ВОПРОСЫ КРИПТОГРАФИЧЕСКОЙ СТОЙКОСТИ БАЗОВОГО АЛГОРИТМА «ЛЮЦИФЕР»

М. В. Одинцов, М. В. Башлаков, А. П. Мартынов, А. В. Точилин

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Преобразование информации и восстановление преобразованной информации связаны с применением алгоритмов криптографического преобразования данных, имеющих определенные характеристики и свойства. Для выявления недостатков и закономерностей преобразований необходимо провести исследования значений выходной последовательности, получаемых в ходе преобразования, а также подсчитать количество появлений фиксированных значений выходной последовательности в зависимости от входных данных. Результаты такого подхода позволяют обнаружить значения входных данных, уязвимых с точки зрения информационной безопасности, и выявляют ненадежные варианты построения криптоалгоритмов.

Большинство из известных криптоалгоритмов при преобразовании данных использует функции, которые можно разделить на две основные группы – функции с элементами подстановки и функции с элементами перестановки. Блоки, выполняющие данные функции, были взяты за основу и при реализации криптоалгоритма «Люцифер» фирмы IBM. Существует несколько модификаций криптоалгоритма «Люцифер», отличающихся от базового варианта криптоалгоритма наличием дополнительных блоков математических преобразований, введение которых обусловлено наличием закономерностей в преобразовании данных и потребностью в обеспечении рассеивания значащих битов данных посредством нелинейных преобразований.

Базовый вариант криптоалгоритма «Люцифер» основан на итерационном применении совокупности криптографических операций, реализующих функции подстановки − S-блок (от англ. S-box (substitution box) − блок подстановки) и перестановки − P-блок (от англ. P-box (permutation box) − блок перестановки). Размерности данных блоков могут быть различными (до 128 разрядов битов данных) и зависят от степени сложности криптосистемы, которую стремится создать пользователь. Стоит отметить, что размерность блока преобразуемых данных (N) равна размерности P-блока, в то время как размерность (n) S-блока зависит от количества используемых в алгоритме S-блоков и определяется как отношение размерности N к количеству S-блоков.

На рис. 1 показана структура базовой версии криптоалгоритма «Люцифер», в которой N = 16 разрядов, а n = 4 разряда.

Входными данными для каждой итерации (за исключением начальной) являются данные, полученные с выхода преобразования на предыдущей итерации. Пользователь криптоалгоритма посредством ввода ключевой информации (ключа), представленной в двоичной системе счисления, определяет выбор одного из двух возможных вариантов подстановки (S_0 или S_1) для каждой позиции блока подстановки.

S-блок преобразует n разрядов входных данных в n разрядов выходных данных. Структура данного блока приведена на рис. 2.

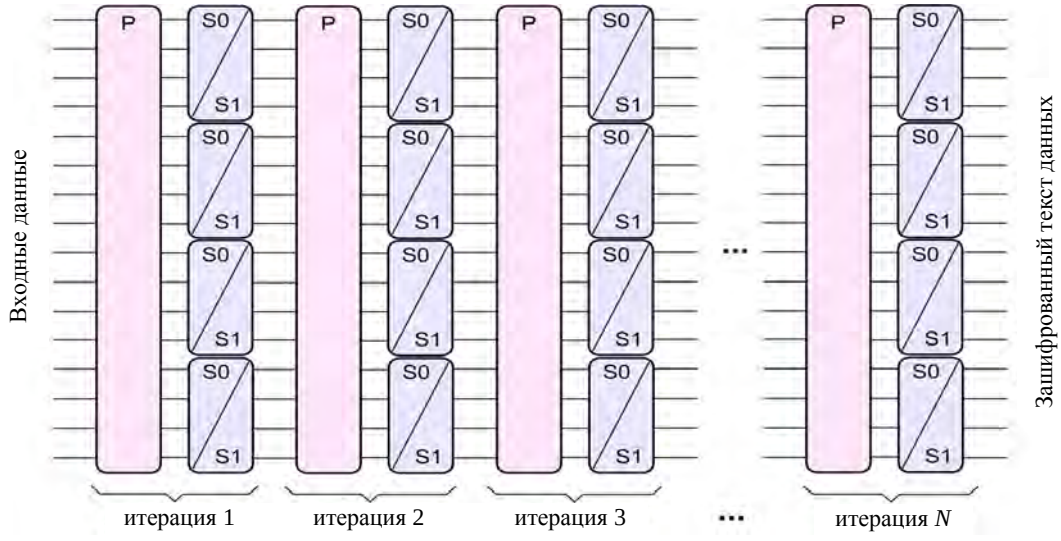

Рис. 1. Структура базовой версии криптоалгоритма «Люцифер»

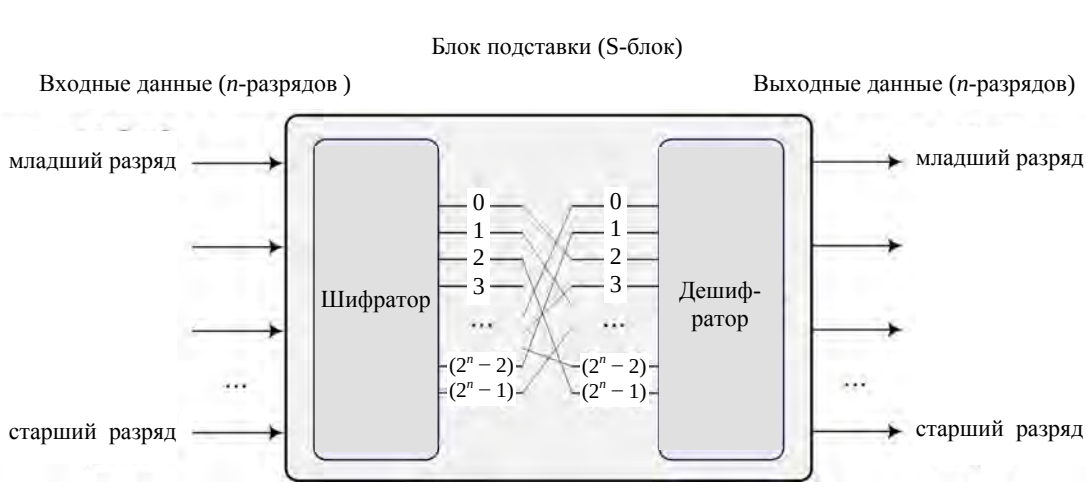

Рис. 2. Структура блока подстановки криптоалгоритма «Люцифер»

S-блок является основным для криптоалгоритма «Люцифер», так как осуществляет нелинейное преобразование информации (т. е. количество единиц и нулей на входе и выходе блока отличаются друг от друга). Данные, поступающие на вход блока подстановки в двоичном n-битном коде, преобразуются в шифраторе в позиционный 2^n-1-разрядный код. Выходы шифратора с помощью перемычек соединяются со входами дешифратора, который осуществляет обратное преобразование 2^n-1-разрядного входного кода в двоичный n-битный выходной код.

P-блок преобразует все N входных битов информации в N выходных битов, осуществляя при этом перемешивание битов. Структура данного блока приведена на рис. 3.

Рис. 3. Структура блока перестановки криптоалгоритма «Люцифер»

P-блок осуществляет линейное преобразование информации (т. е. количество единиц и нулей на входе и выходе блока остается неизменным). Данные в блоке перестановки передаются со входа на выход по заранее установленным перемычкам.

Структура построения криптоалгоритма «Люцифер» во многом определяет криптографическую стойкость как самого алгоритма, так и преобразованных данных. При этом увеличение размерности используемых блоков подстановки и перестановки значительно усложняет работу по определению исходных данных на основании преобразованного текста данных, так как многократно возрастают временные и вычислительные ресурсы. Кроме того, существенным фактором, влияющим на стойкость алгоритма и преобразованного текста, является многоразрядный ключ, определяющий порядок выбора S-блоков.

В данной статье приводятся результаты исследований структуры построения базового варианта криптоалгоритма «Люцифер» в части выявления закономерностей преобразования входных данных, а также определения сочетаний блоков подстановки и перестановки, нежелательных для практического применения ввиду слабых свойств преобразования входных данных.

В ходе проведения исследовательской работы было реализовано программное обеспечение, осуществляющее преобразование данных в соответствии с базовым вариантом криптоалгоритма, при этом рассматривались блоки перестановки и подстановки с различными размерностями. Для более наглядного отображения в данной статье приводятся результаты для случая одной итерации преобразования, когда размерность входных данных и, следовательно, размерность блока перестановки (P-блока) равна 4 разрядам (N = 4), а размерность блока подстановки (S-блока) равна 2 разрядам (n = 2), при этом используемые S-блоки идентичны друг другу, таким образом, значение ключа алгоритма не берется во внимание.

Поясним материал, изложенный в предыдущем абзаце. На вход P-блока последовательно подаются входные данные со значениями от 0000 (двоичная система счисления) до 1111 (двоичная система счисления), что соответствует значениям от 0 до F в 16-ричной системе счисления. После преобразования на выходе P-блока четырехразрядные данные разбиваются на две двухразрядные последовательности, которые поступают на входы идентичных S-блоков, после преобразования в которых данные вновь объединяются в четырехразрядную последовательность (выходную).

В табл. 1 показано количество появлений всех возможных значений выходной последовательности после преобразования на исчерпывающем переборе S- и P-блоков для каждого значения входной последовательности.

Из таблицы видно, что:

1) Входные последовательности, имеющие одинаковые значения во всех четырех разрядах (0000 и 1111 в двоичной системе счисления), имеют на выходе после преобразования только четыре значения. Это связано с тем, что для таких последовательностей P-блок неэффективен, так как не осуществляет перемешивания битов. Поэтому на выходе мы имеем $2^n = 4$ (при разрядности S-блока $n = 2$) выходных значений, что соответствует количеству всех возможных значений, которые могут выдать два двухразрядных S-блока.

2) Входные последовательности, имеющие одинаковые значения в любых двух разрядах (0011, 0101, 0110, 1001, 1010 и 1100 в двоичной системе счисления), имеют на выходе преобразования все возможные значения, причем появление большинства выходных значений имеет равную вероятность.

3) Входные последовательности, имеющие одинаковые значения в любых трех разрядах (0001, 0010, 0100, 0111, 1000, 1011, 1101 и 1110 в двоичной системе счисления), имеют на выходе преобразования все возможные значения с равной вероятностью появления. Исключение составляют выходные последовательности, у которых пары младших и старших разрядов равны друг другу, т. е. выходных последовательностей со значениями 0000, 0101, 1010, 1111 (в двоичной системе счисления) в данном случае быть не может. Это связано с тем, что на входы двух одинаковых S-блоков никогда не поступят одинаковые пары (00, 01, 10, 11), так как на выходе четырехразрядного P-блока всегда будет один разряд, отличающийся от трех других разрядов, и следовательно, на входы двух S-блоков алгоритма всегда будут поступать различные по значению пары.

После анализа выявленных закономерностей преобразования для рассматриваемого случая целесообразно исключить из практического применения в качестве входной последовательности данные с четырьмя одинаковыми разрядами. Для получения текста данных, стойкого к криптоанализу со стороны злоумышленника, лучше всего использовать последовательность, имеющую одинаковые значения в двух любых разрядах.

Важным фактором при построении стойкого криптоалгоритма является выявление вариантов построения функциональных блоков, для которых выходная последовательность может быть определена злоумышленником с высокой долей вероятности по известной входной последовательности. С целью определения таких функциональных блоков были проведены исследования по следующим двум направлениям:

1) Рассматривались структуры криптоалгоритма, в которых для каждого из вариантов S-блока последовательно выбирались все варианты P-блока, при этом на вход P-блока подавались все возможные значения (от 0000 до 1111 в двоичной системе счисления). Подсчитывалось количество совпадений значений входной и выходной последовательностей для каждого из вариантов S-блока при исчерпывающем переборе P-блоков.

2) Рассматривались структуры криптоалгоритма, в которых для каждого из вариантов P-блока последовательно выбирались все варианты S-блока, при этом на вход P-блока подавались все возможные значения (от 0000 до 1111 в двоичной системе счисления). Подсчитывалось количество совпадений значений входной и выходной последовательностей для каждого из вариантов P-блока при исчерпывающем переборе S-блоков.

Для первого исследования были получены результаты, которые отображены на диаграмме на рис. 4.

Таблица 1

Вых. посл-ть	Входная последовательность (16-ая система счисления)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	Количество появлений (10-ая система счисления)															
0	144	0	0	48	0	48	48	0	0	48	48	0	48	0	0	144
1	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
2	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
3	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
4	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
5	144	0	0	48	0	48	48	0	0	48	48	0	48	0	0	144
6	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
7	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
8	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
9	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
A	144	0	0	48	0	48	48	0	0	48	48	0	48	0	0	144
B	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
C	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
D	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
E	0	48	48	32	48	32	32	48	48	32	32	48	32	48	48	0
F	144	0	0	48	0	48	48	0	0	48	48	0	48	0	0	144

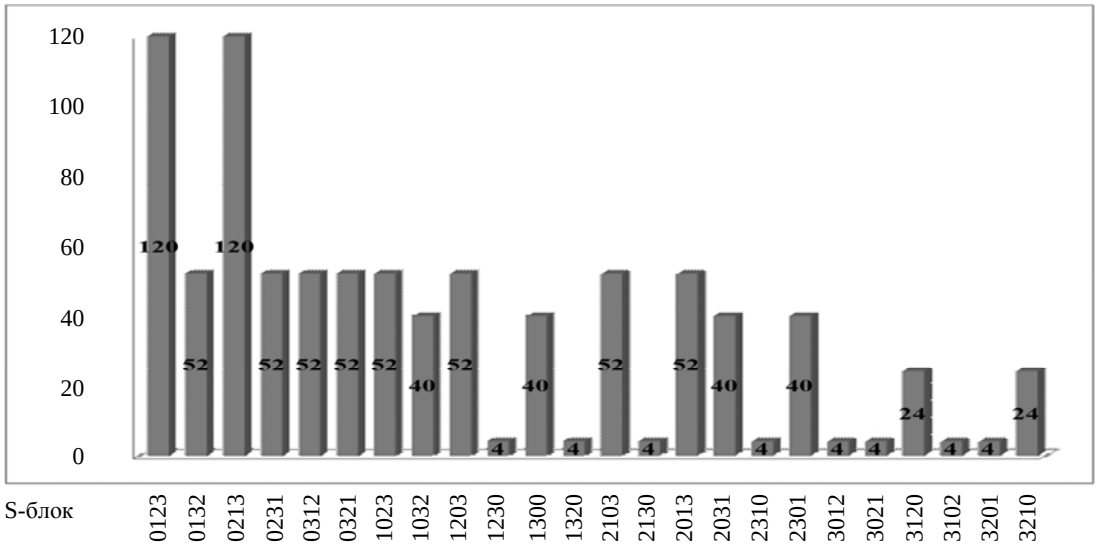

Рис. 4. Диаграмма совпадений входной и выходной последовательностей для каждого варианта S-блока при исчерпывающем переборе P-блоков

На рис. 4 вдоль оси абсцисс показаны все варианты S-блока, на вход которого поступают двухразрядные данные. Цифры от 0 до 3 означают номера входов дешифратора S-блока, к которым в такой последовательности посредством перемычек подсоединены выходы шифратора (например, последовательность цифр 2301 для S-блока означает, что «0» выход шифратора соединен с «2» входом дешифратора, «1» с «3», «2» с «0», а «3» с «1»). Из рисунка видно, что выбор S-блока является важным моментом при построении стойкого криптоалгоритма, при этом наиболее оптимальными вариантами блока подстановки являются блоки, у которых нулевой вывод шифратора соединен с последним входом дешифратора. Такие структуры обеспечивают наибольшую трансформацию входных данных.

Для второго исследования были получены результаты, которые отображены на диаграмме на рис. 5.

На рис. 5 вдоль оси абсцисс показаны все варианты P-блока, на вход которого поступают четырехразрядные данные. Цифры от 0 до 3 означают номера выходов P-блока, к которым в такой последовательности посредством перемычек подсоединены входы P-блока (например, последовательность цифр 2301 для P-блока означает, что «0» вход блока соединен с «2» выходом блока, «1» с «3», «2» с «0», а «3» с «1»). Из рисунка видно, что все P-блоки можно разделить на две группы по количеству совпадений, при этом в среднем разброс появлений совпадений для каждого P-блока на исчерпывающем переборе S-блоков и входных последовательностей можно считать незначительным.

Для определения структур криптоалгоритма, обеспечивающих надежное преобразование без повторения входной последовательности, сформирована табл. 2, содержащая количество совпадений входной и выходной последовательностей для всех возможных сочетаний S- и P-блоков при подаче на вход всех возможных четырехразрядных значений.

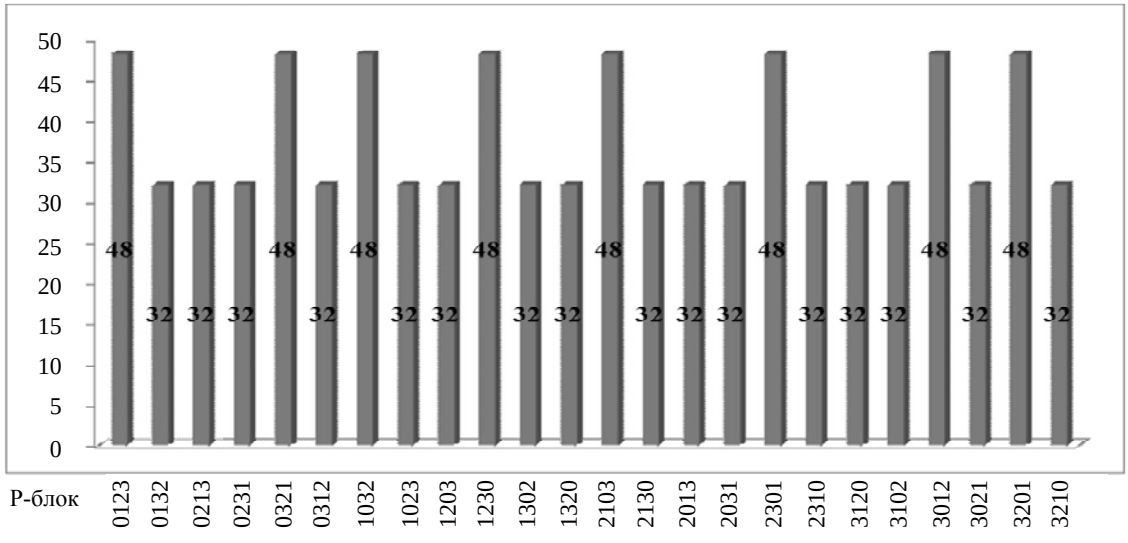

Рис. 5. Диаграмма совпадений входной и выходной последовательностей для каждого варианта P-блока при исчерпывающем переборе S-блоков

Таблица 2

S-бл / P-бл	0123	0132	0213	0231	0312	0321	1023	1032	1203	1230	1302	1320	2103	2130	2013	2031	2310	2301	3012	3021	3120	3102	3201	3210	$\Sigma_{P\text{-блок}}$
0123	16	4	4	1	1	4	4	0	1	0	0	1	4	1	1	0	0	0	0	1	4	1	0	0	48
0132	8	2	8	2	2	2	2	0	2	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	32
0213	8	2	2	2	2	2	2	0	2	0	2	0	2	0	2	2	0	0	0	0	2	0	0	0	32
0231	4	2	4	2	2	2	2	0	2	0	0	0	2	0	2	4	0	4	0	0	0	0	0	0	32
0321	8	4	2	1	1	4	4	0	1	0	2	1	4	1	1	2	0	8	0	1	2	1	0	0	48
0312	4	2	4	2	2	2	2	0	2	0	4	0	2	0	2	0	0	4	0	0	0	0	0	0	32
1032	4	1	16	4	4	1	1	0	4	1	0	0	1	0	4	0	1	0	1	0	0	0	1	4	48
1023	8	2	8	2	2	2	2	0	2	0	0	0	2	0	2	0	0	0	0	0	0	0	0	0	32
1203	4	2	4	2	2	2	2	4	2	0	0	0	2	0	2	4	0	0	0	0	0	0	0	0	32
1230	2	1	8	4	4	1	1	2	4	1	0	0	1	0	4	8	1	2	1	0	0	0	1	2	48
1302	2	2	8	2	2	2	2	2	2	0	0	0	2	0	2	0	0	2	0	0	0	0	0	2	32
1320	4	2	4	2	2	2	2	0	2	0	0	0	2	0	2	4	0	4	0	0	0	0	0	0	32
2103	8	4	2	1	1	4	4	8	1	0	2	1	4	1	1	2	0	0	0	1	2	1	0	0	48
2130	4	2	4	2	2	2	2	4	2	0	0	0	2	0	2	4	0	0	0	0	0	0	0	0	32
2013	4	2	4	2	2	2	2	4	2	0	4	0	2	0	2	0	0	0	0	0	0	0	0	0	32
2031	2	2	8	2	2	2	2	2	2	0	0	0	2	0	2	0	0	2	0	0	0	0	0	2	32
2301	4	4	4	1	1	4	4	4	1	0	0	1	4	1	1	0	0	4	0	1	4	1	0	4	48
2310	2	2	2	2	2	2	2	2	2	0	2	0	2	0	2	2	0	2	0	0	2	0	0	2	32
3120	8	2	2	2	2	2	2	0	2	0	2	0	2	0	2	2	0	0	0	0	2	0	0	0	32
3102	4	2	4	2	2	2	2	4	2	0	4	0	2	0	2	0	0	0	0	0	0	0	0	0	32
3012	2	1	8	4	4	1	1	2	4	1	8	0	1	0	4	0	1	2	1	0	0	0	1	2	48
3021	4	2	4	2	2	2	2	0	2	0	4	0	2	0	2	0	0	4	0	0	0	0	0	0	32
3210	4	1	4	4	4	1	1	0	4	1	4	0	1	0	4	4	1	0	1	0	4	0	1	4	48
3201	2	2	2	2	2	2	2	2	2	0	2	0	2	0	2	2	0	2	0	0	2	0	0	2	32
$\Sigma_{S\text{-блок}}$	120	52	120	52	52	52	52	40	52	4	40	4	52	4	52	40	4	40	4	4	24	4	4	24	896

В данной таблице по столбцам расположены все варианты S-блоков, по строкам – все варианты P-блоков. На пересечении строк и столбцов – количество совпадений входных и выходных данных для определенного сочетания S- и P-блоков. Последние строка и столбец отражают суммарное количество совпадений для данного S- и P-блока, соответственно.

Применение для преобразования данных оптимальных сочетаний блоков перестановки и подстановки в совокупности с применением входных данных, имеющих одинаковые значения в любых двух разрядах, способствует созданию текста данных, стойкого к вскрытию со стороны злоумышленника.

Заключение

В данной статье приведены результаты исследований, которые могут быть применены при создании стойкого криптоалгоритма, основанного на функциях подстановки и перестановки. Приведен способ определения входных данных, уязвимых с точки зрения информационной безопасности. Показан прием, который позволяет выявить слабые места при построении криптоалгоритмов и, наоборот, определить оптимальные сочетания блоков подстановки и перестановки для преобразования данных.

В статье отражены результаты исследования только для четырехразрядного блока входных данных. Приемы и методы, описанные в статье, можно распространить на блоки данных, имеющие значительно большую размерность.

Литература

1. Мартынов А. П., Фомченко В. Н. Криптография и электроника / Под ред. А. И. Астайкина. Саров: РФЯЦ-ВНИИЭФ, 2006.

2. Sorkin A. Lucifer, a cryptographic algorithm // Cryptologia. 1984. N 8. P. 22–42.

3. Smith J. L. U.S. Patent N 3796830. Recirculating Block Cipher Cryptographic System. 1974.

4. Feistel H. U. S. Patent N 3798359. Block Cipher Cryptographic System. 1974.

5. Ben-Aroya I., Biham E. Differential cryptanalysis of Lucifer: Technical report CS0782. Haifa, Technion. 1993. P. 2–9.