УДК 681.3.06

С. А. ГОЛОВАШИЧ, канд. техн. наук, А. Н. ЛЕПЕХА

СТАТИСТИЧЕСКИЙ АНАЛИЗ БСШ «ТОРНАДО»

Рассматривается блочный симметричный шифр (БСШ) «Торнадо». Алгоритм «Торнадо» поддерживает три различных длины блока (128, 256 и 512 бит) и оперирует с ключами длиной не менее 256 бит. В соответствии с условиями проекта NESSIE алгоритм относится к первому классу стойкости. Основным требованием, предъявляемым к БСШ, является устойчивость к известным криптоаналитическим атакам.

Косвенным показателем стойкости криптоалгоритма является его статистическая безопасность. Статистическое исследование шифров позволяет выявить «скрытые» (либо неизвестные) «аномалии» в работе шифратора, которые не удаётся обнаружить аналитическим путём.

Целью данной статьи является проведение исследования статистической безопасности БСШ «Торнадо» и сравнение его статистических показателей с аналогичными показателями криптоалгоритмов, победивших в конкурсах AES и NESSIE. Исследования проводились для версии алгоритма с длиной блока 128 бит.

Методы статистического анализа можно разделить на два класса: методы, основанные на анализе статистических свойств выхода шифратора (криптограмм), и методы, основанные на исследовании корреляционных зависимостей «вход-выход» шифратора.

Для исследования корреляционных свойств алгоритма (в соответствии со вторым подходом) использовалось три теста, позволяющие выявить «простые» статистические зависимости между входом и выходом криптопреобразования: лавинный эффект (AE), строгий лавинный критерий (SAC), тест частичных (однобитных) дифференциалов (TD).

С помощью перечисленных тестов исследована также процедура разворачивания ключа. В рамках этого исследования тесты лавинного эффекта (AE) и строгого лавинного критерия (SAC) использовались для анализа корреляционных зависимостей между битами исходного (пользовательского) ключа и битами развернутого (рабочего) ключа.

1 Конструкции генераторов ПСП на базе БСШ «Торнадо»

Для исследования статистических свойств алгоритма «Торнадо», в соответствии с первым подходом, использовалась методика NIST STS, разработанная Национальным институтом стандартов США (NIST) и использовавшаяся в рамках проекта AES. Этот метод рассматривает любой алгоритм как «чёрный ящик», обладающий n-битными входом и выходом, а также k-битным управляющим входом (вход ключа). Алгоритм считается «статистически безопасным», если ПСП, формируемые генератором на его основе (на случайно выбранном ключе), «выглядят» как случайная битовая последовательность. Исследование проводилось для последовательностей, сформированных в двух режимах применения БСШ: режим «с обратной связью по выходу» (ISO/IEC 10116) и режим «счетчика с плавающим периодом» [3], соответствующих схемам синхронного поточного шифрования (формирования гаммы шифрующей). Для обоих схем исследовались свойства только гаммы шифрующей, то есть текст соответствовал нулевому заполнению. Тестирование проведено для полноциклового и ряда упрощенных версий шифра (с уменьшенным числом циклов и с/без начального и конечного преобразований). Результаты сравнивались со свойствами ПСП, сформированной генератором BBS (эталонная выборка, рекомендованная NIST).

2 Тестирование по методике NIST STS

Пакет NIST STS включает в себя 16 различных статистических тестов, направленных на выявление различных «дефектов» случайности. При этом некоторые из тестов рассчитываются для нескольких различных «тестовых шаблонов» [2], проверка каждого из которых фактически является отдельным тестом. В связи с этим общее количество тестов составляет 189.

Рассмотрим методику тестирования генераторов в соответствии с NIST STS.

Методика тестирования [4].

1. С помощью тестируемого генератора формируется m двоичных последовательностей длиной по n бит: $S_i \in \{0, 1\}^n$, $i = \overline{1, m}$, т.е. $N = m \times n$ бит.

2. Для каждого теста j по результатам тестирования последовательностей $\{S_i\}$ строится вектор вероятностей $P_{i,j} \in [0, 1]$, $i = \overline{1, m}$.

4. Задаётся необходимый уровень значимости α и для каждого теста j, по соответствующему вектору $(P_{1,j}, \ldots, P_{m,j})$ определяют долю последовательностей, прошедших данный тест: $r_j = \#\{P_{i,j} \geq \alpha \mid i = \overline{1, m}\} / m$.

Считается, что генератор прошёл тестирование по j-му тесту, если значение коэффициента r_j находится в пределах доверительного интервала $[r_{min}, r_{max}]$, заданного как $\hat{p} \pm 3\sqrt{\hat{p}(1-\hat{p})/m}$, $\hat{p} = 1 - \alpha$.

5. Для каждого теста j осуществляется проверка вектора вероятностей $(P_{1,j}, \ldots, P_{m,j})$ на подчинение равномерному закону распределения в интервале [0, 1]. Для проверки этой гипотезы используется критерий χ^2 с 9 степенями свободы (интервал [0, 1] разбивается на 10 подинтервалов). По значению χ_j^2 определяется соответствующая вероятность $P_j = P(\chi_j^2, 9)$.

Значения j-го вектора вероятностей могут считаться равномерно распределёнными, если выполняется условие $P_j \geq 0{,}0001$.

6. Принимается окончательное решение о случайности последовательностей, формируемых генератором.

Последовательности, формируемые генератором, считаются «случайными», если для всех 189 тестов соблюдается условие $P_j > 0{,}0001$, а значения коэффициентов r_j находятся внутри доверительного интервала $[r_{min}, r_{max}]$.

При проведении тестирования параметры были выбраны в соответствии с рекомендациями NIST STS, то есть длина одной последовательности $n = 10^6$, количество последовательностей $m = 100$, уровень значимости $\alpha = 0{,}01$.

3 Результаты тестирования по методике NIST STS

В табл. 1 приведены результаты тестирования БСШ «Торнадо» в режиме «обратной связи по выходу шифратора». В табл. 2 сведены результаты тестирования в режиме «счетчика с плавающим периодом».

Таблица 1

Количество циклов	1	1+ IT&FT	2	2+ IT&FT	3	4	4+ IT&FT	Генератор BBS
Количество тестов, в которых тестирование прошло 99% последовательностей	138	124	135	141	138	132	139	134

Продолжение табл. 1

Количество тестов, в которых тестирование прошло более 96% последовательностей	189	188	188	188	188	188	189	189
Количество тестов, в которых значение вероятности P<=0,01	2	3	1	0	0	1	0	0
Количество тестов, в которых значение вероятности P<=0,001	0	1	0	0	0	0	0	0
Количество тестов, в которых значение вероятности P<=0,05	16	11	13	9	2	6	10	—
Непройденный тест	—	Random-Excursion-V	Random-Excursion-V	Aperiodic-Template	Aperiodic-Template	Random-Excursion	—	—

Таблица 2

Количество циклов	1	1+ IT&FT	2	2+ IT&FT	3	4	4+ IT&FT	Генератор BBS
Количество тестов, в которых тестирование прошло 99% последовательностей	123	130	141	133	139	137	133	134
Количество тестов, в которых тестирование прошло более 96% последовательностей	188	188	189	187	189	189	189	189
Количество тестов, в которых значение вероятности P<=0,01	2	1	0	2	1	4	1	0
Количество тестов, в которых значение вероятности P<=0,001	0	0	0	0	0	0	1	0
Количество тестов, в которых значение вероятности P<=0,05	6	6	7	11	13	12	11	—
Непройденный тест	Aperiodic-Template	Aperiodic-Template	Aperiodic-Template	Aperiodic-Template	—	—	—	—

По результатам проведенных испытаний можно сделать следующие частные выводы:

1) значение вероятности P_j по всем тестам для всех протестированных выборок удовлетворяет ограничению $P_j > 0{,}0001$;

2) ряд выборок не прошли ограничение $r_j \geq 0{,}96015$ по некоторому тесту, при этом максимальное отклонение от доверительного диапазона зафиксировано для режима: «с обратной связью по выходу шифратора» – $r_j = 0{,}9508$, «счетчика с плавающим периодом» – $r_j = 0{,}95$;

3) выборки, не прошедшие тестирование, были «забракованы» не более, чем 1 тестом;

4) большинство выборок прошли все тесты, при этом 99% тестов показали «прохождение» не менее чем 97% одиночных последовательностей;

5) полноцикловая версия алгоритма в данном режиме показала результаты, сопоставимые с эталонной выборкой, сформированной ГПСП BBS. Количество тестов, в которых тестирование прошло 99% последовательностей, сопоставимо или выше, чем для BBS генератора.

4 Исследование корреляционных свойств БСШ «Торнадо»

Для исследования корреляционных свойств алгоритма (в соответствии со вторым подходом) использовалось три теста, позволяющие выявить «простые» статистические зависимости между битами входного и выходного блоков криптопреобразования: лавинный эффект (AE), строгий лавинный критерий (SAC), тест частичных (однобитных) дифференциалов (TD).

Параметры тестирования:

$n = 128$ – разрядность блока данных B_t;

$m = 1000$ – количество блоков B_t, тестируемых на каждом ключе K_r;

$k = 100\text{-}10000$ – количество ключей K_r, задействованных в тестировании.

Принятые обозначения:

$w(x)$ – статистика теста;

$W_H(B)$ – вес Хемминга вектора B;

$E_K(B)$ – зашифрование / расшифрование блока данных B на ключе K;

Δ_i – двоичный вектор, в котором установлен только i-й разряд:

$$\Delta_i = (\delta_{n-1}, \ldots, \delta_0)_i : \delta_j = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}, 0 \le i, j < n, \Delta_i \in \{0, 1\}^n;$$

$[B]_i$ – операция «выделения» из двоичного вектора B бита с номером i:

$$[B]_i = [(b_{n-1}, \ldots, b_0)]_i = b_i, b_i \in \{0, 1\}, 0 \le i < n.$$

Предметом исследования первого теста (лавинный эффект – AE) является количество изменившихся выходных разрядов при изменении одного входного разряда y. Исследование выполняется для каждого входного разряда y:

$$w_y(x) = W_H\left(E_{K_r}(B_t) \oplus E_{K_r}(B_t \oplus \Delta_y)\right), B_t \in \{0,1\}^n,$$
$$0 \le y < n, x = r \times m + t, 0 \le r < k, 0 \le t < m.$$

Предметом исследования второго теста (строгий лавинный критерий – SAC) является вероятность изменения некоторого выходного разряда j при изменении одного входного разряда i. Исследование выполняется для каждой пары разрядов «вход–выход» $y = (i, j)$ (по всем «выходным шаблонам» v):

$$w_{y,v}(x) = \frac{1}{k \times m} \sum_{r=0}^{k-1} \sum_{t=0}^{m-1} \phi(v), \phi(v) = \begin{cases} 1, v = ov \\ 0, v \neq ov \end{cases},$$
$$ov = \left[E_{K_r}(B_t) \oplus E_{K_r}(B_t \oplus \Delta_i)\right]_j, B_t \in \{0, 1\}^n,$$
$$y = i \times n + j, 0 \le i, j < n, 0 \le v < 2, x = r \times m + t.$$

Предметом исследования третьего теста (тест частичных (однобитных) дифференциалов – TD) является вероятность определённого «изменения» ov некоторого выходного разряда j

при условии определённого «изменения» iv некоторого входного разряда i (для произвольной пары входных блоков). Исследование выполняется для каждой пары разрядов «вход–выход» $y = (i, j)$ (по всем «шаблонам вход–выход» v):

$$w_{y,v}(x) = \frac{1}{k \times m} \sum_{r=0}^{k-1} \sum_{t=0}^{m-1} \psi(v),\ \psi(v) = \begin{cases} 1, v = iv \times 2 + ov \\ 0, v \neq iv \times 2 + ov \end{cases},$$

$$iv = \left[B_t \oplus B'_t\right]_i,\ ov = \left[E_{K_r}(B_t) \oplus E_{K_r}(B'_t)\right]_j,\ B_t, B'_t \in \{0,1\}^n,$$

$$y = i \times n + j,\ 0 \le i, j < n,\ 0 \le v < 4,\ x = r \times m + t.$$

Для всех перечисленных выше тестов по набранной статистике $w(x)$ были рассчитаны математическое ожидание (M) и дисперсия (D), а также для лавинного критерия минимальное (min) и максимальное (max) зафиксированные значения. Математическое ожидание отражает количество изменившихся бит в блоке (длина блока 128 бита), а дисперсия показывает разброс значений.

Тестирование выполнялось для 1–4-циклового вариантов БСШ «Торнадо». Соответствующие результаты тестирования приведены в табл. 3.

Таблица 3

Тест	1 цикл с IT и FT блоками		2 цикл с IT и FT блоками		3 цикл с IT и FT блоками		4 цикл с IT и FT блоками	
	M	D	M	D	M	D	M	D
AE:	63,796210	33,290935	64,000622	32,005364	63,999146	32,012535	64,000443	32,015113
SAC:	0,500000	0,000006	0,500000	0,000003	0,500000	0,000002	0,500000	0,000003
TD:	0,250000	0,000003	0,250000	0,000004	0,250000	0,000004	0,250000	0,000003

Минимальное зафиксированное значение – 0,492110, а максимальное для строгого лавинного критерия – 0,506650. Из полученных результатов видно, что уже после одного цикла с начальным и конечным преобразованиями (IT и FT) статистика шифра становится удовлетворительной. Для детализации в табл. 4 приводятся результаты тестирования ослабленной версии криптоалгоритма «Торнадо» (без IT и FT преобразований) для 1-4 итераций.

Таблица 4

Тест	1 итерация без IT и FT блоков		2 итерация без IT и FT блоков		3 итерация без IT и FT блоков		4 итерация без IT и FT блоков	
	M	D	M	D	M	D	M	D
AE:	49,023829	250,41669	63,998885	32,001051	63,997372	31,990770	64,000275	31,997621
SAC:	0,500000	0,059994	0,500000	0,000003	0,500000	0,000003	0,500000	0,000003

Как видно из результатов, представленных в табл.4, две итерации шифрования без IT и FT преобразований по приведенным тестам уже обеспечивают статистическую безопасность.

Эквивалентно рассмотренные выше показатели статистической безопасности могут быть выражены через «степени» (degree) «полноты» (d_c), «лавинного» эффекта (d_a), строгого лавинного критерия (d_{sa}) [1]. Алгоритм БСШ может считаться статистически безопасным по этим показателям, если они принимают следующие значения: $d_c = 1$; $d_a \approx 1$; $d_{sa} \approx 1$.

$$d_c = 1 - \frac{\#\{(i,j) \mid a_{ij} = 0\}}{nm},$$

где: i и j – размерности матрицы зависимости (n x m);

a_{ij} – элементы матрицы зависимости, причем, $a_{ij} = \#\left\{x \in \{0,1\}^n \mid \left(f(x^{(i)})\right)_j \neq \left(f(x)\right)_j\right\}$ для $i = \overline{1,n}$, $j = \overline{0,m}$.

$$d_a = 1 - \frac{\sum_{i=1}^{n}\left|\frac{1}{\#X}\sum_{i=1}^{m} 2jb_{ij} - m\right|}{nm},$$

где: $b_{ij} = \#\left\{x \in \{0,1\}^n \mid W_H\left(F(x^{(i)}) - f(x)\right) = j\right\}$ для $i = \overline{1,n}$, $j = \overline{0,m}$.

$$d_{sa} = 1 - \frac{\sum_{i=1}^{n}\sum_{i=1}^{m}\left|\frac{2a_{ij}}{\#X} - 1\right|}{nm}.$$

В табл. 5 приведены результаты, полученные для различных вариантов алгоритма «Торнадо».

Таблица 5

Тип теста	1 итерация без IT и FT	1 итерация + IT и FT	2 итерации без IT и FT	2 итерации + IT и FT	3 итерации + IT и FT	4 цикла + IT и FT
d_c	0,812012	1,000000	1,000000	1,000000	1,000000	1,000000
d_a	0,765328	0,893086	0,999783	0,996816	0,999789	0,999784
d_{sa}	0,755583	0,892801	0,997468	0,996107	0,997478	0,997470

Для сравнения в табл. 6 приведены результаты аналогичного исследования победителей проектов AES и NESSIE. Представлены циклы и соответствующие значения, после которых данные начинают удовлетворять указанным критериям.

Таблица 6

Наименование шифра	Циклы	Число бит, которые изменились	Полнота, d_c	Критерий распространения, d_a	Обнаруженные линейные факторы, d_{sa}
Camellia	4 + 0,5 5 + 0,5	63,555463 64,004316	1,000000 1,000000	0,999271 0,999254	0,991995 0,991951
SAFER++	2 + 0,5	63,996523	1,000000	0,999224	0,991944
RC6	3+0,5 4+0,5 5+0,5	60,301572 63,923282 63,994611	1,000000 1,000000 1,000000	0,942141 0,998479 0,999273	0,937845 0,991661 0,992041
Rijndael	2 3	64,247014 64,001791	1,000000 1,000000	0,996140 0,999350	0,991466 0,992043

Как видно из табл. 5, БСШ «Торнадо» удовлетворяет рассмотренным критериям уже после одного цикла шифрования. Сравнивая эти данные с результатами, представленными в табл. 6, можно отметить, что степень полноты, лавинный эффект и строгий лавинный критерий для БСШ «Торнадо» достигаются так же быстро, как и для БСШ «RIJNDAEL». Степень полноты и лавинного эффекта наступают для БСШ «Торнадо» быстрее, чем для БСШ Camellia и RC6.

6 Статистическое исследование процедуры разворачивания ключа БСШ «Торнадо»

Так же как и процедура шифрования, процедура разворачивания ключа должна удовлетворять требованиям статистической безопасности. Для проверки статистической безопасности процедуры разворачивания ключей мы применили описанную методику тестирования NIST STS, а также воспользовались тестами корреляционного анализа. Тесты корреляционного анализа были расширены, чтобы иметь возможность проанализировать влияние входных полублоков пользовательского ключа (64 бита) на выходные полублоки развернутого «сырого»ключа.

На рис. 1 приводится диаграмма прохождения тестов для ПСП, сгенерированной процедурой разворачивания ключей БСШ «Торнадо». В табл. 7 приведены сводные результаты тестирования.

Рис. 1

Таблица 7

Количество циклов	Процедура разворачивания ключей БСШ «Торнадо»	Генератор BBS
Количество тестов, в которых тестирование прошло 99% последовательностей	142	134
Количество тестов, в которых тестирование прошло более 96% последовательностей	189	189
Количество тестов, в которых значение вероятности P<=0,01	4	0
Количество тестов, в которых значение вероятности P<=0,001	3	0
Количество тестов, в которых значение вероятности P<=0,05	12	—
Непройденный тест	—	—

По результатам проведенных испытаний можно сделать следующие частные выводы:

1. Значение вероятности P_j по всем тестам для всех протестированных выборок удовлетворяет ограничению $P_j > 0{,}0001$;

2. Выборок, не прошедших ограничение $r_j \geq 0{,}96015$ по некоторому тесту, зафиксировано не было;

3. Выборок, не прошедших какой-либо тест в ходе тестирования, зафиксировано не было;

4. Полученные результаты сопоставимы с результатами для эталонной выборки, рекомендованной NIST STS. Кроме того, количество тестов, в которых тестирование прошло 99% последовательностей для предлагаемой процедуры разворачивания ключа, выше, чем для BBS генератора.

Для более адекватной оценки статистической безопасности процедуры разворачивания ключей были проведены исследования ее корреляционных свойств, аналогичные рассмотренным исследованиям процедуры шифрования. Процедура разворачивания ключа может рассматриваться как блочное преобразование: вход – 7 полублоков исходного пользовательского ключа (7 x 64 = 448 бит), выход – 4 x 5 + 4 полублоков «сырого» рабочего (развернутого) ключа ((4 x 5 + 4) x 64 = 1536 бит). Использовались тесты лавинного эффекта (AE) и строгого лавинного критерия (SAC). Результаты представлены в табл. 8 и табл. 9.

Таблица 8

Наименование теста	Зависимость между отдельными битами	
	M	D
AE:	799,993670	400,242937
SAC:	0,500000	0,000027
da	0,998758	
ds	0,991720	
dc	1,000000	

Таблица 9

Наименование теста	Зависимость между входными-выходными полублоками	
	M	D
AE: Min:	31,981905	15,999699
Max:	32,012294	16,026774
SAC: Min:	0,500000	0,000027
Max:	0,500000	0,000027

Выводы

Результаты статистического тестирования алгоритма «Торнадо» в режимах поточного шифрования с использованием методики NIST STS показали, что четырехцикловый вариант алгоритма является «статистически безопасным». Полученные данные сопоставимы с эталонной выборкой, сгенерированной генератором ПСП BBS. Кроме того, в режиме «усиленного» поточного шифрования (счетчик с «плавающим периодом»), начиная с трех циклов шифрования без начального и конечного преобразований, выборок, не прошедших какой-либо тест, не наблюдалось. Для более адекватной оценки «статистической безопасности» БСШ был применен корреляционный анализ, который показал, что одноцикловая версия криптоалгоритма является «статистически безопасной».

Аналогичным исследованиям подверглась процедура разворачивания ключа для выявления статистических зависимостей в развернутом («сыром») ключе. Исследование не выявило каких-либо скрытых аномалий в сгенерированной выборке. Количество тестов, в которых тестирование прошло 99% выборок, выше, чем для предлагаемой эталонной выборки ГПСП BBS.

Проведенное исследование показало, что существенное влияние на показатели статистической безопасности оказывают начальное и конечное преобразования IT и FT.

Обобщая полученные результаты, можно сказать, что статистическая безопасность алгоритма «Торнадо» достигается на таком же числе итераций, что и для алгоритма Rijndael (FIPS-197), но меньшем, чем для алгоритмов, победивших в проекте NESSIE.

Список литературы: 1. *NESSIE* Call for Cryptographic Primitives, Version 2.2, 8th March 2000 // NESSIE home page. http://cryptonessie.org. 2. «*A Statistical* Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications», NIST Special Publication 800-22, Washington, 2000. 3. *Головашич С.А.* Безопасность режимов блочного шифрования // Радиотехника: Всеукр межвед. науч.-техн. сб. 2001. Вып. 119. С. 135. 4. *Потий А.В., Орлова С.Ю. и др.* Статистическое тестирование генераторов случайных и псевдослучайных чисел с использованием набора статистических тестов NIST STS // Там же. 2000. Вып. 114. С. 14 – 21. 5. *Гриненко Т.А., Горбенко Ю.И., Орлова С.Ю.* Метод формирования и свойства псевдослучайных последовательностей на эллиптических кривых // Там же. 2001. Вып. 119. С. 119 – 123.

Харьковский национальный университет радиоэлектроники

Поступила в редколлегию 11.06.2003