УДК 004.056:003.26

ТЕОРЕТИЧЕСКОЕ ПРИМЕНЕНИЕ DFA К ГОСТ Р 34.12–2015 «КУЗНЕЧИК»

Красовский А.В.

ЮФУ ИТА ИКТИБ, Таганрог, e-mail: an.krasowsckij@gmail.com

Современная конфиденциальность гарантируется стойкостью криптографических алгоритмов. Данные алгоритмы используются во множестве разнообразных исполнений. Функции хэширования присутствуют в «block chain», ассиметричные алгоритмы шифрования в протоколах передачи данных системы «Bitcoin», симметричные алгоритмы шифрования внедрены в смарт карты и т.д. Анализ и поиск уязвимостей криптографических алгоритмов позволяет поддерживать высокий уровень конфиденциальности. В настоящий момент современным стандартом шифрования РФ является шифр Кузнечик [1]. Анализ Кузнечика – это актуальная проблема безопасности РФ. Одним из самых продуктивных способов анализа является DFA. Соответственно автор данной статьи считает крайне актуальным вопросом анализ шифра Кузнечик методом DFA в теории, что позволит выявить общие положения для применения практического анализа Кузнечика с помощью DFA.

Ключевые слова: DFA, Кузнечик, ГОСТ Р 34.12–2015, теоретический анализ

THEORETICAL APPLICATION OF DFA TO GOST R 34.12–2015 «KUZNYECHIK»

Krasovsky A.V.

SFU ETA ICTIS, Taganrog, e-mail: an.krasowsckij@gmail.com

Modern confidentiality guaranteed by the strength of cryptographic algorithms. This algorithms used in many different implementations. Hash functions used in «block chain», asymmetric cipher algorithms used in data transfer protocol in «Bitcoin» system, symmetric cipher algorithms used in smart cards etc. Analysis of crypto algorithms vulnerability allows support high level of confidentiality. Today Kuznyechik [1] is modern cipher standard in Russia Federation. Analysis of Kuznyechik is actual security problem of Russia Federation. One of the most effective approach for analysis is DFA. Author of this paper consider that analysis of Kuznyechik by DFA is very topical theme for research and it allow find common rules for practical analysis of Kuznyechik with DFA.

Keywords: DFA, Kuznyechik, GOST R 34.12–2015, theoretical analysis

В данной работе в разделе 1 описан шифр Кузнечик, в разделе 2 говорится о используемых свойствах шифра, в разделе 3 описан DFA и детали его применения, в разделе 4 описывается алгоритм применения DFA к Кузнечику.

1. Структура шифра Кузнечик

ГОСТ 34.12–2015 «Кузнечик» является блочным симметричным шифром. Он реализован в соответствии с SP сетью, где процесс дешифрования обратен шифрованию. Вход/выход и промежуточные значения имеют размерность 128 бит, ключ имеет размерность 256 бит. Далее все незатронутые детали описания шифра являются не важными для DFA и приведены в [1].

Блоки замены байта p и $\overline{p}$ применяются в рамках блоков S и $\overline{S}$ соответственно и имеют размерность 8 бит. Кузнечик имеет предустановленные таблицы замены, которые можно считать массивами с индексами. Выходом блоков p и $\overline{p}$ является значение, взятое в таблице замены по индексу равному значению входа.

Блоки замены S и $\overline{S}$ имеют входную/выходную размерность 128 бит. Обозначим логическое разбиение 128-битного текста на 16 байт как $a = a_{15} \| a_{14} \| \ldots \| a_0$, $a \in V_{128}$. Схематичное представление блоков S и $\overline{S}$ приведено на рис. 1.

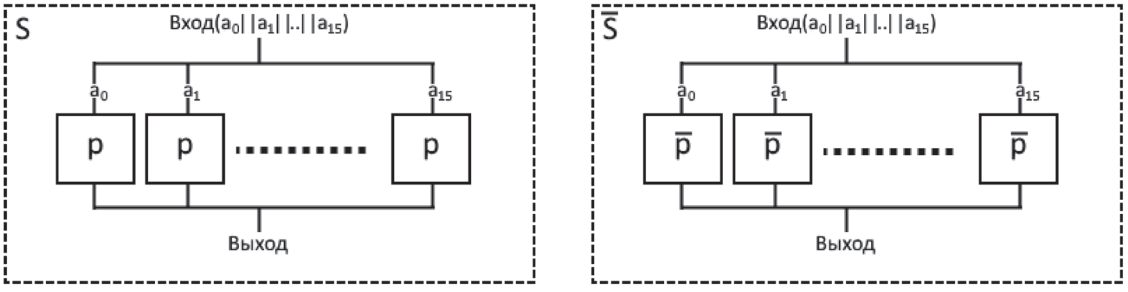

Рис. 1. Блоки S и $\overline{S}$

Блок l имеет размерность входа/выхода 128/8 бит соответственно. Выход генерируется в соответствии с уравнением $\ell(a)$. Умножение у сложение происходят в поле

$$GF(2)[x]/\ p(x),$$

где $p(x) = x^8 + x^7 + x^6 + x + 1$.

Блок R и $\overline{R}$ имеют размерность входа/выхода 128 бит. Они используют блок l для вычисления нового старшего байта

$$\ell\left(a^{15}_{\text{вход}} \| a^{14}_{\text{вход}} \| \ldots \| a^{0}_{\text{вход}}\right) \| a^{15}_{\text{вход}}.$$

А выходом является значение

$$\ell\left(a^{15}_{\text{вход}} \| a^{14}_{\text{вход}} \| \ldots \| a^{0}_{\text{вход}}\right) \| a^{15}_{\text{вход}} \| a^{14}_{\text{вход}} \| \ldots \| a^{1}_{\text{вход}}.$$

Блок L и $\overline{L}$ имеют размерность входа/выхода 128 бит. Они используют R и $\overline{R}$ соответственно последовательно 16 раз.

Процесс шифрования/дешифрования отображаются формулой (1) соответственно. Обозначим $C \in V_{128}$ как закрытый текст и $P \in V_{128}$ как открытый текс, тогда шифрования/дешифрования можно представить:

$$C = X(K_{10})LSX(K_9)\ldots LSX(K_1)(P),$$
$$P = X(K_1)\overline{SL}X(K_2)\ldots\overline{SL}X(K_{10})(C)$$

Ключ шифра имеет размерность 256 бит, а подключ 128 бит. Генерируется 10 подключей для 9 раундов и заключающего X блока. Для выработки подключей используется 32 постоянных продекларированных в стандарте значений C_i.

2. Свойства шифра Кузнечик

Основным свойством шифра Кузнечик для DFA является дифференциальное свойство (ДС) S и $\overline{S}$ блока, а так же L и $\overline{L}$ блока. Данное положение обусловлено характером метода. DFA предполагает сравнение промежуточных значений и дифференциалов различных ПЗ.

Блоки L и $\overline{L}$ обладают свойством дистрибутивности, что упрощает их использование относительно DFA. Блоки S и $\overline{S}$ обладают ДС блоков p и $\overline{p}$. При изучении ДС блоков p и $\overline{p}$ было выявлено, что разные дифференциалы входов образуют разное количество уникальных выходных дифференциалов. Данное ДС для уникальности обозначим как свойство неравномерности распределения (СНР). Далее рассматривается СНР p блока.

СНР представлен на рис. 2, где $a, b \in V_{128}$ это левая и правая часть входного дифференциала соответственно, а значение в матрице кол-во уникальных выходных дифференциалов.

a/b	.0	.1	.2	.3	.4	.5	.6	.7	.8	.9	.A	.B	.C	.D	.E	.F
0.	1	108	102	109	109	107	100	107	107	106	105	110	109	105	111	104
1.	110	110	105	108	106	107	106	102	110	110	107	104	113	105	109	109
2.	102	102	110	106	108	105	98	105	111	107	105	108	109	102	104	106
3.	112	113	109	100	114	113	110	103	111	107	108	107	108	107	107	108
4.	105	107	107	106	106	109	110	104	108	103	106	111	104	109	111	105
5.	106	110	108	108	104	107	103	106	114	110	104	108	104	112	104	109
6.	110	107	111	103	105	104	108	114	109	110	103	106	106	107	107	108
7.	110	106	105	101	108	104	107	108	104	112	109	107	107	104	107	106
8.	103	110	104	108	114	102	103	107	106	107	105	107	110	100	110	102
9.	104	108	105	108	110	105	107	113	101	107	109	113	107	105	100	106
A.	113	105	109	111	109	101	102	107	110	100	106	110	107	103	105	106
B.	110	103	105	106	104	101	110	110	110	112	110	113	105	111	108	105
C.	111	106	111	105	107	109	99	104	103	105	106	111	109	103	106	108
D.	109	106	113	102	103	112	108	104	105	111	106	106	105	105	111	105
E.	105	112	107	105	104	109	106	109	102	107	109	107	109	106	103	104
F.	106	111	108	112	106	107	114	107	113	112	112	113	103	108	109	112

Рис. 2. СНР p блока

Другим свойством p и $\overline{p}$ блоков является неравномерность распределения повторений (СНП). СНП заключается в неравномерности повторений выходных дифференциалов.

На основе СНП был создан алгоритм восстановления значений (АВЗ) [2], который позволяет восстанавливать возможные значения на входе/выходе S блока зная дифференциалы на входе и выходе.

3. Описание DFA

Метод DFA (дифференциальный анализ ошибки) был впервые представлен в 1996 году [3] для RSA. Позже теория DFA была развита для применения к симметричным алгоритмам [4] и получила широкое распространение. DFA предполагает внедрение ошибки в промежуточное значения (ПЗ) этапов вычисления открытого/закрытого текста. Для DFA требуется несколько процессов шифрования/дешифрования. Так же DFA требует знания открытого и закрытого текста или одного из них в зависимости от цели анализа. Данный метод может быть активным не инвазивным или полуинвазивным.

В данной работе для теоретического анализа используется ошибка при которой изменяется один бит в ПЗ. ПЗ принимает значения до входа следующего блока и после выхода предыдущего. При изучении структуры шифра было выявлено, что DFA требует восстановления первых или последних двух подключей. В таком случае восстановление ключа требует двух этапов. На рис. 3 схематически изображаются области ПЗ для двух этапов, которым необходимо внести ошибку при шифровании и восстановления 9, 10 подключей.

4. Алгоритм применения DFA к Кузнечику

Алгоритм применения DFA прежде всего заключается в представлении процесса шифрования как указано на рис. 3. Видно, что $ПЗ_n, ПЗ_{n+1}, ПЗ_{n+2}$, где $n = 1, 4, 7, 10$ образуют группы. В данных группах ПЗ в которые внедряется ошибка приведут к схожему результату восстановления ключа. Чёрным выделен блок восстановления, к которому необходимо применять АВЗ.

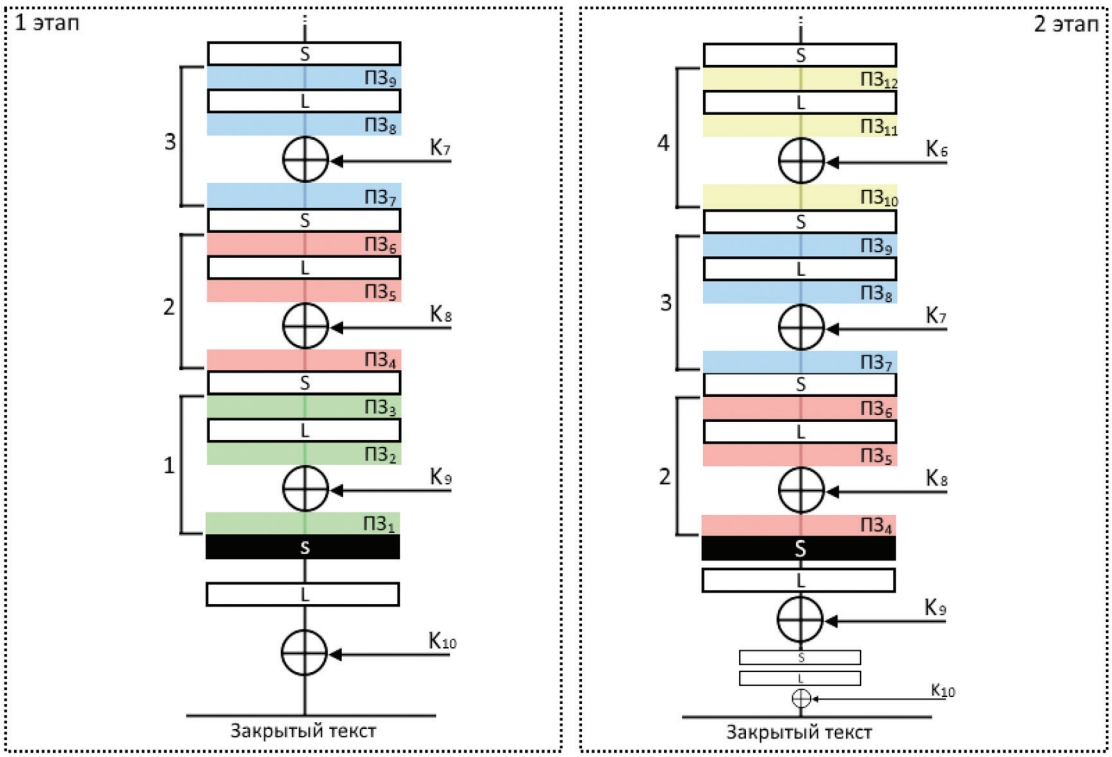

Рис. 3. Этапы анализа Кузнечика с помощью DFA

Количество восстановленных подключей в зависимости от группы

Этап	гр. *i* кол. диф. на вх.	гр. *i*+1 кол. диф. на вх.	гр. *i*+2 кол. диф. на вх.	гр. *i* кол. подключей	гр. *i*+1 кол. подключей	гр. *i*+2 кол. подключей
Этап №1	1	100	2^{119}	$2^{16} - 2^{48}$	$2^{112} - 2^{128}$	$2^{128} - 2^{128}$
Этап №2	1	100	2^{119}	$2^{32} - 2^{96}$	$2^{128} - 2^{128}$	$2^{128} - 2^{128}$

В первую очередь выполняется первый этап алгоритма применения DFA. Оба этапа производятся для одного и того же набора подключей. Ошибка изменяется случайный бит в запланированном ПЗ или группе. Алгоритм первого этапа следующий: шифруется текст *P* и получается закрытый текст *C*, шифруется текст *P* и в какой либо ПЗ внедряется ошибка и получается *C'*, дифференциал $C \oplus C'$ восстанавливается до выхода блока восстановления, дифференциал в каком либо ПЗ восстанавливается до входа блока восстановления, для блока восстановления применяется АВЗ, возможные значения проходят через *L* блок и восстанавливается возможные десятые подключи.

Второй этап аналогичен первому, только последний *S* и *L* блок отбрасываются так как в $ПЗ_3$ возможно вычислить список возможных значений на основе закрытого текста и списка возможных десятых подключей. После восстановления возможных девятых подключей следует для всех пар 10 и 9 подключей вычислить остальные и отфильтровывать их.

Группа в ПЗ которой внедряется ошибка влияет на количество восстановленных подключей. В таблице приведены средние значения количества дифференциалов на входе блока восстановления для двух этапов в зависимости от группы в которую внедрена ошибка и максимальное/минимальное количество восстановленных первых/вторых подключей. Следует сказать, что на рис. 3 и в таблице используется только по 3 группы, но их может быть больше. Слишком удалённая группа от блока восстановления восстановит все возможные ключи, т.е. сложность увеличится до сложности полного перебора.

Значения в таблице представлены без вероятностного фактора фильтрации дифференциалов в АВЗ, что значительно увеличивает кол-во восстанавливаемых ключей.

В данной работе был описан способ применения метода DFA к шифру Кузнечик, представлено описание алгоритма применения DFA в общем виде. В работе описанные дифференциальные свойства блоков шифра и описан сам шифр. Так же приведена таблица сложностей восстановления ключа в зависимости от групп внедрения ошибки.

Можно заключить, что шифр Кузнечик потенциально имеет слабость относительно DFA без учёта фильтрации дифференциалов при применении АВЗ.

Список литературы

1. ГОСТ 34.12.-2015. Кузнечик [Электронный ресурс]. – URL: http://www.tc26.ru/standard/draft/GOSTR-bsh.pdf (дата обращения 21.08.2017).

2. Красовский А.В. Анализ криптографической стойкости шифра «Кузнечик» методом связанных ключей. [Электронный ресурс]. – URL: https://www.scienceforum.ru/2017/pdf/36877.pdf (дата обращения 13.01.2018).

3. Dan Boneh, Richard A. Demillo, Richard J. Lipton, On the Importance of Checking Cryptographic Protocols for Faults, Lecture Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT97, pp. 37–51, 1997.

4. Eli Biham, Adi Shamir. Differential Fault Analysis of Secret Key Cryptosystems. [Электронный ресурс]. – URL: https://pdfs.semanticscholar.org/440f/a56b0618578b34c7a4fb781fc40388bf8e18.pdf (дата обращения 14.01.2018).