проходит все 19 слоев, а ни один из неправильных этого сделать не может. Атака реализуется в несколько шагов:

1. Сформировать 19 групп по 2^{20} различных пар A_t^g, B_t^g (g = 1, ..., 19; t = 1, ..., 2^{20}) открытого текста в каждой с разностями $A_t^g \oplus B_t^g = (\beta, \alpha_t^g, 0, 0)$. Каждое значение α_t^g выбрано в соответствии с (1).

Для каждой пары A_t^g, B_t^g запросить пару шифртекстов $X_t^g = CAST(A_t^g)$ и $Y_t^g = CAST(B_t^g)$. Сохранить их в памяти вместе с соответствующими им значениями α_t^g.

Перебрать все возможные подключи key = 0,...,2^{222}-1 и для каждого из них выполнить следующие действия:

a. $g := 1$;

b. частично расшифровать последними шестью раундами с подключом key хранящиеся в памяти пары шифртекста из группы group и получить пары P_t^g и Q_t^g;

c. если $P_t^g \oplus Q_t^g \neq (\alpha_t^g, ?, ?, ?)$ для всех t = 1,..., 2^{20}, то key — это неверный подключ, отбросить его и перейти к пункту (3), беря следующий подключ-кандидат; если хотя бы одна из пар обеспечивает условие $P_t^g \oplus Q_t^g = (\alpha_t^g, ?, ?, ?)$, то перейти к пункту (d);

d. если $g < 19$, то $g := g + 1$ и идти на (b); иначе — (e);

e. это значит, что g = 19 и подключ прошел все 19 слоев. Он является правильным.

Вероятность успеха атаки. Вычислим вероятность того, что все неправильные подключи-кандидаты были отброшены, а правильный — остался.

Пара X_t^g, Y_t^g, частично расшифрованная с неправильным подключом, не удовлетворяет дифференциалу $(\beta, \alpha_t^g, 0, 0) \xrightarrow{2\text{ раундов }(p=2^{-17})} (\alpha_t^g, ?, ?, ?)$, следовательно, разность $P_t^g \oplus Q_t^g$ принимает любое значение (в том числе и $(\alpha_t^g, ?, ?, ?)$) равновероятно, т. е. с вероятностью 2^{-32}. Следовательно, вероятность возникновения такой разности среди 2^{20} пар приблизительно равна 2^{-12}, а вероятность возникновения ее в 19 группах одновременно составляет примерно 2^{-228}. Значит, вероятность того, что хотя бы один неправильный подключ-кандидат пройдет все 19 слоев фильтра, приблизительно равна 2^{-6}.

Пара X_t^g, Y_t^g, частично расшифрованная с правильным подключом, подчиняется указанному дифференциалу, поэтому вероятность того, что $P_t^g \oplus Q_t^g = (\alpha_t^g, ?, ?, ?)$, равна 2^{-17}, а вероятность возникновения такой разности среди 2^{20} пар приблизительно равна 0,999665 (см. распределение Пуассона [11]). Значит, вероятность возникновения такой разности в 19 группах одновременно примерно равна 0,9936.

Нахождение оставшихся подключей. После того как 222-битовый подключ (состоящий из подключей 6 раундов) найден, необходимо расшифровать хранящиеся в памяти шифртексты на 6 последних раундов. Затем провести аналогичную атаку, перебирая раундовые подключи один за другим. Каждый раунд содержит два подключа: 5-битовый и 32-битовый, значит, перебор в этих случаях составляет 2^{37} вместо 2^{222}, поэтому сложность атаки в целом решающим образом зависит от сложности нахождения 222-битового подключа. Для реализации атаки необходимо примерно

2^{247} частичных шестираундовых расшифрований, что эквивалентно 2^{244} полных 48-раундовых шифрований. Также требуется примерно 2^{24} выбранных открытых текстов и 2^{29} байт памяти для хранения их и все α_t^g.

Во избежание ошибок данная атака была реализована в упрощенном виде. Предполагалось, что все, за исключением 19 бит, были известны (аналогично сделано в [12]), и эти биты были успешно найдены для 10 случайно выбранных ключей.

Заключение

В работе описана дифференциальная атака на шифр CAST-256, которая является более эффективной, чем ранее известные атаки на этот шифр. Данная атака основана на усеченной дифференциальной характеристике, покрывающей 18 раундов шифра.

СПИСОК ЛИТЕРАТУРЫ:

1. Advanced Encryption Standard (AES) project. 1997-2000. URL: http://csrc.nist.gov/encryption/aes.
2. New European Schemes for Signatures, Integrity, and Encryption. Deliverables of the NESSIE project. 2003. URL: https://www.cosic.esat.kuleuven.be/nessie/.
CRYPTREC project. 2000-2002. URL: http://www.cryptrec.go.jp/english/.
3. *Schneier B.* A Self-study course in block-cipher cryptanalysis // Cryptologia. 2000. Vol. 24. № 1. P. 18–34.
4. *Adams C.* The CAST-256 Encryption Algorithm. AES submission. 1998. URL: www.networkdls.com/Articles/cast-256.pdf.
5. *Wagner D.* The boomerang Attack // Proc. of Fast Software Encryption'99. Lecture Notes in Computer Science. Springer-Verlag. 1999. Vol. 1636. P. 156–170.
6. *Seki H., Kaneko T.* Differential Cryptanalysis of CAST-256 Reduced to Nine Quad-Rounds // IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2001. Vol. E84-A. № 4. P. 913–918.
7. *Biham E., Shamir A.* Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. 1991. Vol. 4. P. 3–72.
8. *Knudsen L.* Truncated and higher order differentials // Proc. of Fast Software Encryption'94. Lecture Notes in Computer Science. Springer-Verlag. 1995. Vol. 1008. P. 196–211.
9. *Biryukov A., Kushilevitz E.* Improved cryptanalysis of RC5 // Proc. of Eurocrypt'98. Lecture Notes in Computer Science. Springer-Verlag. 1998. Vol. 1403. P. 85–99.
10. *Боровков А. А.* Теория вероятностей. М.: Наука, 1976. – 352 с.
11. *Daemen J., Knudsen L., Rijmen V.* The block cipher SQUARE // Proc. of Fast Software Encryption'97. Lecture Notes in Computer Science. Springer-Verlag. 1997. Vol. 1267. P. 149–165.