УДК 519.7

М.А. ПУДОВКИНА, С.В. СВЕТЛОВ

Национальный исследовательский ядерный университет «МИФИ», Москва

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ РАЗНОСТНОЙ ХАРАКТЕРИСТИКИ В НЕКОТОРЫХ КОНЕЧНЫХ ГРУППАХ

В работе экспериментально исследуется наибольший элемент матрицы переходов разностей для случайного биективного отображения и подстановок, применяемых в различных алгоритмах шифрования. Разностная характеристика рассматривается над группами, представимыми прямым произведением групп, используемых в криптографии.

Развитие общего подхода [1] в работе [2], позволило построить атаки на блочные шифры Midori и Scream при помощи введенной разностной характеристики (аффинная равномерность). Одной из задач, возникающих в таких исследованиях, является изучение этой характеристики для нелинейного компонента шифра (S-блока).

В статье [3] проведено экспериментальное исследование разностной характеристики биективных отображений относительно различных групп. В настоящей работе предлагается рассмотрение дифференциальной характеристики в конечных группах, являющихся прямым произведением некоторых групп, естественных для криптографической практики [4].

Пусть $s: G \to G$ – биективное отображение, $\mathrm{q}^{(\circ,\circ)}(s) = \| q_{\epsilon,\delta}^{(\circ,\circ)}(s) \|$ – матрица переходов разностей, элементы которой заданы условием

$$q_{\epsilon,\delta}^{(\circ,\circ)}(s) = |\{\alpha \in G: s(\alpha \circ \epsilon) = s(\alpha) \circ \delta\}|,$$

$$(G,\circ) = (H_1,*_1) \times (H_2,*_2),$$

$$(H_i,*_i) \in \{(V_{2^{m/2}},\oplus), (Z_{2^{m/2}},+), (Z_{2^{m/2}+1},\odot), (H_1,*_1) \neq (H_2,*_2)\}.$$

Будем рассматривать значение $q^{(\circ,\circ)}(s) = \max\{ q_{\epsilon,\delta}^{(\circ,\circ)}(s) : \epsilon,\delta \in G^{\times} \}$. В табл. 1 приведены значения характеристики для 8-битных подстановок, используемых в различных шифрах.

Для каждого случая была сгенерирована выборка из 1000000 8-битных подстановок. Для каждой выборки рассчитано выборочное среднее значение характеристики. Результаты экспериментов приведены в табл. 2.

Таблица 1. Значение характеристики для известных S-блоков

S-box	$(\oplus,+)$	$(+,\oplus)$	$(\oplus,\odot)$	$(\odot,\oplus)$	$(+,\odot)$	$(\odot,+)$
AES	5	6	7	8	7	7
BelT	6	7	8	8	7	8
Fantomas	16	20	32	16	9	8
iScream	20	16	20	12	9	9
Kalyna pi0	7	8	7	7	8	7
Kalyna pi1	6	7	8	7	7	7
Kalyna pi2	8	7	7	8	7	7
Kalyna pi3	7	7	8	9	7	7
Khazad	8	8	10	10	11	14
Kuznechick	8	7	7	8	8	7
Liliput_AE	10	9	12	9	12	8
Picaro	6	7	6	10	9	13
SMS4	8	7	8	8	9	8
Safer	32	16	224	8	28	11
Scream	10	15	12	10	8	7
Snow 3G	8	8	8	8	7	8
TEA1	10	10	8	10	7	8
TEA2	10	12	8	12	7	7
ZUC_S0	8	12	16	8	9	7
ZUC_S1	7	6	6	7	7	7

Таблица 2. Выборочное среднее значение характеристики

$(\oplus,+)$	$(+,\oplus)$	$(\oplus,\odot)$	$(\odot,\oplus)$	$(+,\odot)$	$(\odot,+)$
8,231	8,240	8,231	8,241	7,281	7,280

Список литературы

1. Wagner D., “Towards a Unifying View of Block Cipher Cryptanalysis”. In: Roy, B., Meier, W. (eds) Fast Software Encryption. FSE 2004. Lecture Notes in Computer Science, vol 3017. Springer, Berlin, Heidelberg. DOI: https://doi.org/10.1007/978-3-540-25937-4_2

2. Baudrin J., Felke P., Leander G., Neumann P., Perrin L., Stennes L., “Commutative Cryptanalysis Made Practical”. 2023. *IACR Transactions on Symmetric Cryptology* 2023 (4): 299-329. DOI: https://doi.org/10.46586/tosc.v2023.i4.299-329.

3. Власова В.В., Пудовкина М.А. “О свойствах максимального элемента матрицы вероятностей переходов разностей биективного отображения относительно различных групповых операций”, *ПДМ. Приложение*, 2019, № 12, p. 203–205, DOI: https://doi.org/10.17223/2226308X/12/57.

4. Погорелов Б.А., Пудовкина М.А., “О группах, порождённых преобразованиями смешанного типа и группами наложения ключа”, *ПДМ. Приложение*, 2016, № 9, p. 14–16, DOI**:** https://doi.org/10.17223/2226308X/9/5