

*А. В. Архангельская, Ж. А. Чиненова*

# ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ХАРАКТЕРИСТИК БЛОЧНОГО АЛГОРИТМА ШИФРОВАНИЯ TWIS

Блочный алгоритм шифрования TWIS [1] был впервые представлен в 2009 г. на Международной конференции по безопасности информационных систем (International Conference on Information Systems Security — ICISS) и предназначен для устройств с ограниченными ресурсами. Шифр построен на обобщенной структуре Фейстеля и состоит из десяти раундов зашифрования/расшифрования. Над блоками шифруемого текста производятся два вида операций: линейные сдвиги и применение нелинейного отображения (узла замены). Для увеличения стойкости алгоритма перед зашифрованием данных применяется алгоритм развертывания ключа.

Криптографическая схема зашифрования для алгоритма TWIS показана на рис. 1, где $P_i$ — блоки открытого текста, $T_i$ — промежуточные блоки шифруемого текста, $C_i$ — блоки шифрованного текста, $RK_i$ — раундовые ключи, а функция $G$ имеет два аргумента: 32-битовый раундовый ключ и блок данных длиной 64 бита. Функция расшифрования является обратной к функции зашифрования, т. е. все операции в алгоритме зашифрования заменены на обратные и выполняются в обратном порядке.

Алгоритм развертывания ключа (рис. 2) позволяет вычислить 32-битовые цикловые (раундовые) ключи $RK_i$ $(0 \le i \le 10)$ по 128-битовому ключу шифрования $K$. Диффузионная матрица и узел замены, на вход которого подается 6 бит, а возвращается 8 бит, обеспечивают свойство рассеивания при выработке зашифрованного текста.

Для получения криптографических характеристик алгоритма TWIS были изучены преобразования разностей, т. е. побитовых сумм по модулю два, между шифруемыми значениями на отдельных раундах шифрования. Линейные примитивы шифра не влияют на разности двух входных текстов в силу ассоциативности операции сложения по модулю два, в то время как нелинейные примитивы изменяют значение разности и характеризуются вероятностным распределением выходных разностей относительно входных разностей. В работе [2] описана разностная атака на алгоритм шифрования TWIS, для реализации которой используются следующие свойства узла замены:

1. Первые два бита входной последовательности, подаваемой на узел замены, не участвуют в операции: $O = S(I \oplus 0x3f)$, где $S$ — узел замены, $O$ — выходная последовательность, а $I$ — входная последовательность;

2. Входные разности 0x01 и 0x25 переходят в 0x00 с вероятностью $2^{-5}$.

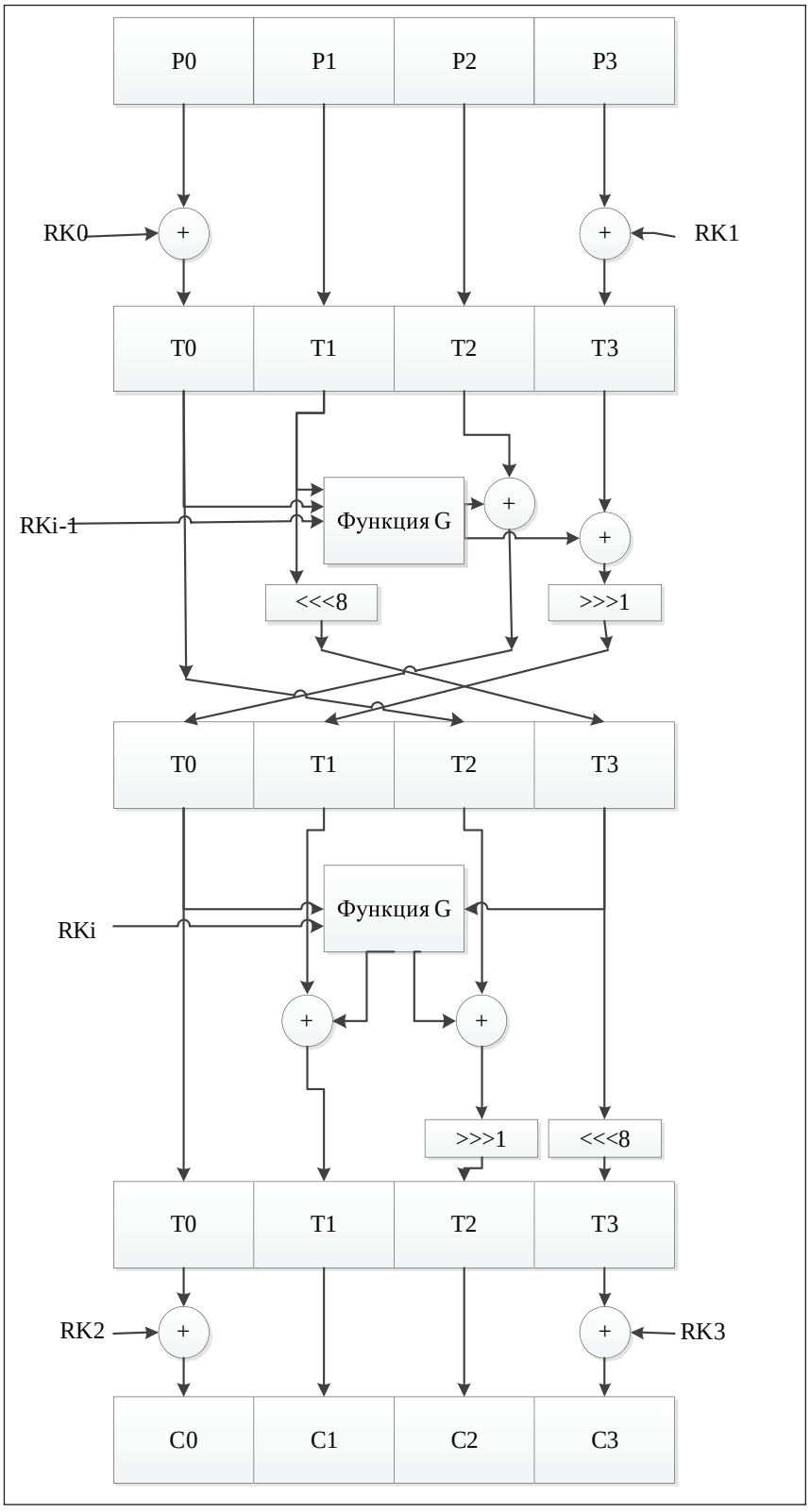


*Рис. 1. Схема зашифрования алгоритма TWIS*

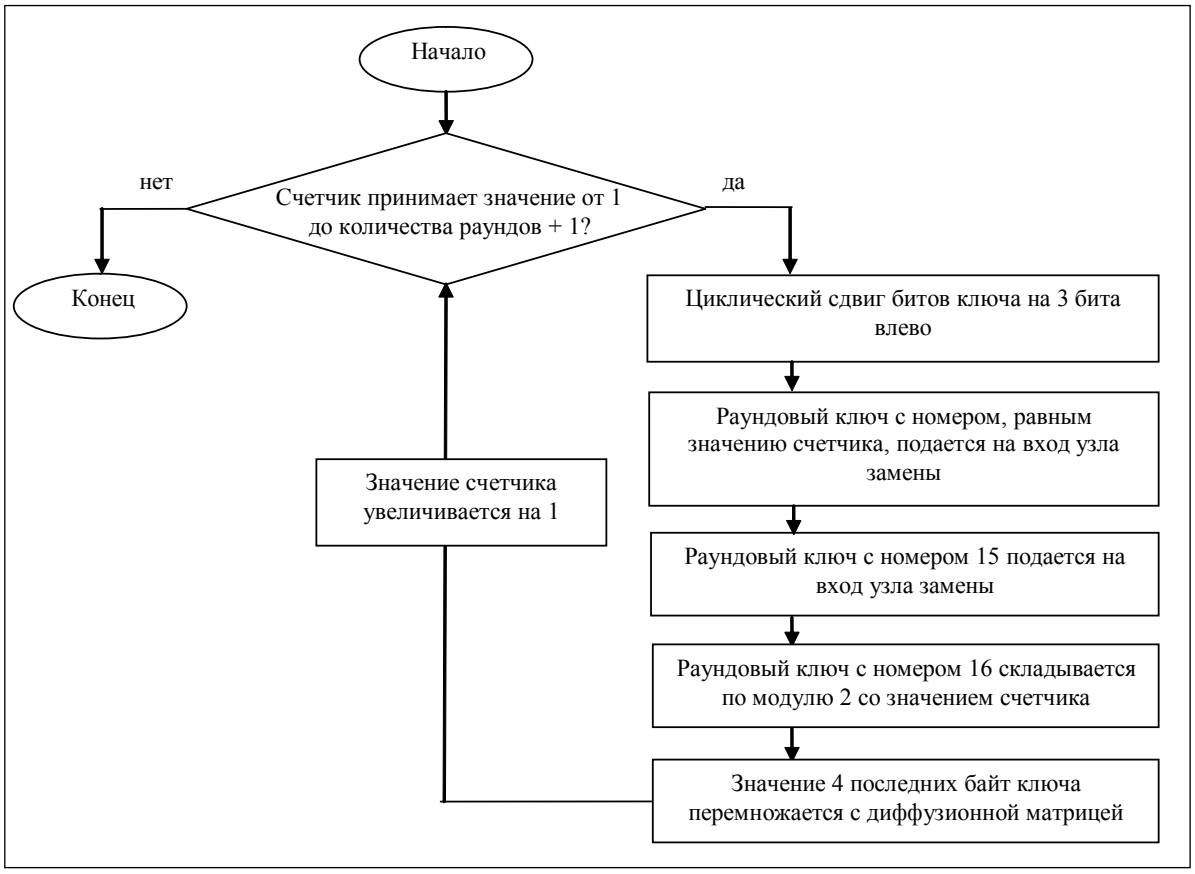


*Рис. 2. Алгоритм развертывания ключа*

Требуемое количество текстов для проведения данной атаки равно $2^{20}$, а сложность ее проведения равна перебору $2^{21}$ открытых текстов. Однако данная атака не использует все свойства алгоритма и проводится при некоторых ограничениях.

Авторами статьи получено распределение вероятностей узла замены, в котором присутствуют следующие значения вероятностей: $0, 2^{-5}, 2^{-4}, 1{,}5 \cdot 2^{-4}, 1$. Наибольшую важность имеют входные разности, в распределении вероятностей выходных текстов которых содержится большая неравномерность, т. е. наибольший разброс вероятностей. В работе [2] используются разности, вероятность перехода которых в заданную разность равна 1, которые могут быть исключены из рассмотрения при разностном анализе искусственной заменой существующего распределения вероятностей на аналогичное, в котором отсутствуют единичные вероятности при ненулевых разностях.

На основании полученного вероятностного распределения проведены экспериментальные исследования изменения разностей на протяжении шести раундов для двух вариантов входных разностей. В первом случае на вход подавались разности, которые с вероятностью $2^{-5}$ дают ту же разность, во втором — разности, имеющие наибольшую вероятность на выходе, т. е. $1{,}5 \cdot 2^{-4}$. Результаты экспериментов, проведенных для описанных вариантов входов, представлены в таблицах 1 и 2 соответственно. На вход в первом случае подавались четыре блока текстов с разностями, равными 14, а во втором случае — равными 11.

*Таблица 1. Изменение вероятностей при подаче на вход разности, сохраняющей свое значение*

| T0 | | | | T1 | | | | T2 | | | | T3 | | | | Вероятность | Номер раунда |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 14 | 0 | 0 | 0 | 14 | 0 | 0 | 0 | 14 | 0 | 0 | 0 | 14 | | |
| 0 | 0 | 0 | 0 | 0 | 14 | 0 | 0 | 0 | 0 | 0 | 14 | 0 | 0 | 14 | 0 | $2^{-5}$ | 1 |
| 0 | 0 | 0 | 0 | 0 | 7 | 14 | 0 | 0 | 0 | 7 | 7 | 0 | 14 | 0 | 0 | | |
| 0 | 0 | 0 | 0 | 0 | 7 | 14 | 0 | 0 | 0 | 7 | 7 | 0 | 14 | 0 | 0 | | |
| 0 | 7 | 9 | 7 | 0 | 4 | 135 | 0 | 0 | 0 | 0 | 0 | 7 | 14 | 0 | 0 | $2^{-17}$ | 2 |
| 0 | 7 | 9 | 7 | 7 | 10 | 135 | 0 | 13 | 134 | 0 | 14 | 14 | 0 | 0 | 7 | | |
| 0 | 7 | 9 | 7 | 7 | 10 | 135 | 0 | 13 | 134 | 0 | 14 | 14 | 0 | 0 | 7 | | |
| 10 | 140 | 135 | 14 | 138 | 132 | 67 | 141 | 0 | 7 | 9 | 7 | 10 | 135 | 0 | 7 | $2^{-47}$ | 3 |
| 10 | 140 | 135 | 14 | 128 | 3 | 67 | 138 | 11 | 71 | 115 | 247 | 135 | 0 | 7 | 10 | | |
| 10 | 140 | 135 | 14 | 128 | 3 | 67 | 138 | 11 | 71 | 115 | 247 | 135 | 0 | 7 | 10 | | |
| 139 | 68 | 48 | 125 | 13 | 134 | 213 | 55 | 10 | 140 | 135 | 14 | 3 | 67 | 138 | 128 | $1{,}125 \cdot 2^{-78}$ | 4 |
| 139 | 68 | 48 | 125 | 14 | 197 | 195 | 183 | 118 | 227 | 22 | 201 | 67 | 138 | 128 | 3 | | |
| 139 | 68 | 48 | 125 | 14 | 197 | 195 | 183 | 118 | 227 | 22 | 201 | 67 | 138 | 128 | 3 | | |
| 120 | 38 | 213 | 126 | 84 | 163 | 49 | 212 | 139 | 68 | 48 | 125 | 197 | 195 | 183 | 14 | $1{,}6875 \cdot 2^{-108}$ | 5 |
| 120 | 38 | 213 | 126 | 145 | 96 | 134 | 218 | 32 | 94 | 108 | 22 | 195 | 183 | 14 | 197 | | |
| 120 | 38 | 213 | 126 | 145 | 96 | 134 | 218 | 32 | 94 | 108 | 22 | 195 | 183 | 14 | 197 | | |
| 177 | 62 | 234 | 204 | 50 | 0 | 107 | 160 | 120 | 38 | 213 | 126 | 96 | 134 | 218 | 145 | $1{,}42 \cdot 2^{-139}$ | 6 |
| 177 | 62 | 234 | 204 | 82 | 134 | 177 | 49 | 242 | 203 | 90 | 56 | 134 | 218 | 145 | 96 | | |

*Таблица 2. Изменение вероятностей при подаче на вход разностей с наибольшей вероятностью*

| T0 | | | | T1 | | | | T2 | | | | T3 | | | | Вероятность | Номер раунда |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 11 | 0 | 0 | 0 | 11 | 0 | 0 | 0 | 11 | 0 | 0 | 0 | 11 | | |
| 0 | 0 | 0 | 0 | 0 | 64 | 0 | 0 | 0 | 0 | 0 | 11 | 0 | 0 | 11 | 0 | $1{,}5 \cdot 2^{-4}$ | 1 |
| 0 | 0 | 0 | 0 | 0 | 64 | 11 | 0 | 128 | 0 | 5 | 133 | 0 | 11 | 0 | 0 | | |
| 0 | 0 | 0 | 0 | 0 | 64 | 11 | 0 | 128 | 0 | 5 | 133 | 0 | 11 | 0 | 0 | | |
| 128 | 64 | 14 | 132 | 0 | 37 | 133 | 128 | 0 | 0 | 0 | 0 | 64 | 11 | 0 | 0 | $1{,}5 \cdot 2^{-13}$ | 2 |
| 128 | 64 | 14 | 132 | 64 | 46 | 133 | 128 | 7 | 14 | 0 | 0 | 11 | 0 | 0 | 64 | | |

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 128 | 64 | 14 | 132 | 64 | 46 | 133 | 128 | 7 | 14 | 0 | 0 | 11 | 0 | 0 | 64 | | |
| 71 | 32 | 133 | 128 | 34 | 153 | 66 | 224 | 128 | 64 | 14 | 132 | 46 | 133 | 128 | 64 | $1{,}5 \cdot 2^{-34}$ | 3 |
| 71 | 32 | 133 | 128 | 12 | 28 | 194 | 160 | 247 | 98 | 201 | 114 | 133 | 128 | 64 | 46 | | |
| 71 | 32 | 133 | 128 | 12 | 28 | 194 | 160 | 247 | 98 | 201 | 114 | 133 | 128 | 64 | 46 | | |
| 251 | 126 | 11 | 210 | 228 | 206 | 79 | 87 | 71 | 32 | 133 | 128 | 28 | 194 | 160 | 12 | $1{,}5 \cdot 2^{-63}$ | 4 |
| 251 | 126 | 11 | 210 | 248 | 12 | 239 | 91 | 34 | 97 | 194 | 113 | 194 | 160 | 12 | 28 | | |
| 251 | 126 | 11 | 210 | 248 | 12 | 239 | 91 | 34 | 97 | 194 | 113 | 194 | 160 | 12 | 28 | | |
| 218 | 109 | 45 | 42 | 177 | 86 | 227 | 212 | 251 | 126 | 11 | 210 | 12 | 239 | 91 | 248 | $1{,}25 \cdot 2^{-97}$ | 5 |
| 218 | 109 | 45 | 42 | 189 | 185 | 184 | 44 | 122 | 189 | 187 | 20 | 239 | 91 | 248 | 12 | | |
| 218 | 109 | 45 | 42 | 189 | 185 | 184 | 44 | 122 | 189 | 187 | 20 | 239 | 91 | 248 | 12 | | |
| 199 | 4 | 3 | 56 | 98 | 247 | 18 | 157 | 218 | 109 | 45 | 42 | 185 | 184 | 44 | 189 | $1{,}875 \cdot 2^{-133}$ | 6 |
| 199 | 4 | 3 | 56 | 219 | 79 | 62 | 206 | | | | | 184 | 44 | 189 | 185 | | |

Данные результаты получены для узла замены с суженным распределением вероятностей, тогда как в работе [2] рассматривается реальное распределение вероятностей, что позволяет построить атаку на все 10 раундов алгоритма TWIS. Проведенные эксперименты показали, что блочный алгоритм шифрования TWIS стоек к разностному анализу, так как уже к концу шестого раунда распределение выходных разностей становится равновероятным (вероятность перехода становится меньше $2^{-128}$). Таким образом, можно сделать вывод, что при использовании другого узла замены, реальное распределение вероятностей которого совпадает с суженным распределением, алгоритм TWIS будет стоек к разностному анализу при количестве раундов больше шести.

Для восстановления одного раундового ключа требуется опробовать пары входных открытых текстов с заданной разностью и отбросить ненужные тексты. Выходная разность напрямую зависит от входной, таким образом, для входной разности существует множество текстов, соответствующих определенным разностям. Если будем подавать открытые тексты на вход с заданной разностью, то по выходным разностям можно составить систему уравнений, решением которой и будет раундовый ключ.

Для оценки сложности атаки рассмотрим схему, в которой фиксируется конкретная пара текстов с заданной разностью и для этой разницы отбраковываются ключи, которые не будут отвечать выходной разности. Так как ключевое множество раундовых ключей имеет мощность $2^{32}$, результат испытания следует задать как двоичный вектор размерностью $2^{32}$, где 0 означает, что данный ключ отбракован, а 1, соответственно, что ключ подходит для данной пары текстов. При условии, что вероятность перехода равна $2^{-18}$, количество ненулевых значений в векторе будет равно $2^{32} \cdot 2^{-18} = 2^{14}$. Чтобы определить единственный ключ с заданной вероятностью, надо отбраковать $2^{14} - 1$ ключей.

Определим, с какой вероятностью отбраковывается ключ. Так как одна позиция фиксируется 0, таких наборов $\binom{2^{32}-1}{2^{14}-1}$, но в реальном наборе на одном определенном месте 1, поэтому вероятность отбраковки ключа равна

$$1-\frac{\binom{2^{32}-2}{2^{14}-2}}{\binom{2^{32}-1}{2^{14}-1}}=1-\frac{2^{14}-1}{2^{32}-1}.$$

Если имеется t текстов, то вероятность отбраковки ключа равна

$$1-\left(\frac{2^{14}-1}{2^{32}-1}\right)^{t},$$

а для отбраковки всех ключей кроме истинного необходимо рассчитать пересечение событий по всем ключам кроме одного. Поскольку ключ должен быть определен с заданной вероятностью δ,

$$\delta=\left(1-\left(\frac{2^{14}-1}{2^{32}-1}\right)^{t}\right)^{2^{14}-1}.$$

Отсюда получается, что искомая сложность равна

$$t=\log_{\frac{2^{14}-1}{2^{32}-1}}\left(1-\sqrt[2^{14}-1]{\delta}\right),$$

но это не точное число, а максимально возможное. Точное число не может быть определено, так как оно зависит от первой пары текстов и алгоритма выбора последующих.

Алгоритм нахождения одного раундового ключа при условии, что злоумышленнику известен алгоритм зашифрования и он может подавать на вход любые разности, имеет следующий вид:

1. Фиксируются входные разности $\Delta_1$ и $\Delta_2$, подаваемые на вход функции G, тогда на выходе получается $\Delta_2, S(\Delta_1 \oplus RKi) \oplus \Delta_2$.

2. Складываются по модулю два значения на выходе, получается $S(\Delta_1 \oplus RKi)$.

3. Если выходная разность равняется ожидаемой разности $\Delta_3$, то $RKi$ заносится в промежуточное множество.

4. Проверяется, является ли $RKi$ отбракованным ключом, при положительном исходе проверки $RKi$ удаляется из промежуточного множества.

5. Указанные действия повторяются до тех пор, пока в промежуточном множестве не останется один ключ.

Очевидно, что количество операций напрямую зависит от количества проверяемых текстов. При каждом опробовании выполняется 5 операций, которые для упрощения оценки будем считать однородными и элементарными, т. е. число операций для определения одного раундового ключа равно $5t$. Поскольку на каждом раунде узел замены применяется дважды, общее количество операций для 10 раундов равно

$$5(t_{11}+5(t_{12}+5(t_{21}+5(t_{22}+5(t_{31}+5(t_{32}+5(t_{41}+5(t_{51}+5t_{52}))))))))),$$

где $t_{ij}$ — количество операций на i-м раунде при j-м применении узла замены.

Если усреднить значение сложности, то получится приблизительно $2^{23} \cdot t$, где $t$ определено ранее. При $\delta = 0{,}9$ получаем $t \approx 0{,}96$ и сложность равна приблизительно $2^{23}$ элементарных операций, что меньше полного перебора.

Построим линейное приближение узла замены, единственного нелинейного примитива алгоритма TWIS. При составлении соотношения между входными и выходными битами узла замены необходимо помнить, что первые два бита входного текста не влияют на выходной текст, поэтому не будем их учитывать.

Для построения таблицы аффинных приближений узла замены необходимо выполнить следующие действия:

1. Перебрать все возможные двоичные векторы $a$ и $b$ длиной 6 и 8 соответственно, являющиеся линейными коэффициентами входной и выходной последовательностей.

2. Вычислить значение выражения

$$\left(\sum_{i=1}^{6}\oplus a_i X_i\right)\oplus\left(\sum_{j=1}^{8}\oplus b_j Y_j\right),$$

где $X_i$ — биты входной последовательности, $Y_j$ — биты входной последовательности, $a_i$ и $b_j$ — соответствующие координаты векторов a и b.

3. Подсчитать количество наборов $N(a,b)$, на которых указанное выражение равняется 1.

4. Определить значение величины $\varepsilon(a,b) = N(a,b) - 32$ и занести ее в ячейку таблицы с индексами $a,b$.

Полученные значения $\varepsilon(a,b)$, деленные на 64, являются отклонением вероятности для данного аффинного приближения от равновероятного. При помощи построенной диаграммы отклонений были выделены аффинные приближения с наибольшим отклонением и построена следующая система уравнений, являющаяся приближением узла замены:

$$\begin{cases} x_3 \oplus x_2 = y_0 \oplus y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_5, p = 0{,}765625 \\ x_0 \oplus x_1 \oplus x_2 = y_1 \oplus y_3 \oplus 1, p = 0{,}734375 \\ x_1 \oplus x_3 \oplus x_5 = y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6, p = 0{,}71875 \\ x_4 = y_0 \oplus y_2 \oplus y_3 \oplus y_7, p = 0{,}703125 \\ x_0 = y_0 \oplus y_1 \oplus y_2 \oplus y_3 \oplus y_4 \oplus y_6, p = 0{,}6875 \\ x_1 \oplus 1 = y_1 \oplus y_2 \oplus y_7, p = 0{,}671875 \end{cases}, \quad (*)$$

где $x_i$ — $i$-й бит входного текста, $y_j$ — $j$-й бит входного текста, $\rho$ — вероятность.

Решение системы (*) позволяет определить значение битов ключа с некоторой вероятностью, которая вычисляется по лемме о набегании знаков [3. Р. 79–89], согласно которой

$$\varepsilon_{i_1,i_2,\ldots,i_k} = 2^{k-1}\prod_{j=1}^{k}\varepsilon_{i_j},$$

где $\varepsilon_{i_j}$ — отклонение вероятности от 0,5 в $j$-м уравнении системы (*) на $i$-м раунде шифрования, $\varepsilon_{i_1, i_2, \ldots, i_k}$ — результирующее отклонение вероятности от 0,5 для системы (*). При подстановке полученных значений $\varepsilon_{i_1, i_2, \ldots, i_k} = 0{,}0029$. Таким образом, результирующее отклонение вероятности отличается от равновероятного. Однако уже на втором раунде результирующее отклонение вероятности стремится к нулю, что позволяет утверждать о стойкости алгоритма TWIS к линейному анализу. Рассматривать нахождение отдельных битов раундового ключа не имеет смысла, так как уже на втором раунде не будет хватать известных значений для решения системы уравнений, аналогичной системе (*). Также следует отметить, что сложность полного перебора снижена из-за того, что только 6 бит ключа влияют на выходную последовательность узла замены.

В результате проведенной работы были получены распределение вероятностей и линейная аппроксимация узла замены блочного алгоритма шифрования TWIS. Также была выявлена связь между вероятностью определения истинного ключа и количеством опробуемых для вычисления истинного ключа текстов, оценена сложность указанной атаки, которая оказалась меньше сложности полного перебора.

## СПИСОК ЛИТЕРАТУРЫ:

1. *Shrikant Ojha, Naveen Kumar, Kritika Jain, Sangeeta Lal*. TWIS – A Lightweight Block Cipher // Lecture Notes in Computer Science. Vol. 5905/2009. 2009. P. 280–291.

2. *Onur Kocak, Nese Oztop*. Cryptanalysis of TWIS Block Cipher // Symmetric Key Encryption Workshop. 2011. URL: http://skew2011.mat.dtu.dk/proceedings/Cryptanalysis%20of%20TWIS%20Block%20Cipher.pdf (дата обращения: 18.10.2012).

3. *Douglas R. Stinson*. Cryptography "Theory and Practice". Chapman&Hall/CRC Taylor&Francis Group, 2006.