показателей сильной нелинейности и совершенности (таблица). Во всех экспериментах полученные оценки совпали для каждого из рассмотренных блочных алгоритмов.

Оценки показателей сильной нелинейности и совершенности

n	m	$\exp\Gamma(g)$	$\operatorname{esn} A$	$\operatorname{epf} A$
8	3	4	3	7
15	5	4	3	7
16	5	7	4	8
32	9	7	4	8
33	11	4	3	6

Таким образом, при равноудалённом (или приблизительно равноудалённом) размещении обратных связей на регистре сдвига:

1) число раундов для достижения алгоритмом сильной нелинейности ($\operatorname{esn} A$) близко к величине n/m;
2) число раундов для достижения алгоритмом совершенности ($\operatorname{epf} A$) не меньше γ и не больше 2γ, где $\gamma = 2\exp\Gamma(g)$;
3) число раундов шифрования при синтезе шифров данного класса целесообразно установить не меньше $2\exp\Gamma(g)$.

ЛИТЕРАТУРА

1. *Фомичёв В. М., Мельников Д. А.* Криптографические методы защиты информации. Ч. 1. Математические аспекты: учебник для академического бакалавриата. М.: Юрайт, 2016. 209 с.
2. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.

УДК 519.7 DOI 10.17223/2226308X/11/24

ПРОПОЗИЦИОНАЛЬНОЕ КОДИРОВАНИЕ ПРЯМЫХ И ОБРАТНЫХ РАУНДОВЫХ ПРЕОБРАЗОВАНИЙ В АТАКАХ НА НЕКОТОРЫЕ БЛОЧНЫЕ ШИФРЫ[1]

И. В. Отпущенников, А. А. Семёнов, О. С. Заикин

Описывается атака на блочные шифры, основанная на известной концепции «встреча посередине». В рамках предлагаемой атаки для решения уравнений криптоанализа используются алгоритмы решения проблемы булевой выполнимости. Основное нововведение заключается в том, что в пропозициональной кодировке шифра учитывается информация не только от прямых, но и от обратных раундовых преобразований. Для ряда сокращённых по числу раундов блочных шифров построены оценки трудоёмкости атак из класса «угадывай и определяй» с использованием нового принципа кодирования. В некоторых случаях новые атаки оказались в разы эффективнее аналогов, в которых используются стандартные методы кодирования.

Ключевые слова: *блочный шифр, ГОСТ 28147-89, DES, PRESENT, криптоанализ, задача булевой выполнимости.*

[1]Работа поддержана грантом РНФ № 16-11-10046. Дополнительно И. В. Отпущенников поддержан Советом по грантам при Президенте РФ (стипендия № СП-4751.2016.5).

Современные блочные шифры — это симметричные криптографические алгоритмы, преобразующие дискретную информацию посредством простых операций над битами. Основными такими операциями являются перестановки и подстановки (соответственно линейная и нелинейная компоненты шифрующего преобразования). Композиции этих (и некоторых других) операций объединяются в раунды. Каждый раунд можно считать базовым блоком алгоритма, поскольку два различных раунда устроены одинаково в смысле своей алгоритмической природы. Число раундов, обозначаемое далее через N, может существенно варьироваться от шифра к шифру (например, $N = 16$ для DES, $N = 32$ для ГОСТ 28147-89, $N = 31$ в случае PRESENT, $N = 10$ в случае AES-128 и т. д.). Каждый раунд вносит свой вклад в обеспечение рассеивания и перемешивания информации, содержащейся в открытом тексте и секретном ключе. Если ключ выбран случайно (в соответствии с равномерным распределением на множестве возможных ключей), то результатом нескольких качественных раундовых преобразований будет криптограмма, статистически неотличимая от случайного слова.

Итак, пусть F — блочный шифр, состоящий из N раундов. Далее будем рассматривать представление F в виде, который назовём регистровой моделью данного шифра. Будем предполагать, что изначально открытый текст и секретный ключ записаны в два регистра (в виде двоичных слов) соответствующих длин. Регистр, в котором хранится секретный ключ, обозначим R_z. Для состояний второго регистра будем использовать обозначение R^i, $i \in \{0, 1, \ldots, N\}$. Полагаем, что состояние R^0 хранит открытый текст x, а состояние R^N — криптограмму y. Для каждого $i \in \{1, \ldots, N\}$ имеет место

$$R^i = f_i\left(z_i, R^{i-1}\right), \tag{1}$$

где f_i — шифрующее преобразование раунда с номером i (i-я раундовая функция), а z_i — некоторое подмножество бит регистра R_z (раундовый ключ). Будем рассматривать только такие шифры, в которых блок открытого текста и блок шифртекста имеют одинаковую длину n.

Пусть y — произвольная криптограмма. Процедуре её расшифрования соответствуют следующие соотношения:

$$R^{N-j} = f_{N-j+1}^{-1}\left(z_{N-j+1}, R^{N-j+1}\right), \quad j \in \{1, \ldots, N\}. \tag{2}$$

Функции вида f_i^{-1}, $i \in \{1, \ldots, N\}$, совпадают с f_i для фейстелевых шифров и отличны от f_i для шифров, основанных на SP-сети.

Далее будем использовать для криптоанализа шифра F, относящегося к описанному классу, подход, основанный на алгоритмах решения проблемы булевой выполнимости (SAT) [1]. Более конкретно, речь пойдёт о поиске секретного ключа на основе одной или нескольких известных пар блоков открытых текстов и соответствующих криптограмм. Применение SAT-подхода для решения этой задачи на первом этапе предполагает пропозициональное кодирование алгоритма, задающего F. Для этой цели можно использовать автоматические трансляторы алгоритмов в SAT. В наших экспериментах использовался программный комплекс TRANSALG [2, 3]. Применительно к описанному классу шифров мы рассмотрели два способа сведения задач их криптоанализа к SAT. Первый способ, называемый далее стандартным, уже использовался ранее в целом ряде работ в рамках направления, известного как «SAT-based cryptanalysis» (см., например, [4 – 7] и др.). Этот способ подразумевает кодирование в КНФ последовательности раундовых преобразований вида (1). Затем в построенную формулу подставляются известные открытый текст и криптограмма. Если полученную SAT-задачу удаётся решить, то из найденного выполняющего набора можно эффективно выделить искомый

секретный ключ. Второй способ, кратко описанный далее, является, насколько нам известно, новым.

Представим N в виде $N = N_1 + N_2$, где $N_1, N_2 \geqslant 1$ — натуральные числа. Пусть R^{N_1} — состояние второго регистра, которое хранит результат применения к открытому тексту x и секретному ключу z первых N_1 раундов шифрования в соответствии с соотношениями (1). Двоичное слово, хранящееся в R^{N_1}, — это значение дискретной функции вида

$$F_{N_1}\colon \{0,1\}^n \times \{0,1\}^{|z|} \to \{0,1\}^n,$$

где через $|z|$ обозначена длина секретного ключа. Построим КНФ $C\left(F_{N_1}\right)$, кодирующую алгоритм вычисления функции F_{N_1}. Пусть $\{u_1, \ldots, u_n\}$ — булевы переменные в $C\left(F_{N_1}\right)$, которые кодируют выход F_{N_1}. Теперь рассмотрим первые N_2 шагов расшифрования криптограммы y в соответствии с соотношениями (2). По аналогии со сказанным выше имеем функцию

$$F_{N_2}^{-1}\colon \{0,1\}^n \times \{0,1\}^{|z|} \to \{0,1\}^n$$

и КНФ $C\left(F_{N_2}^{-1}\right)$, кодирующую алгоритм её вычисления. Пусть $\{v_1, \ldots, v_n\}$ — булевы переменные, кодирующие выход $C\left(F_{N_2}^{-1}\right)$. Рассмотрим формулу

$$C(F) = C\left(F_{N_1}\right) \wedge C\left(F_{N_2}^{-1}\right) \wedge (u_1 \equiv v_1) \wedge \ldots \wedge (u_n \equiv v_n), \tag{3}$$

где через $\equiv$ обозначена логическая эквивалентность. Отталкиваясь от стандартных свойств процедур пропозиционального кодирования, несложно показать, что формула $C(F)$ выполнима, и из выполняющего её набора можно эффективно извлечь секретный ключ z, применение которого (в рамках шифрующего алгоритма F) к открытому тексту x даёт криптограмму y. При этом формула (3), в отличие от стандартной кодировки, содержит дополнительную информацию, порождённую кодированием процедуры расшифрования. Отметим, что при $N_1 = N_2$ задачу поиска набора, выполняющего формулу (3), можно рассматривать как «SAT-вариант метода встречи посередине» в применении к криптоанализу шифра F на основе известного текста и криптограммы.

Используя описанную процедуру кодирования в SAT как прямых, так и обратных раундовых преобразований, мы построили атаки из класса «угадывай и определяй» (guess and determine, [5]) для ряда урезанных по числу раундов блочных шифров. Конкретно, рассмотрены 6-раундовая версия шифра DES (DES-6), 6- и 8-раундовые версии шифра ГОСТ 28147-89 (ГОСТ-6, ГОСТ-8) и 6-раундовая версия шифра PRESENT (PRESENT-6). Для оценивания трудоёмкости атак был использован метод [8], который строит оценки трудоёмкости «SAT-разбиений» трудных вариантов SAT. Для этой цели применяется стохастическое оценивание каждого конкретного разбиения, а процедура поиска разбиения с хорошей оценкой трудоёмкости организована в виде процедуры оптимизации оценочной функции специального вида. Данная оценочная функция, как отмечено в [7], является конкретизацией понятия «UNSAT-иммунность», введённого Н. Куртуа в [6]. Для вычислительных расчётов использовались средства PDSAT [9] и ALIAS [10], которые запускались на кластере ИДСТУ СО РАН «Академик В. М. Матросов» (`http://hpc.icc.ru/`).

Таблица содержит оценки трудоёмкости (в секундах) для атак, использующих стандартную процедуру кодирования в SAT (отмечена как Standard) и процедуру, представленную в настоящей работе (отмечена как Middle).

Процедура	DES-6	ГОСТ-6	ГОСТ-8	PRESENT-6
Standard	$9{,}99 \cdot 10^7$	$7{,}86 \cdot 10^8$	$2{,}30 \cdot 10^{26}$	$8{,}72 \cdot 10^{14}$
Middle	$7{,}28 \cdot 10^7$	$7{,}15 \cdot 10^8$	$3{,}24 \cdot 10^{24}$	$2{,}16 \cdot 10^{14}$

Комментарии. На первый взгляд, процедура кодирования обратных преобразований не даёт существенного выигрыша (за исключением, пожалуй, 8-раундовой версии шифра ГОСТ 28147-89, где выигрыш составил около 100 раз). Тем не менее описанный метод демонстрирует весьма интересный феномен. Множества угадываемых бит (guessed bits, [5]), которые построены для кодировки типа Middle, содержат не только переменные, кодирующие биты неизвестного секретного ключа, но и ряд вспомогательных переменных, вводимых при переходе от формулы (3) к КНФ. Авторам не известны другие атаки из класса «угадывай и определяй», для которых наблюдается данное свойство. В заключение отметим, что описанная атака на 6-раундовый вариант шифра PRESENT превосходит по эффективности лучшую из известных нам атак данного типа [11].

ЛИТЕРАТУРА

1. *Biere A., Heule M., van Maaren H., and Walsh T. (eds.)* Handbook of Satisfiability, Frontiers in Artificial Intelligence and Applications. V. 185. IOS Press, 2009.
2. *Отпущенников И. В., Семенов А. А.* Технология трансляции комбинаторных проблем в булевы уравнения // Прикладная дискретная математика. 2011. № 1. С. 96–115.
3. *Otpuschennikov I., Semenov A., Gribanova I., et al.* Encoding cryptographic functions to SAT using Transalg system // Frontiers in Artificial Intelligence and Applications. 2016. V. 285. P. 1594–1595.
4. *Massacci F. and Marraro L.* Logical cryptanalysis as a SAT problem // J. Automated Reasoning. 2000. V. 24(1/2). P. 165–203.
5. *Bard G. V.* Algebraic Cryptanalysis. Springer, 2009.
6. *Courtois N. T., Gawinecki J. A., and Song G.* Contradiction immunity and guess-then-determine attacks on GOST // Tatra Mountains Math. Publ. 2012. V. 53(1). P. 2–13.
7. *Semenov A., Zaikin O., Otpuschennikov I., et al.* On cryptographic attacks using backdoors for SAT // Proc. AAAI Conf. 2018. P. 6641–6648.
8. *Semenov A. and Zaikin O.* Algorithm for finding partitionings of hard variants of Boolean satisfiability problem with application to inversion of some cryptographic functions // SpringerPlus. 2016. V. 5(1). P. 1–16.
9. *Заикин О. С., Семенов А. А.* Применение метода Монте-Карло к прогнозированию параллельного времени решения проблемы булевой выполнимости // Вычислительные методы и программирование. 2014. Т. 15. С. 22–35.
10. *Kochemazov S. and Zaikin O.* ALIAS: A modular tool for finding backdoors for SAT // Proc. SAT Conf. 2018. (to be published)
11. *Yeo S., Li Z., Khoo K., and Low Y.* An enhanced binary characteristic set algorithm and its applications to algebraic cryptanalysis // LNCS. 2017. V. 10355. P. 518–536.

УДК 519.7 DOI 10.17223/2226308X/11/25

О НЕАБЕЛЕВЫХ ГРУППАХ НАЛОЖЕНИЯ КЛЮЧА И МАРКОВОСТИ АЛГОРИТМОВ БЛОЧНОГО ШИФРОВАНИЯ

Б. А. Погорелов, М. А. Пудовкина

Для абелевой группы наложения ключа $(X, *)$ и разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X ранее авторами рассматривались $*_{\mathbf{W}}$-марковские преобразования и