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

$*_{\mathbf{W}}$-марковские алгоритмы, частным случаем которых являются $*$-марковские алгоритмы блочного шифрования, представленные на конференции EUROCRYPT в 1991 г. В данной работе для неабелевой группы $(X, *)$ описываются свойства $*_{\mathbf{W}}$-марковских алгоритмов и преобразований. Получены ограничения на строения групп $(X, *)$, $\langle g_k | k \in X\rangle$, а также на блоки $W_0, \ldots, W_{r-1}$, вытекающие из условия сохранения частичной раундовой функцией $g_k : X \to X$ нетривиального разбиения $\mathbf{W}$ для каждого $k \in X$. Для всех неабелевых групп порядка 2^m, имеющих циклическую подгруппу индекса два, приведены примеры $*_{\mathbf{W}}$-марковских подстановок.

Ключевые слова: *марковский алгоритм блочного шифрования, гомоморфизм, группа диэдра, обобщённая группа кватернионов, матрица разностей переходов, импримитивная группа.*

Пусть $(X, *)$ — произвольная группа на множестве X с бинарной операцией $*$ и единичным элементом e; $\alpha^b = \alpha b = b(\alpha)$ — образ элемента $\alpha \in X$ при действии на него подстановкой $b \in S(X)$. Рассмотрим l-раундовый алгоритм блочного шифрования $\mathrm{C}_l(*, b)$, у которого раундовая функция $g : X^2 \to X$, определяемая подстановкой $b \in S(X)$, задана условием

$$g : (x, k) \mapsto (x * k)^b \text{ для всех } (x, k) \in X^2.$$

Раундовой функции g соответствуют частичные функции $g_k : X \to X$, где $g(x, k) = g_k(x)$ для каждых $(x, k) \in X^2$. Заметим, что к данному классу относятся XSL-алгоритмы блочного шифрования, у которых $b = sh$, где s — преобразование слоя перемешивания (s-боксы); h — преобразование линейного слоя. Неабелевость группы наложения ключа позволяет в некоторых случаях повышать стойкость алгоритмов блочного шифрования относительно линейного и разностного методов.

Пусть K — множество всех раундовых ключей итерационного алгоритма блочного шифрования (в данной работе $K = X$). Для $\theta, \varepsilon \in X$ положим

$$\hat{p}_{\theta,\varepsilon}(b) = |X|^{-1} \left| \left\{ \alpha \in X : (\theta * \alpha)^b = \varepsilon * \alpha^b \right\} \right|.$$

Зафиксируем произвольное нетривиальное разбиение $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$ множества X, $e \in W_0$. Положим

$$\hat{p}_{\theta,W_c}(b) = \sum_{\theta' \in W_c} \hat{p}_{\theta,\theta'}(b),\ \theta \in X,\ c \in \{0, \ldots, r-1\}.$$

В [1] введено понятие $*$-марковского алгоритма блочного шифрования, а в [2] — $*_{\mathbf{W}}$-марковского алгоритма блочного шифрования и $*_{\mathbf{W}}$-марковского преобразования.

Определение 1. Преобразование $b \in S(X)$ называется $*_{\mathbf{W}}$-марковским для разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, $|X| \geqslant r \geqslant 2$, если $\hat{p}_{\theta,W_c}(b) = a_{j,c}$ для каждых $(j, c) \in \{0, \ldots, r-1\}^2$, $\theta \in W_j$ и некоторых $a_{j,c}$, $0 \leqslant a_{j,c} \leqslant 1$.

Условие $*_{\mathbf{W}}$-марковости алгоритма $\mathrm{C}_l(*, b)$ равносильно $*_{\mathbf{W}}$-марковости подстановки b.

Рассмотрим преобразование $\sigma_k \in S(X)$, заданное условием $\sigma_k : x \mapsto x * k$ для каждого $k \in X$, и группу $X^* = \langle \sigma_k | k \in X\rangle$. Пусть $\rho : X \to S(X)$ — правое регулярное представление группы $(X, *)$. Очевидно, что $\rho(X) = X^*$ и $\rho(k) = \sigma_k$ для каждого $k \in X$; $g_k = \sigma_k b$ для каждого $k \in X$.

Будем говорить, что *раундовая функция g сохраняет разбиение* $\mathbf{W}$ *справа*, если $W^{g_k} \in \mathbf{W}$ для всех $(W,k) \in \mathbf{W} \times X$.

Получены ограничения на группы $(X,*)$, $G = \langle b, X^* \rangle$, а также на блоки $W_0, \ldots, W_{r-1}$, вытекающие из условия сохранения раундовой функцией нетривиального разбиения $\mathbf{W}$. Доказано, что $\mathbf{W}$ — система импримитивности группы G. Кроме того, показано, что $(W_0,*)$ — подгруппа группы $(X,*)$, причём W_j — j-й правый смежный класс группы $(X,*)$ по $(W_0,*)$ для $j = 0, \ldots, r-1$.

Из импримитивности группы G следуют включения

$$b \in \mathrm{IG}_{\mathbf{W}}, \quad \langle g_k | k \in X \rangle \leqslant \mathrm{IG}_{\mathbf{W}},$$

где $\mathrm{IG}_{\mathbf{W}}$ — максимальная подгруппа группы $S(X)$, сохраняющая разбиение $\mathbf{W}$.

Если группа $G = \langle b, X^* \rangle$ импримитивна с системой импримитивности $\mathbf{W}$, то существует естественный гомоморфизм $\varphi_{\mathbf{W}} : G \to S(\{0, \ldots, r-1\})$, $1 = \varphi_{\mathbf{W}}(e)$. Доказано, что если $(W_0,*)$ нормальна в $(X,*)$ ($(W_0,*) \lhd (X,*)$), $\mathbf{W}$ — множество всех смежных классов группы $(X,*)$ по $(W_0,*)$, то условие $*_{\mathbf{W}}$-марковости алгоритма $\mathrm{C}_l(*,b)$ эквивалентно существованию у него гомоморфизма, задаваемого отображением $\varphi_{\mathbf{W}}$.

Для криптографических приложений представляют интерес группы порядка 2^m. В [3, теорема 12.5.1] описаны все неабелевы группы порядка 2^m, обладающие циклической подгруппой индекса два. Таких групп всего четыре, включая группу диэдра и обобщённую группу кватернионов. Для всех четырёх групп описаны $*_{\mathbf{W}}$-марковские подстановки из $S(X)$ относительно разбиения $\mathbf{W} = \{W_0, \ldots, W_{r-1}\}$, блоками которого являются все правые смежные классы группы $(X,*)$ по подгруппе $(W_0,*)$, но $(W_0,*) \not\lhd (X,*)$.

ЛИТЕРАТУРА

1. *Lai X., Massey J. L., and Murphy S.* Markov ciphers and differential cryptanalysis // EUROCRYPT 1991. LNCS. 1991. V. 547. P. 17–38.
2. *Погорелов Б. А., Пудовкина М. А.* Разбиения на биграммах и марковость алгоритмов блочного шифрования // Математические вопросы криптографии. 2017. Т. 8. № 1. С. 107–142.
3. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.

УДК 519.7 DOI 10.17223/2226308X/11/26

АТАКИ ИЗ КЛАССА «УГАДЫВАЙ И ОПРЕДЕЛЯЙ» И АВТОМАТИЧЕСКИЕ СПОСОБЫ ИХ ПОСТРОЕНИЯ[1]

А. А. Семёнов

Представлен краткий обзор подходов к построению криптографических атак, относящихся к классу «угадывай и определяй». Основной акцент сделан на относительно недавних работах, в которых описаны автоматические способы построения таких атак с ипользованием алгоритмов решения проблемы булевой выполнимости (SAT). С этой целью задачи построения атак из рассматриваемого класса ставятся как задачи оптимизации на булевом гиперкубе специальных оценочных функций. Для решения последних используются метаэвристические алгоритмы, широко применяемые в дискретной оптимизации. В упомянутых работах введены два типа оценочных функций, которые можно рассматривать как конкретиза-

[1]Работа выполнена при финансовой поддержке Российского научного фонда, проект № 16-11-10046.