СТАТИСТИЧЕСКОЕ ТЕСТИРОВАНИЕ РОССИЙСКОГО СТАНДАРТА ФУНКЦИИ ХЭШИРОВАНИЯ ГОСТ 34.11-2012 («СТРИБОГ»)

Мордашов Александр Сергеевич, *г. Москва*

Статистическое тестирование блочных шифров для анализа случайности выходных последовательностей относительно входных было впервые применено на конкурсе для блочных шифров AES (Advanced Encryption Standard, конкурсе по выявлению кандидатов на звание американского стандарта шифрования) и на конкурсе для хэш–функций SHA–3 (Secure Hash Algorithm – 3, конкурсе по поиску кандидата на дополнение и дальнейшую замену SHA–1 и SHA–2). Исследования проводились Национальным институтом стандартов и технологий США (National Institute of Standards and Technology, NIST). В дальнейшем была предложена альтернативная методика для тестирования случайности отображения входных последовательностей блочных шифров в выходные. Таким образом, хороший криптографический примитив должен успешно проходить статистическое тестирование, а для нового разрабатываемого алгоритма выполняться соответствующая процедура. В рамках данной работы будет предложена методика тестирования 256–битного ГОСТ 34.11–2012 ("Стрибог") и приведены полученные результаты.

***Ключевые слова**: статистическое тестирование, ГОСТ 34.11–2012, "Стрибог", хэш–функция, блочный шифр, российский стандарт функции хэширования, случайные криптографические преобразования.*

STATISTICAL ANALYSIS OF RUSSIAN HASH FUNCTION STANDARD GOST 34.11-2012 («STREEBOG»)

Alexander Mordashov, *Moscow*

The first time statistical analysis of block ciphers was applied to AES candidates (Advanced Encryption Standard, the process to choose and ratify the symmetric block cipher as a standard by National Institute of Standards and Technology of United States, NIST) and SHA–3 candidates (Secure Hash Algorithm – 3, which was chosen in the NIST hash function competition to complement the older SHA–1 and SHA–2). The analysis was developed and held by NIST specialists. Later an alternative method of statistical testing of the output sequences of block ciphers was proposed. So every good hash function or block cipher has to be statistically tested and every new developed cryptographic primitive has to pass such procedure. In this paper, a method of testing of 256–bit GOST 34.11–2012 ("Streebog") is proposed and the results of testing are shown.

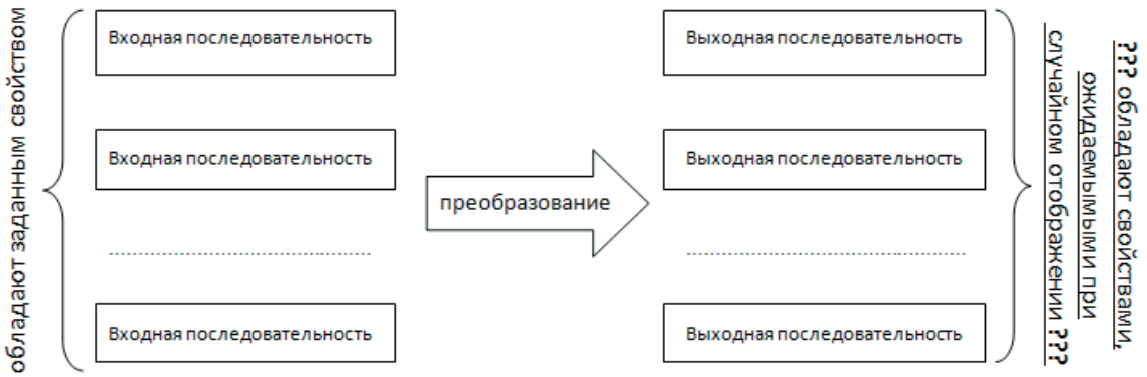
***Keywords**: statistical analysis, GOST 34.11–2012, Streebog, hash function, block cipher, Russian hash function standard, random cryptographic transformations.*

Введение

Цель работы – проведение исследования криптографических свойств 256-битного российского стандарта функции хеширования ГОСТ 34.11-2012 («Стрибог»)[1].

Для разработки методики статистического исследования хэш-функций использовались работы J.Soto [1][2][3], A. Doganaksoy [4][5], F.Sulak[6]. В [1] приведена методика тестирования криптографических примитивов с длинными выходными последовательностями. В [2] и [3] данная методика была использована для тестирования шифров кандидатов на конкурсе AES, при этом для получения длинных последовательностей для тестирования проводилась конкатенация выходных последовательностей блочных шифров. В [4] была предложена альтернативная методика статистического тестирования блочных шифров и хэш-функций без конкатенации выходных последовательностей, которая дала более сильные результаты, чем в [3]. В [6] был приведён способ изменения методики [1] для возможности её применения к блочным шиф-

1 ГОСТ 34.11 – 2012 описан в «Информационная технология. Криптографическая защита информации. Функция хэширования», www.infotecs.ru .



рам и хэш-функциям без конкатенации выходных последовательностей.

После анализа вышеприведённых работ были поставлены следующие задачи:

Разработать методику статистического тестирования свойств 256-битной хэш-функции.

Провести статистическое тестирование свойств 256-битного российского стандарта ГОСТ 34.11-2012 («Стрибог») в зависимости от числа раундов выполнения криптографических преобразований.

Разработка методики статистического тестирования свойств 256-битной хэш-функции.

Хэш-функция может быть представлена в виде отображения множества входных последовательностей во множество выходных последовательностей. В соответствии с [4] данное отображение должно быть неотличимым от случайного отображения. То есть при тестировании свойства хэш-функции для множества входных последовательностей с заданными свойствами множество выходных последовательностей должно обладать свойствами, ожидаемыми от множества выходных последовательностей при случайном отображении.

Тестируемые свойства хэш-функций были выбраны в соответствии с [2], [3], [4]:

- Лавинный эффект
- Корреляция входных и выходных данных
- Возможность работы в режиме CBC
- Устойчивость к входным последовательностям малого веса
- Устойчивость к входным последовательностям большого веса
- Линейная независимость выходных последовательностей для линейно зависимых входных последовательностей
- Размер множества выходных последовательностей
- Стойкость к коллизиям

Для разработки методики были использованы следующие наборы тестов:

NIST [1]

CRYPT-X[2]

DIEHARD [3]

TESTU01 [4]

Дональда Кнута[5]

Али Доганаксоя [4][5]

Генераторы истинно случайных чисел (физические генераторы) порождают последовательности, обладающие некоторыми свойствами, называемыми свойствами случайных последовательностей. Статистические тесты последовательностей на случайность производят проверку, обладает ли тестируемая последовательность заданным свойством случайной последовательности. В тестах CRYPT-X было предложено разбить тесты на группы по характеру тестируемых свойств последовательностей. Множество групп было дополнено и имеет вид:

- Uniformity tests
- Pattern tests
- Period tests
- Compression tests
- Dependence tests
- Cumulative sums tests
- Integer tests
- Other tests
- Cryptographic randomness tests

Тесты из выше озвученных наборов были раз-

2 Тесты, разработанные в Квинслендском техническом университете.

3 Тесты, разработанные в Государственном университете Флориды. http://stat.fsu.edu/pub/diehard/

4 Библиотека тестов для проверки генераторов случайных чисел http://www.iro.umontreal.ca/~simardr/testu01/tu01.html

5 Использовались алгоритмы, приведённые в главе 3 книги Дональд Кнут Искусство программирования, том 2. Получисленные алгоритмы = The Art of Computer Programming, vol.2. Seminumerical Algorithms. — 3-е изд. — М.:"Вильямс», 2007.

Таблица 1.

1.	*Uniformity Tests*	Частотный побитовый тест NIST, частотный блочный тест NIST
2.	*Pattern Tests*	Тест на совпадение неперекрывающихся шаблонов NIST, тест на совпадение перекрывающихся шаблонов NIST.
3.	*Period Tests*	Тест на линейную сложность NIST, тест на периодичность NIST
4.	*Compression Tests*	Тест Лемпеля-Зива
5.	*Dependence Tests*	тест рангов бинарных матриц NIST, тест приблизительной энтропии NIST, тест бинарной производной CRYPT-X
6.	*Cumulative Sums Tests*	Тест случайных проходов TESTU01
7.	*Integer Tests*	Критерий собирания купонов Кнута, критерий «максимум-t» Кнута
8.	*Other Tests*	Тест на самую длинную последовательность единиц в блоке NIST
9.	*Cryptographic Randomness Tests*	SAC тест, тест покрытия, тест на коллизии, тест линейной оболочки

биты на эти группы. В каждой группе при этом могут присутствовать однотипные тесты, совместная реализация которых в методике тестирования не целесообразна. Ввиду этого среди однотипных был произведён выбор наилучших по следующей оценочной функции:

$td_i(A_l, P_i) = r_i$ – статистический тест на случайность

$$F\left(td_{i_k}\left(A, P_{i_k}\right)\right) = \frac{ShrtSq\left(td_{i_k}\left(A, P_{i_k}\right)\right)}{Time\left(td_{i_k}\left(A, P_{i_k}\right)\right) \cdot NumSq\left(td_{i_k}\left(A, P_{i_k}\right)\right)} \rightarrow max$$

$$F(td_{i_k}(A, P_{i_k})) \neq 0$$

$ShrtSq$ – функция, равная 1, если для теста возможно вычисление статистики для примитивов с короткими выходными последовательностями, и равная 0 иначе;

$Time$ – время работы теста для одной входной последовательности;

$NumSq$ – число требуемых последовательностей для работы теста;

A – множество тестируемых последовательностей;

P – множество параметров теста;

i – номер группы тестов;

k – номер теста в группе;

r – результат выполнения теста.

После выбора наилучших тестов среди однотипных были получены результаты, приведенные в таблице 1.

В 9 группе представлены тесты из [4], проводящие тестирование непосредственно криптографического примитива с короткой выходной последовательностью.

В группах 1-8 представлены тесты, предназначенные для тестирования длинных бинарных последовательностей на случайность. Данные тесты были адаптированы в соответствии с результатами работы [6] для применения к хэш-функциям с 256-битными выходными последовательностями.

После адаптации тестов из групп 1-8 можно сформулировать методику тестирования:

1) Для первого раунда выполнения криптографического преобразования применить тесты в соответствии с тестируемыми свойствами:

Лавинный эффект	SAC тест
Корреляция входных и выходных данных	Адаптированные тесты
Возможность работы в режиме CBC	Адаптированные тесты
Устойчивость к входным последовательностям малого веса	Адаптированные тесты
Устойчивость к входным последовательностям большого веса	Адаптированные тесты
Линейная независимость выходных последовательностей при линейно зависимых выходных последовательностях	Тест линейно оболочки
Размер множества выходных последовательностей	Тест покрытия
Стойкость к коллизиям	Тест на коллизии

2) Выполнить шаг 1 для множества выходных последовательностей последующих раундов выполнения криптографического преобразования;

3) Результат тестирования – минимальное

количество раундов выполнения криптографических преобразований, после которых хэш-функция проходит все тесты, то есть становится неотличимой от случайного отображения.

Тестирование ГОСТ 34.11-2012 («Стрибог»)

Для проведения тестирования была программно реализована описанная методика. Также был программно реализован алгоритм «Стрибог» и протестирована его 256-битная версия.

Были получены следующие результаты:

Свойство	Результат применения методики
Лавинный эффект изменения открытого текста	3
Корреляция входных и выходных данных	1
Возможность работы в режиме CBC	2
Устойчивость к входным данным малого веса	2
Устойчивость к входным данным большого веса	2
Линейная независимость выходных последовательностей для линейно зависимых входных последовательностей	1
Размер множества выходных последовательностей	1
Стойкость к коллизиям	3

Из таблицы видно, что ГОСТ 34.11-2012 «Стрибог», имеющий 13 раундов криптографических преобразований, обладает всеми заданными свойствами после 3 раундов выполнения. Данный результат показывает хорошие статистические свойства алгоритма в соответствии с составленной методикой. При этом наибольшую слабость данный алгоритм проявил при тестировании лавинного эффекта и стойкости к коллизиям.

Заключение

В данной работе был произведён анализ работ по статистическому тестированию блочных шифров и хэш-функций и составлена методика для тестирования 256-битных хэш-функций.

По составленной методике был проведён статистический анализ 256-битного варианта ГОСТ 34.11-2012 («Стрибог»). В соответствии с ней алгоритм становится неотличимым от случайного отображения после 3-х раундов выполнения криптографических преобразований. При этом наибольшую слабость данный алгоритм проявил при тестировании лавинного эффекта и стойкости к коллизиям.

Литература (References):

1. A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo «A statistical test suite for random and pseudorandom number generators for cryptographic applications», c. 2.1 – 3.24 // NIST Special Publication 800-22, Revision 1a, April 2010.
2. Juan Soto «Randomness Testing of the AES Candidate Algorithms», c. 5 // NIST Interagency or Internal Report (NIST IR) 6390, September 1999.
3. Juan Soto «Randomness Testing of the Advanced Encryption Standard Finalist Candidates», c. 4 – 10 // NIST Interagency or Internal Report (NIST IR) 6483, April 2000.
4. Ali Doganaksoy, Barıs¸ Ege, Onur Kocak and Fatih Sulak «Cryptographic Randomness Testing of Block Ciphers and Hash Functions», c. 2 – 11 // Cryptography ePrint Archive: Report 2010/564, 11 November 2010.
5. Ali Doganaksoy, Barıs¸ Ege, Onur Kocak and Fatih Sulak «Statistical Analysis of Reduced Round Compression Functions of SHA-3 Second Round Candidates», c. 7 – 9 // Cryptography ePrint Archive: Report 2010/611, 29 November 2010.
6. Fatih Sulak «Cryptographic Random Testing of Block Ciphers and Hash Functions», c.7 – 39 // Publication of the Middle East Technical University Ph.D Examinations, February 2011.