(многогранник) в многомерном евклидовом пространстве. Многогранник P^ℓ описан как выпуклая оболочка вершин. Справедливо

Утверждение 2. Если $\ell_1 < \ell_2$, то для соответствующих многогранников P^{ℓ_1} и P^{ℓ_2} выполняется условие $P^{\ell_1} \subset P^{\ell_2}$, то есть многогранники P^ℓ для ℓ-грамм при разных ℓ вложены в друг друга.

Итак, показано, что изучение неэндоморфных шифров сводится к изучению максимальных неэндоморфных шифров. При этом распределения вероятностей на l-граммах могут рассматриваться и как независимые, что характерно для блочных шифров, и как порождённые режимом гаммирования. Справедлива

Теорема 2. Совершенными максимальными шифрами являются шифры с вероятностями ключей $P(K^\ell)$ из многогранника P^ℓ, и только они.

Данная теорема является аналогом теоремы К. Шеннона, доказанным для общего класса неэндоморфных неминимальных шифров.

ЛИТЕРАТУРА

1. *Шеннон К.* Терия связи в секретных системах // Работы по теории информации и кибернетике. М.: Наука, 1963. С. 333–402.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001.
3. *Зубов А. Ю.* Совершенные шифры. М.: Гелиос АРВ, 2003.
4. *Титов С. С., Гутарин Д. С., Коновалова С. С. и др.* Комбинаторные проблемы существования совершенных шифров // Труды ИММ УрО РАН. 2008. Т. 13. №4. С. 61–73.
5. *Медведева Н. В., Тимофеева Г. А.* Сравнение линейных и нелинейных методов доверительного оценивания для статистически неопределенных систем // Автоматика и телемеханика. 2007. №4. С. 51–60.

УДК 519.7

О СВЯЗЯХ МЕЖДУ ОСНОВНЫМИ ПОНЯТИЯМИ РАЗНОСТНОГО АНАЛИЗА ИТЕРАТИВНЫХ БЛОЧНЫХ ШИФРОВ

А. И. Пестунов

Обозначаются некоторые из проблем и несоответствий в существующей терминологии разностного анализа итеративных блочных шифров. Предлагается один из возможных наборов определений, позволяющий сформировать единообразную систему понятий, которая согласована с существующими терминами. Формализованы соответствия между основными понятиями, в частности показано, что в рамках предлагаемого набора определений дифференциал, характеристика и усечённый дифференциал являются усечёнными характеристиками. Формализовано и обобщено понятие объединения дифференциалов и характеристик.

Ключевые слова: *терминология, дифференциальный криптоанализ, разностный анализ, блочный шифр, дифференциал, характеристика.*

Разностный (дифференциальный) анализ [1] — это распространённый подход к анализу стойкости итеративных блочных шифров, однако несмотря на его популярность и наличие ряда разновидностей [2 – 5] к настоящему времени не выработана строгая единообразная терминология, его описывающая: основные понятия вводятся либо не строго, либо с использованием авторских определений. Такая ситуация не мешает разраба-

тывать атаки на шифры, но приводит к тому, что одни и те же понятия определяются по-разному даже признанными учёными. Кроме того, отсутствуют формализованные связи между основными понятиями данного метода: характеристики могут называться дифференциалами, дифференциалы могут объединяться с характеристиками, вероятность усечённой характеристики может вычисляться по аналогии с неусечённой, хотя корректность подобных действий строго не обоснована.

Некоторые проблемы теоретического обоснования разностного анализа уже затрагивались в работах отечественных и зарубежных авторов. В [6] предложена модель марковского шифра и сформулирована гипотеза стохастической эквивалентности, в [7] предложена модель для создания шифра, доказуемо стойкого к классическим вариантам разностного и линейного анализа. Работа [8] посвящена изложению разностного анализа в общем виде применительно к произвольным итеративным блочным шифрам с аддитивным раундовым ключом, в работе [9] теоретически исследована вероятность сохранения однобитовой разности после сложения и вычитания. Автор [10] аналитически вычисляет вероятность успеха разностной атаки в зависимости от параметров блочных шифров. Заметим также, что отечественные учёные уже обращались к выработке общей криптографической терминологии, хотя разностный анализ детально не затрагивался [11, 12].

Рассмотрим некоторые вопросы, возникающие при изучении существующей терминологии разностного анализа. Мы не будем классифицировать эти вопросы, а только покажем, что существуют вполне конкретные несоответствия.

Вопрос 1. Входит ли шифр в определения дифференциала и характеристики? Вопрос возникает в связи с тем, что одни авторы определяют дифференциалы и характеристики соответственно как пару или набор блоков (чисел) [1], а другие говорят о разностях открытых и шифрованных текстов [3, 6]. В первом случае дифференциалы и характеристики, состоящие из одинаковых разностей, могут относиться к разным шифрам, а во втором случае подразумевается конкретизация шифра.

Вопрос 2. Входит ли вероятность в определения дифференциалов и характеристик? В исходной работе по разностному анализу [1] характеристика определяется как набор разностей и только затем вводится понятие вероятности характеристики применительно к конкретному шифру. В то же время автор [8] определяет характеристику как последовательность, состоящую и из разностей, и из вероятностей.

Вопрос 3. Является ли объединение дифференциалов характеристикой? Во многих работах авторы строят дифференциалы и характеристики, называя похожие объекты по-разному. Например, в работе [13] объект

$$(a, b, 0, c) \xrightarrow{\text{8 раундов}} (e, e, 0, 0) \xrightarrow{\text{8 раундов}} (g, h, f, 0)$$

назван усечённой характеристикой, а объект

$$(0, a, 0, 0) \xrightarrow{\text{8 раундов}} (0, b, c, d) \xrightarrow{\text{4 раунда}} (h, h, f, g)$$

— уже усечённым дифференциалом.

Вопрос 4. Можно ли объединять дифференциал и характеристику? В работе [1] даётся определение объединения двух характеристик. В более поздних работах [3, 6] появились понятия дифференциала, а также усечённых дифференциалов и характеристик, однако строгих определений объединения этих объектов не введено. Другими словами, не даются ответы на вопросы о возможности объединения усечённых и неусечённых характеристик и дифференциалов.

Вопрос 5. Как вычислять вероятность объединения усечённых характеристик и дифференциалов? В [6] вводится понятие марковского шифра и показывается, что, согласно уравнению Колмогорова — Чепмена, вероятность характеристики для такого шифра равна произведению вероятностей характеристик, из которых она состоит. Для усечённых характеристик и дифференциалов такого утверждения нет.

Вопрос 6. Является ли дифференциал характеристикой? В работе [6] отмечено, что одноraундовые дифференциал и характеристика «совпадают». Отсюда вытекает актуальность установления соответствий между характеристиками и дифференциалами вне зависимости от числа раундов, а также установления соответствий между ними и их усечёнными аналогами.

Список перечисленных вопросов может быть расширен, но и его достаточно, чтобы увидеть существующие проблемы. В настоящей работе предлагается один из возможных наборов определений, позволяющий сформировать единообразную систему понятий, которая согласована с существующими терминами. Формализованы соответствия между основными понятиями, в частности показано, что в рамках предлагаемого набора определений дифференциал, характеристика и усечённый дифференциал являются усечёнными характеристиками. Формализовано и обобщено понятие объединения дифференциалов и характеристик.

Основной идеей, лежащей в основе предлагаемой системы понятий, является использование масок для работы с неизвестными битами в усечённых разностях.

Определение 1. Пусть $I = \{r_0, \ldots, r_T\} \subseteq \{0, 1, \ldots, R\}$, где $T \leqslant R$, причём $r_0 = 0$ и $r_T = R$. Пусть также $\Delta = (\delta^{r_0}, \ldots, \delta^{r_T})$ и $M = (m^{r_0}, \ldots, m^{r_T})$ — упорядоченные множества, где $\delta^r \in \{0,1\}^s$, $m^r \in \{0,1\}^s$, $m^r \neq 0$ и $r \in I$. Тогда упорядоченная тройка (I, Δ, M) называется *R-раундовой усечённой характеристикой*. Обозначим её

$$(\delta^{r_0}, m^{r_0}) \xrightarrow{r_1 - r_0 \text{ раундов}} (\delta^{r_1}, m^{r_1}) \xrightarrow{r_2 - r_1 \text{ раундов}} \ldots \xrightarrow{r_T - r_{T-1} \text{ раундов}} (\delta^{r_T}, m^{r_T}).$$

В этом определении роли масок играют величины m^r. При $T = 1$ и, следовательно, $r_T = R$ и $I = \{r_0, r_1\}$ усечённая характеристика является усечённым дифференциалом, а при единичных масках усечённые характеристики и дифференциалы являются неусечёнными. Отсюда следует эквивалентность одноraундовых характеристик и дифференциалов. Свойство «усечённости» выражается не только в наличии масок, но и в том, что задействованы не все раунды. Часто маски имеют вид, подобный $(0^{32}, 1^{32}, 0^{32}, 1^{32})$, другими словами, все биты определённых подблоков масок равны 0 или 1 одновременно, поэтому усечённые характеристики обычно обозначаются следующим образом:

$$(?, a, ?, b) \to (?, ?, ?, c) \to (d, e, ?, f) \to (?, g, h, ?),$$

где $a, b, c, d, e, f, g, h \in \{0,1\}^l$, l — размер подблока.

Определение 2. Пусть E — R-раундовый блочный шифр с блоком размера s, (I, Δ, M) — R-раундовая усечённая характеристика и $p \in [0, 1]$. Будем говорить, что *шифр E допускает (имеет) усечённую характеристику (I, Δ, M) с вероятностью p*, если при случайно и независимо выбранных ключах раундов и блоках открытого текста C^0 и D^0 выполняется равенство

$$\mathrm{P}\big((C^{r_1} \oplus D^{r_1})\&m^{r_1} = \delta^{r_1}\&m^{r_1}, \ldots, (C^{r_T} \oplus D^{r_T})\&m^{r_T} = \\ = \delta^{r_T}\&m^{r_T} \big| (C^{r_0} \oplus D^{r_0})\&m^{r_0} = \delta^{r_0}\&m^{r_0}\big) = p.$$

Определение 3. Характеристика $(\widehat{I}, \widehat{\Delta}, \widehat{M})$ *присоединима* к $\widetilde{R}$-раундовой характеристике $(\widetilde{I}, \widetilde{\Delta}, \widetilde{M})$, если выполняются равенства $\widetilde{m}^{\widetilde{R}} = \widehat{m}^0$ и $\delta^{\widetilde{R}} \& m^{\widetilde{R}} = \widehat{\delta}^0 \& \widehat{m}^0$.

Определение 4. Пусть $H_1 = (\widetilde{I}, \widetilde{\Delta}, \widetilde{M})$ и $H_2 = (\widehat{I}, \widehat{\Delta}, \widehat{M})$ — соответственно $\widetilde{R}$- и $\widehat{R}$-раундовые усечённые характеристики, причём H_2 присоединима к H_1, тогда *объединением* H_1 и H_2 назовём характеристику $H = (I, \Delta, M)$, где $I = \{0 = \widetilde{r}_0, \ldots, \widetilde{r}_{\widetilde{T}} = \widetilde{R} + \widehat{r}_0, \widetilde{R} + \widehat{r}_1, \ldots, \widetilde{R} + \widehat{r}_{\widehat{T}} = \widetilde{R} + \widehat{R}\}$, $\Delta = (\widetilde{\delta}^{\widetilde{r}_0}, \ldots, \widetilde{\delta}^{\widetilde{r}_{\widetilde{T}}}, \widehat{\delta}^{\widehat{r}_1}, \ldots, \widehat{\delta}^{\widehat{r}_{\widehat{T}}})$ и $M = (\widetilde{m}^{\widetilde{r}_0}, \ldots, \widetilde{m}^{\widetilde{r}_{\widetilde{T}}}, \widehat{m}^{\widehat{r}_1}, \ldots, \widehat{m}^{\widehat{r}_{\widehat{T}}})$. По аналогии с операцией конкатенации будем использовать обозначение $H = H_1|H_2$.

Определение 5. Пусть дана последовательность усечённых характеристик H_1, …, H_L, для которых выполняется следующее свойство: H_{l+1} может быть присоединена к H_l, $l = 1, \ldots, L-1$. Тогда *объединением* L характеристик H_1, H_2, …, H_L называется характеристика $H = (\ldots((H_1|H_2)|H_3)|\ldots)|H_L$. Легко видеть, что определённая таким образом операция объединения ассоциативна, поэтому можно использовать запись $H = H_1|H_2|H_3|\ldots|H_L$.

Используя введённые определения, легко показать, что любую усечённую характеристику можно представить в виде объединения усечённых дифференциалов. Вычислить вероятность объединения усечённых характеристик можно с использованием уравнения Колмогорова — Чемпена по аналогии с тем, как это сделано в [6] для неусечёных характеристик.

Утверждение 1. Пусть марковский шифр E представим в виде композиции $E = E^1 \circ \ldots \circ E^L$, где E_l, $l = 1, \ldots, L$, могут быть раундами или композицией раундов. Пусть также E_l допускает некоторую характеристику H_l с вероятностью p_l. Тогда шифр E допускает характеристику $H = H_1|\ldots|H_L$ с вероятностью $p_1 \cdot \ldots \cdot p_L$.

Из этого утверждения следует очевидная справедливость общепринятого обозначения для характеристик, состоящих из нескольких дифференциалов:

$$\Delta_0 \xrightarrow[p_1]{} \Delta_1 \xrightarrow[p_2]{} \Delta_2 \xrightarrow[p_3]{} \ldots \xrightarrow[p_{L-1}]{} \Delta_{L-1} \xrightarrow[p_L]{} \Delta_L;$$

$$\Delta_{\text{in}} \xrightarrow[p]{\widetilde{R}\,\text{раундов}} \Delta_{\text{mid}} \xrightarrow[q]{\widehat{R}\,\text{раундов}} \Delta_{\text{out}}.$$

ЛИТЕРАТУРА

1. *Biham E. and Shamir A.* Differential cryptanalysis of DES-like cryptosystems // J. Cryptology. 1991. No. 4. P. 3–72.
2. *Пестунов А. И.* Блочные шифры и их криптоанализ // Вычислительные технологии. 2007. Т. 12. Спец. вып. № 4. С. 42–49.
3. *Knudsen L.* Truncated and higher order differentials // LNCS. 1995. V. 1008. P. 196–211.
4. *Biham E., Biryukov A., and Shamir A.* Cryptanalysis of Skipjack reduced to 31 round using impossible differentials // J. Cryptology. 2005. No. 18. P. 291–311.
5. *De Cannière C., Biryukov A, and Preneel B.* An introduction to block cipher cryptanalysis // Proc. IEEE. 2006. V. 94. No. 2. P. 346–356.
6. *Lai X. and Massey J.* Markov ciphers and differential cryptanalysis // LNCS. 1991. V. 547. P. 17–38.
7. *Vaudenay S.* Decorrelation: a theory for block cipher security // J. Cryptology. 2003. No. 16. P. 249–286.

8. *Агибалов Г. П.* Элементы теории дифференциального криптоанализа итеративных блочных шифров с аддитивным раундовым ключом // Прикладная дискретная математика. 2008. № 1. С. 34–42.
9. *Пестунов А. И.* О вероятности протяжки однобитовой разности через сложение и вычитание по модулю // Прикладная дискретная математика. 2012. № 4. С. 53–60.
10. *Selçuk A. A.* On probability of success in linear and differential cryptanalysis // J. Cryptology. 2007. No. 21. P. 131–147.
11. Словарь криптографических терминов / под ред. Б. А. Погорелова и В. Н. Сачкова. М.: МНЦМО, 2006. 94 с.
12. *Погорелов Б. А., Черемушкин А. В., Чечета С. И.* Об определении основных криптографических понятий // Доклад на конф. «Математика и безопасность информационных технологий», МаБИТ-03, МГУ, 23–24 октября 2003. М., 2003.
13. *Knudsen L. R., Robshaw M. J. B., and Wagner D.* Truncated differentials and Skipjack // LNCS. 1999. V. 1666. P. 165–180.

УДК 056.55

УЯЗВИМОСТЬ КРИПТОСИСТЕМЫ МАК-ЭЛИСА, ПОСТРОЕННОЙ НА ОСНОВЕ ДВОИЧНЫХ КОДОВ РИДА — МАЛЛЕРА

И. В. Чижов, М. А. Бородин

Предлагается новый алгоритм восстановления секретного ключа по открытому для криптосистемы Мак-Элиса, построенной на основе двоичных кодов Рида — Маллера $RM(r, m)$. В случае, если значение $d = (r, m-1)$ ограничено, алгоритм имеет полиномиальную сложность $\mathrm{O}(n^d + n^4 \log_2 n)$, где $n = 2^m$. Практические результаты показывают, что предложенная атака позволяет осуществить взлом криптосистемы Мак-Элиса, построенной на основе двоичного кода Рида — Маллера длины $n = 65526$ битов, менее чем за 7 ч на персональном компьютере.

Ключевые слова: *криптосистема Мак-Элиса, коды Рида — Маллера, полиномиальная сложность атаки.*

Рассматривается криптосистема Мак-Элиса, оригинальная версия которой использует коды Гоппы [1]. В 1994 г. В. М. Сидельников в работе [2] предложил использовать для построения криптосистемы Мак-Элиса коды Рида — Маллера, которые позволяют увеличить скорость расшифрования и передачи криптограммы.

На сегодняшний день самым успешным из опубликованных алгоритмов восстановления секретного ключа по открытому для криптосистемы Мак-Элиса, основанной на двоичных кодах Рида — Маллера $RM(r, m)$, является алгоритм Л. Миндера и А. Шокроллахи, предложенный ими в 2007 г. в [3]. Этот алгоритм имеет субэкспоненциальную сложность, его идея заключается в сведении задачи взлома криптосистемы с параметрами кода $RM(r, m)$ к такой же задаче, но для кода $RM(1, m)$. В данной работе предложен другой алгоритм сведения, который имеет полиномиальную сложность для некоторого подмножества кодов Рида — Маллера.

Полученные теоретические результаты можно кратко представить в виде теорем.

Теорема 1. Пусть $(r, m-1) = 1$. Тогда существует алгоритм со сложностью $\mathrm{O}(n^4 \log_2 n)$ битовых операций, который по порождающей матрице кода $RM^\sigma(r, m)$ находит перестановку σ', такую, что $RM^{\sigma\cdot\sigma'}(r, m) = RM(r, m)$.

И обобщение теоремы 1: