УДК 681.3.06

ИССЛЕДОВАНИЕ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ МИНИ-ШИФРОВ BABY-ADE И BABY-AES

В.И. ДОЛГОВ, А.А. КУЗНЕЦОВ, Р.В. СЕРГИЕНКО, О.И. ОЛЕШКО

Приводятся результаты исследований полных дифференциалов уменьшенных моделей шифров Baby-ADE и Baby-AES

The results of researching the total differentials of reduced models of Baby-ADE and Baby-AES ciphers are given.

ВВЕДЕНИЕ

В настоящее время в Украине проходит открытый конкурс по выдвижению и отбору кандидатов на национальный стандарт блочного симметричного шифрования. Основным требованием, предъявленным к алгоритмам-кандидатам, естественно, выдвинута высокая стойкость к известным методам криптоанализа, при этом рекомендовано учитывать опыт прошедших конкурсов по отбору криптоалгоритмов AES и NESSIE. Конечно, результаты прошедших зарубежных конкурсов оказывают большое влияние на принимаемые решения. В частности, безусловно, впечатляет, что несомненным фаворитом американского, да и европейского конкурсов стал алгоритм Rijndael, который сегодня известен как национальный стандарт шифрования США AES – Advanced Encryption Standard [1, 2]. Своей победой алгоритм во многом обязан убедительному обоснованию авторами стойкости шифра к известным атакам, а также простоте описания и структуры, где четко разделены функции между слоем нелинейных замен SubByte и слоем линейного рассеивания, реализованным композицией процедур ShiftRow и MixColumn. Конкурировать с решением, прошедшим тщательную экспертизу многих авторитетных криптографов, трудно. В этих условиях представляется оправданным (целесообразным) строить предложения вокруг или рядом с общепринятым и считающимся проверенным решением.

Одной из таких реализаций этого подхода является алгоритм криптографических преобразований информации с динамически управляемыми криптопримитивами, названный ADE (Algorithm of Dynamic Encryption), который был предложен в качестве кандидата на национальный стандарт шифрования Украины [12]. Основной задачей разработчиков шифра стало усовершенствование AES с целью повышения его потенциальной устойчивости к атакам, которые могут использовать простоту его алгебраического описания [2, 4, 13].

По мнению многих отечественных и зарубежных криптографов, дополнительное повышение показателей стойкости шифра может быть достигнуто на основе введения в шифрующие преобразования механизмов динамического управления промежуточными состояниями [6, 7, 17]. Это, однако, в общем случае может привести к усложнению алгоритма и снижению скорости преобразований. Удачным компромиссом, по мнению авторов разработки, является динамическое изменение блоков замены и параметров матриц линейного рассеивания с помощью битов цикловых подключей. Это, с одной стороны, приводит только к некоторому замедлению процедуры формирования подключей, не уменьшая ощутимо скорости шифрования, а с другой – позволяет получить дополнительное повышение сложности (размерности) системы алгебраических уравнений, описывающих процедуру зашифрования, не затрагивая принципиальной основы использованных в AES решений. Авторами было сделано предположение, что сохранение структуры исходного (базового) шифра обеспечивает наследование его показателей стойкости к статистическим атакам в «модернизированном решении».

Наилучшим способом проверки этой гипотезы является сравнение показателей стойкости AES и его усовершенствованной конструкции. Конечно, для блоковой длины шифра 128 бит и его полной цикловой длины такую задачу выполнить практически невозможно. Поэтому здесь был использован развиваемый и в других наших работах подход [10, 14], заключающийся в выполнении сравнения показателей стойкости шифров, на уровне их пропорционально уменьшенных моделей.

Построенная нами модель уменьшенного шифра AES во многом повторяет принципы, по которым создана одна из наиболее удачных его мини-версий шифра – mini-AES, описание которой было опубликовано в открытой печати [3, 8]. Все дополнительно введенные в шифр ADE преобразования и операции мы постарались сохранить и в уменьшенной его модели – baby-ADE. Как и в mini-AES, в нашем шифре Baby-ADE исходное входное сообщение, названное открытым текстом, разбивается на блоки по 16 бит каждый. За одно применение алгоритма осуществляется шифрование только одного блока открытого текста. Процесс повторяется до тех пор, пока не будут зашифрованы все блоки. Для зашифрования используется ключ длиной 16 бит. В процессе зашифрования шифртекст составляется из зашифрованных блоков, последовательность которых соответствует очередности блоков открытого текста.

Особенности реализации отдельных компонентов шифра Baby-ADE и процедуры расширения ключа подробно изложены в нашей предыдущей работе [10].

1. ПОНЯТИЯ И ОПРЕДЕЛЕНИЯ ДИФФЕРЕНЦИАЛЬНОГО КРИПТОАНАЛИЗА. ПРИНЦИПЫ ПОСТРОЕНИЯ АТАКИ

Как известно, сущность дифференциального криптоанализа заключается в использовании специфических входов в так называемые таблицы распределения разностей S-блоков, используемых блочным шифром [5]. Переходы с более высокими значениями особенно полезны для атаки. Таблица распределения разностей S-блока – это $n \times s$ матрица размера $2^n \times 2^s$. Строки матрицы индексированы векторами из множества V_n, представляющими входные разности, в то время как колонки индексированы векторами из множества V_s, представляющими собой выходные разности. Ячейка в таблице, индексированная парой входов (α, β), указывает на число пар входов (входных векторов), имеющих входную разность α, переходящих при подстановке в выходную разность β. Таблица как раз и позволяет найти наиболее вероятные значения переходов входной разности в выходную, которые используются для построения подходящих одноцикловых дифференциальных характеристик.

Напомним также, что содержание ячеек таблицы распределения дифференциальных разностей может быть только четным числом, сумма значений в каждой строке всегда равна 2^n, а первая строка в таблице имеет вид $(2^n, 0, \ldots, 0)$.

При проведении разности через несколько циклов шифрования используется понятие многоцикловой дифференциальной характеристики. Многоцикловая характеристика создается путем объединения одноцикловых характеристик, удовлетворяющих условию «сшивки» $\beta_{i-1} = \alpha_i$ (значение входной разности текущего цикла α_i совпадает со значением выходной разности предыдущего цикла β_{i-1}).

Вероятность r-цикловой дифференциальной характеристики определяется (в предположении статистической независимости ключевых битов) как произведение вероятностей составляющих ее одноцикловых характеристик по формуле

$$p^{(r)} = \prod_{i=1}^{r} p^{(1)}(\alpha_i \to \beta_i).$$

Пары $(\Delta x_j, \Delta y_{j+i}) = (\alpha, \beta)$, которые определяются разностью на входе j-го цикла, и разностью после цикла $j + i$, называют i-цикловым дифференциалом, а последовательность значений $(\alpha, \beta_1, \beta_2, \ldots, \beta_{i-1}, \beta)$, где каждое $\beta_k, k = 1, \ldots, i-1$ – значение разности после k-го цикла, называется i-цикловой дифференциальной характеристикой, которая принадлежит i-цикловому дифференциалу (α, β) (здесь уже α и β обозначают разности на входе и выходе i-цикловой характеристики). Вероятность i-циклового дифференциала $P^{(i)}(\Delta y_i = \beta \mid \Delta x_1 = \alpha)$ определяется как сумма вероятностей принадлежащих ему характеристик:

$$P^{(i)}(\Delta y_i = \beta \mid \Delta x_1 = \alpha) = \sum_{\forall \beta_1, \ldots \beta_{i-1} \neq 0} p^{(i)}(\Delta y_1 = \beta_1, \ldots, \Delta y_i = \beta \mid \Delta x_1 = \alpha)$$

(под чертой стоит обусловленное значение события).

Всегда справедливо неравенство:

$$P^{(r)} \geq p^{(r)}.$$

Сама атака дифференциального криптоанализа осуществляется путем поиска дифференциальных характеристик, которые позволяют фиксированную входную разность (разность открытых текстов) довести с вероятностью, большей, чем дает атака прямого перебора ключей, к фиксированной разности на входе предпоследнего цикла. И если такую характеристику удается найти, то на основе изучения статистики прохождения пар отобранных открытых текстов (с фиксированными битовыми разностями) через последний цикл шифрования можно построить процедуру определения ключевых бит шифра. Тут речь идет о ключевых битах, которые принимают участие в формировании фиксированных разностей последнего (или первого для шифра в режиме расшифровывания) цикла. В общем случае, если найден подключ последнего цикла, то последующее повторение этой процедуры для шифра с уменьшенным числом циклов позволяет определить и подключи остальных циклов.

Так как дифференциальный криптоанализ восстанавливает биты ключа на последнем цикле, то для успешной атаки на шифр необходим многоцикловый дифференциал (дифференциальная характеристика), который покрывает почти все циклы шифра и имеет вероятность, которая значительно превышает значение 2^{-n} (здесь n – размер ключа в битах). Соответственно, критерием защищенности r-циклового шифра от атак дифференциального криптоанализа считается выполнение неравенства

$$P^{(r-1-q)} \leq 2^{1-n},$$

где $q = 1$ или $q = 2$ определяется возможностью реализации NR-атаки с разным количеством циклов (атаки с N = q подобранными заключительными циклами). Значение $P^{(r-1-q)}$ характеризует сложность выполнения наиболее ресурсоемкого этапа дифференциального криптоанализа – подбора правильной пары открытых текстов. Правильная пара позволяет предположить значения битов подключа последнего цикла. Естественно, остается воспользоваться дополнительными приемами, чтобы восстановить все биты подключа (и ключа в целом).

При определении стойкости S-блоков к атакам дифференциального криптоанализа исполь-

зуется понятие дифференциальной δ-равномерности, введенное для оценки свойств S-блоков [15]. Напомним здесь его.

Определение. Пусть F будет $n\times s$ S-блоком, где $n\ge s$. Пусть δ будет наибольшим значением в дифференциальной таблице S-блока (исключая первый вход в первую строку), а именно

$$\delta=\max_{\alpha\in V_n,\alpha\neq 0}\max_{\beta\in V_s}\left|\{x\,|\,F(x)\oplus F(x\oplus\alpha)=\beta\}\right|.$$

Тогда говорят, что S-блок F является дифференциально δ-равномерным и соответственно δ называют равномерностью булевой функции $f: Z_2^n\to Z_2^s$.

Очевидно, что дифференциальная равномерность S-блока заключена в границах $2^{n-s}\le\delta\le 2^n$. S-блок считается хорошим по этому показателю, если значение δ достаточно мало.

По аналогии с этим определением мы введем в рассмотрение *условную* Δ_k*-равномерность всего набора шифрующих преобразований* (*условную* Δ_k*-равномерность шифра*).

Для блочного симметричного шифра $n=\{K,M,C,T\}$, где K, M и C – конечные множества, обозначающие ключевое пространство, пространство сообщений и пространство шифртекстов, а $T: K\times M\to C$ – шифрующее преобразование такое, что для $x\in M$ имеем $y=T_k(x)$. Значение

$$\Delta_k=\max_{\alpha\in V_n,\alpha\neq 0}\max_{\beta\in V_s}\left|\{x\,|\,T_k(x)\oplus T_k(x\oplus\alpha)=\beta\}\right|$$

и будем называть условной Δ_k-равномерностью шифра. Индекс k здесь подчеркивает, что преобразования $y=T_k(x)$ для всех $x\in M$ являются ключе зависимыми (Δ_k вычисляется при фиксированном значении ключа зашифрования). Нас далее будет интересовать поведение значения Δ_k при изменении числа циклов шифрования и изменении ключей зашифрования.

2. МЕТОДИКА ИССЛЕДОВАНИЯ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ ШИФРОВ BABY-ADE И MINI-AES

В наших исследованиях в качестве S-блока (подстановки) рассматривается целиком весь набор шифрующих (дешифрующих) преобразований для одного ключа, так что общее число различных подстановок равно мощности ключевого пространства K. Это значит, что для уменьшенных версий шифров таблица дифференциалов имеет размер $2^{16}\times 2^{16}$ (в мини-версиях используются 16-битные «блоки данных», т.е. возможно 2^{16} вариантов входных и столько же выходных разностей). Как и в случае S-блоков в атаке Ф. Шамира и Э. Бихама, при построении таблицы просматриваются все возможные разности (суммы по модулю 2) различных пар открытых текстов (входов в таблицу по строкам) и соответствующие разности пар зашифрованных текстов (входов в таблицу по столбцам). Полученные числа являются индексами входов (по строкам и по столбцам) в ячейки таблиц распределения разностей (дифференциалов) шифра. Сама таблица разностей получается заполнением ячеек числами, соответствующими количествам пар входных разностей (входов в таблицу по строкам), образующих заданные значения выходных разностей (входов в таблицу по столбцам) при вариации по всему множеству пар входов шифра, формирующих заданную входную разность, т.е. каждая строка таблицы соответствует конкретному значению входной разности, а каждый столбец соответствует конкретному значению выходной разности, а значения соответствующих ячеек таблицы соответствуют количеству возможных пар с рассматриваемыми значениями входных разностей, образующих заданные значения выходных разностей.

Естественно, что значения в ячейках таблицы не превышают числа 2^{16}. Суммы всех значений для каждой строки также равны 2^{16}. Кроме того, значение 2^{16} встречается в таблице всего 1 раз для значений входной и выходной разностей, равных 0, т.е. при прохождении через шифр пар одинаковых открытых текстов, которые преобразуются в пары одинаковых шифртекстов. Этот случай из рассмотрения исключается, как неинформативный.

При использовании ЭВМ таблица представляется в виде двумерного массива элементов размером 2 байта каждый. В результате, общий объем памяти, требуемый для запоминания всех данных таблицы для одного значения ключа зашифрования равен $2^{16}\times 2^{16}=2^{32}$ байт = 4 Гбайт.

Для более полного представления дифференциальных свойств шифра можно выполнить усреднение Δ_k-равномерности еще и по всему множеству ключей (при этом придем к аналогу так называемого линейного корпуса (*linear hull*) при линейном криптоанализе [18]). Следует, однако, заметить, что и для уменьшенных версий шифров полный объем вычислений достигнет уже значения 2^{48}, что опять много.

С другой стороны, здесь не идет речь о построении атак на шифры. Полезность нашего подхода видится в сравнении показателей стойкости малых версий шифров. Для этого можно перейти к оценкам интересующих нас показателей в среднестатистическом смысле, т.е. ориентироваться на обработку результатов статистических экспериментов для ограниченного набора ключей (выборки из генеральной совокупности), по которым оценивать затем уже свойства генеральной совокупности, привлекая известные методы обработки статистики.

3. РЕЗУЛЬТАТЫ СТАТИСТИЧЕСКИХ ИССЛЕДОВАНИЙ ДИФФЕРЕНЦИАЛЬНЫХ СВОЙСТВ МИНИ ВЕРСИЙ ШИФРОВ ADE И AES

При проведении статистического эксперимента построено 1000 вариантов таблиц, каждая для случайно выбранного значения 16-битного

ключа зашифрования. Определялись следующие показатели:

– среднее по множеству из 1000 случайно выбранных ключей зашифрования (по множеству таблиц) значение $\Delta^{(r)}$-равномерности r –циклового шифра

$$\Delta^{(r)} = \frac{1}{1000}\sum_{i=1}^{1000}\Delta_{k_i}^{(r)},$$

где $\Delta_{k_i}^{(r)}$ – значение показателя равномерности (максимальное значение заполнения каждой из таблиц) для r-циклового шифра с ключом зашифрования k_i, $r = 2, 4, 6, 8$;

– $\Delta^{(r)}$-равномерность r-циклового шифра при построчном рассмотрении таблиц распределения дифференциалов (выполнялось усреднение значений максимального числа переходов фиксированной входной разности (XOR) открытых текстов в выходную разность соответствующих шифртекстов для строк таблиц дифференциалов);

– среднеквадратическое отклонение условной $\Delta_k^{(r)}$-равномерности для выборки из 1000 ключей;

– абсолютные значения условной $\Delta_k^{(r)}$-равномерности r-циклового шифра по выборке из 1000 ключей зашифрования;

– математическое ожидание минимальных значений максимумов числа переходов r-циклового шифра.

Поскольку в эксперименте участвовало только 1000 реализаций ключей зашифрования, то использовался метод доверительных интервалов, являющийся методом математической статистики, специально предназначенным для построения множества приближенных значений неизвестных параметров вероятностных распределений [9].

Напомним кратко его сущность. Пусть $X_1, X_2, \ldots, X_n$, $n \geq 2$, независимые случайные величины, подчиняющиеся одному и тому же нормальному закону с неизвестными параметрами $EX_i = \theta_1$ и $DX_i = \theta_2$, причём требуется построить интервальную оценку $u(\theta) = \theta_1$. Пусть

$$\bar{X} = \frac{1}{n}\cdot\sum_{i=1}^{n} X_i$$

и

$$s^2 = \frac{1}{n-1}\cdot\sum_{i=1}^{n}(X - \bar{X})^2.$$

Количество реализаций $N = 1000$ (из 65535) было выбрано исходя из положений центральной предельной теоремы теории вероятностей, в соответствии с которыми при больших значениях N исходов случайного эксперимента среднее арифметическое будет иметь распределение, близкое к нормальному закону [9].

В соответствии с положениями теории математической статистики случайная величина $T = \sqrt{n}(\bar{X} - \theta)/s$ подчиняется распределению Стьюдента с $n-1$ степенями свободы, которое не зависит от неизвестных параметров θ_1 и θ_2 ($|\theta_1| \leq \infty$, $\theta_2 > 0$), и при любом положительном t вероятность события

$$\left\{\bar{X} - \frac{t\cdot s}{\sqrt{n}} < \theta_1 < \bar{X} + \frac{t\cdot s}{\sqrt{n}}\right\}$$

зависит лишь от t. Если указанный интервал принять за интервальную оценку для θ_1, то ему будет соответствовать доверительная вероятность

$$P_c(\theta_1, \theta_2) = P\{|T| < t\} = 1 - \alpha,$$

не зависящая от параметров $\theta = \{\theta_1, \theta_2\}$. доверительным интервалом, а концевые точки интервала – доверительными пределами.

В результате, задаваясь доверительной вероятностью $P_c(\theta_1, \theta_2) = 0{,}99 \rightarrow (\alpha = 0{,}01)$, на основании таблицы распределения Стьюдента [9, 11] для заданных значений α и n = 1000 (в наших экспериментах) получаем t = 2,576, и, следовательно, $\frac{t\cdot s}{\sqrt{n}} = \frac{2{,}576\cdot s}{\sqrt{1000}} = 0{,}081\cdot s$. Это соотношение и было использовано для определения доверительных пределов.

Результаты статистических исследований дифференциальных свойств мини-шифров baby-ADE и mini-AES приведены в таблицах 1–5. Характеристики, представленные в них, были получены, как отмечено выше, при обработке 1000 реализаций таблиц. Доверительный интервал задавался уровнем значимости α = 0,01, что соответствует доверительной вероятности $P = (1-\alpha)\cdot 100\% = 99\%$.

В качестве примера приведем расчет доверительного интервала при оценке Δ_k^r-равномерности 4-х циклового шифра baby-ADE (для математического ожидания максимального значения числа максимумов переходов). При $r = 4$ для шифра baby-ADE из табл. 1 находим $\Delta^{(r)} = 20{,}064$. Как следует из табл. 4, среднеквадратическое отклонение для этого значения числа циклов составило $s = 1{,}213$, и, следовательно,

$$\frac{t\cdot s}{\sqrt{n}} = \frac{2{,}576\cdot s}{\sqrt{1000}} = 0{,}081\cdot 1{,}213 = 0{,}098.$$

Это значит, что можно считать попавшими в доверительный интервал все значения Δ_k^r, удовлетворяющие условиям

$$20 - 0{,}01 \leq \Delta^r \leq 20 + 0{,}01 \rightarrow$$

$$\rightarrow 19{,}99 \leq \Delta^r \leq 20{,}01.$$

Как видно из представленных результатов, для среднего по множеству таблиц максимального значения дифференциалов обоих шифров характерен переходный процесс установления стационарного значения при изменении числа циклов.

Таблица 1

$\Delta^{(r)}$ -равномерность *r*-циклового шифра

Шифр	Количество циклов						
	2	3	4	5	6	7	8
babyADE	3254±59	301,3±7,3	20,064±0,348	19,170±0,124	19,120±0,092	19,166±0,093	19,106±0,091
miniAES	4955±24	640,6±4,6	43,066±0,999	20,538±0,202	19,082±0,093	19,122±0,092	19,122±0,096

Таблица 2

$\Delta^{(r)}$ -равномерность *r* -циклового шифра при построчном рассмотрении таблиц распределения дифференциалов

Шифр	Количество циклов						
	2	3	4	5	6	7	8
babyADE	61,2±0,5	13,475±0,047	11,3559±0,0006	11,3459±0,0004	11,3456±0,0004	11,3458±0,0004	11,3458±0,0004
miniAES	77,3±0,2	16,103±0,01	11,4065±0,0012	11,3488±0,0004	11,3456±0,0004	11,3458±0,0004	11,3456±0,0004

Таблица 3

Среднеквадратическое отклонение условной Δ_k^r -равномерности для выборки из 1000 ключей

Шифр	Количество циклов						
	2	3	4	5	6	7	8
babyADE	154,9	11,815	1,213	1,209	1,208	1,208	1,208
miniAES	182,2	20,609	1,355	1,211	1,208	1,208	1,208

Таблица 4

Абсолютные значения условной $\Delta_k^{(r)}$ -равномерности *r*-циклового шифра по выборке из 1000 ключей зашифрования

Шифр	Количество циклов						
	2	3	4	5	6	7	8
babyADE	5632	1088	72	40	24	22	26
miniAES	5632	768	108	36	24	24	28

Таблица 5

Математическое ожидание минимальных значений максимального числа переходов *r*-циклового шифра

Шифр	Количество циклов						
	2	3	4	5	6	7	8
babyADE	16,5±0,2	10,00±0,005	8,93±0,08	8,89±0,08	8,85±0,08	8,91±0,08	8,90±0,08
miniAES	18,6±0,4	10,00	9,01±0,08	8,85±0,08	8,93±0,08	8,92±0,08	8,86±0,08

Интересно отметить, что подобный эффект «насыщения» полного дифференциала после четырех циклов теоретически обоснован К. Нюберг для DES-подобных шифров в ее работе [16].

Другой интересный момент, который можно вынести из полученных результатов, состоит в том, что зафиксированное изменение Δ^r -равномерности с изменением числа циклов шифров можно интерпретировать как более полную характеристику динамики достижения полноты лавинного эффекта. С точки зрения дифференциальных свойств шифра полный лавинный эффект (вхождение в «трубку», задаваемую доверительными границами) наступает для обоих шифров на пятом – шестом циклах (для baby-ADE на цикл раньше). Механизм перехода в стационарное состояние можно объяснить тем, что формирование результирующего дифференциала при проходе каждого цикла осуществляется на основе вероятностного суммирования независимых (для независимых и равновероятных битов подключа) переходов. Этот эффект статистического усреднения подтверждается данными табл. 2, в которой приводятся средние (по множеству из 1000 ключей) значения Δ^r -равномерности *r*-циклового шифра при построчном рассмотрении таблиц распределения дифференциалов. Усреднение максимальных значений числа переходов, полученных для строк каждой из таблиц дает результат близкий к определяемому в табл. 1 показателю Δ^r -равномерности. Расхождение результатов можно пояснить наличием общих входных или выходных разностей у части переходов (их статистической зависимостью).

ВЫВОДЫ

Представленные результаты свидетельствуют, что дифференциальные свойства шифра baby-ADE не хуже дифференциальных свойств шифра mini-AES. Если быть более точным, то можно отметить, что введенные в шифр baby-ADE механизмы динамического (ключевого) управления привели к небольшому улучшению его дифференциальных свойств. Представляется, что эти выводы можно перенести и на полные версии шифров.

В целом можно сделать вывод о том, что для обоих шифров AES и ADE сложность атаки дифференциального криптоанализа (если бы можно было реализовать атаку на полные дифференциалы) несколько меньше сложности атаки полного перебора ключей (для малых версий шифра, судя по данным таблицы 4, не более чем в несколько десятков раз). Если это соотношение сохраняется и для больших шифров, то шифры AES и ADE действительно являются устойчивыми к атакам дифференциального криптоанализа.

Литература

[1] Final report of European project number IST-1999-12324, named New European Schemes for Signatures, Integrity, and Encryption, April 19, 2004— Version 0.15 (beta), Springer-Verlag.

[2] *S. Landau,* Polynomials in the Nation's Service: Using Algebra to Design the Advanced Encryption Standard, THE MATHEMATICAL ASSOCIATION OF AMERICA, 111 (February, 2004), pp. 89–117.

[3] A Description of Baby Rijndael, ISU CprE/Math 533; NTU ST765-U, February 19, 2003.

[4] *S. Murphy and M. J. Robshaw.* Essential Algebraic Structure within the AES. In Advances in Cryptology. CRYPTO 2002, volume 2442 of Lecture Notes in Computer Science, Springer Verlag Heidelberg, 2002, pp. 1 – 16.

[5] *E. Biham and A. Shamir.* Differential cryptanalysis of DES-like cryptosystems, Journal of Cryptology, Vol. 4, No. 1, 1991, pp. 3-72.

[6] *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002 – 816 с.

[7] *Молдавян А.А., Молдавян Н.А., Гуц Н.Д., Изотов Б.В.* Криптография. Скоростные шифры // Санкт – Петербург, "БХВ-Петербург", 2002, 493 с.

[8] *R. C-W. Phan,* Mini Advanced Encryption Standard (Mini-AES): A Tested for Cryptanalysis Students, Cryptologya, XXVI (4), 2002.

[9] *Вентцель Е. С.* Теория вероятностей. – М.: Наука, – 1964. С. 576.

[10] *Долгов В.И., Кузнецов А.А., Сергиенко Р.В., Белоковаленко А.Л.* Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE) // Прикладная радиоэлектроника. – 2008. – Т.7 – № 3. С. 215-224.

[11] *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся Втузов. – М.: Наука, 1980. – 976 с.

[12] *Кузнецов А.А., Сергиенко Р.В., Наумко А.А.* Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption) Радиотехника: Всеукр. межвед. науч.-техн. сб. – Харьков: ХНУРЭ. – 2008, (в печати).

[13] *Nicolas Courtois.* How Fast can be Algebraic Attacks on Block Ciphers? Cryptology ePrint Archive, Report 2006/168, 2006. Available at: http://eprint.iacr.org /2006/ 168. pdf.

[14] *Долгов В.И., Лисицкая И.В., Руженцев В.И.* Анализ циклических свойств блочных шифров // Прикладная радиоэлектроника – 2007. – Т.6, №2 – С. 257-263.

[15] *J. Seberry, X.M. Zhang, Y. Zheng.*: Relationships among nonlinearity criteria. Presented at EUROCRYPT-94, 1994.

[16] *K. Nyberg, L. Knudsen,* "Provable Security Against Differential Cryptanalysis" // Proceeding of Crypto-92, Copyright – Springer-Verlag, 1998, pp. 566-574.

[17] *B. Schneier, J. Kelsey, D. Whiting, D. Wagner, Hall C., Ferguson N. Twofish:* A 128-bit Block Cipher. // http:// www.schneier.com — 15 June 1998.

[18] *K. Nyberg,* "Linear Approximations of Block Ciphers", Advances in Cryptology - EUROCRYPT '94 (Lecture Notes in Computer Science no. 950), Springer-Verlag, , 1995, pp. 439-444.

Поступила в редколлегию 7.09.2009

Долгов Виктор Иванович, доктор технических наук, профессор кафедры «Безопасности информационных технологий» ХНУРЭ. Область научных интересов: математические методы защиты информации.

Кузнецов Александр Александрович, доктор технических наук, профессор. Область научных интересов: алгебраическая теория блоковых кодов, криптография и теория аутентификации, методы обеспечения помехоустойчивости, имитостойкости и скрытности каналов управления и связи.

Сергиенко Роман Викторович, кандидат технических наук по специальности системы защиты информации. Область научных интересов: алгебраическая теория блоковых кодов, криптографические средства защиты информации.

Олешко Олег Иванович, старший преподаватель кафедры БИТ ХНУРЭ. Область научных интересов: криптография и криптоанализ БСШ, сетевая безопасность.