

## **АНАЛИЗ КРИПТОСТОЙКОСТИ ШИФРА ТОРНАДО**

Одной из первоочередных задач в области информационных технологий для Украины является создание блочного симметричного шифра (БСШ), отвечающего современным требованиям. В этом журнале представлено описание нового БСШ Торнадо. Основной целью настоящей статьи является анализ стойкости этого шифра к известным криптоаналитическим атакам.

При рассмотрении стойкости шифра к различным атакам будем пользоваться понятием ослабленного шифра Торнадо. Под ослабленным вариантом шифра Торнадо будем понимать алгоритм, который получен исключением из оригинального варианта преобразований  $IT$ ,  $FT$  и  $CP_{bit}$ , а объединение полублоков с выходом  $F$ -функции происходит с использованием сложения по модулю 2 вместо сложения / вычитания по модулю  $2^{64}$ . В этом случае  $F$ -функция алгоритма имеет Rijndael-подобную структуру. Формат многих операций шифра Торнадо – 64 бита, поэтому для удобства 64-битные слова, из которых состоит полублок шифра Торнадо, будем называть колонками по аналогии с 32-битными колонками в шифре Rijndael [1].

### **1 Атаки грубой силы**

Большинство атак грубой силы применимы к любому блочному шифру, и сложность конкретной атаки зависит только от длины блока  $n$  или длины ключа  $k$ , независимо от структуры алгоритма.

Атака полного перебора ключей является самым простым способом поиска ключа шифрования. Сложность такой атаки зависит от длины ключа и составляет, как известно, не менее  $2^{k-1}$  шифрований с помощью исследуемого шифра. Для обеспечения защищенности от этой атаки в шифрах используют ключи большого размера. Поскольку минимальная длина ключа шифра Торнадо составляет 256 бит, исчерпывающий поиск ключа требует  $2^{255}$  шифрований и на практике неосуществим.

К словарной атаке уязвимы шифры, обладающие недостаточной длиной блока. Для выполнения атаки требуется таблица размером  $2^n$  блоков, а для построения такой таблицы необходимо  $2^n$  шифрований. Минимальная длина блока Торнадо – 128 бит, следовательно, словарная атака на практике неосуществима.

Далее будем говорить, что алгоритм защищен от некоторой криптоаналитической атаки, если ее реализация превышает или равна сложности атаки грубой силы

### **2 Дифференциальный и линейный криптоанализ**

Наиболее известными и мощными методами выполнения атак на БСШ являются предложенные в начале 90-х дифференциальный криптоанализ [2, 3] и линейный криптоанализ [4]. Известны четыре критерия оценки стойкости алгоритма к этим криптоатакам [5]:

- точный критерий – максимум вероятностей выполнения дифференциалов и шаблонов линейной аппроксимации;
- теоретический критерий – верхние границы вероятностей выполнения дифференциалов и шаблонов линейной аппроксимации;
- эвристический критерий – максимальные вероятности дифференциальной и линейной характеристик;
- практический критерий – верхние границы вероятностей дифференциальных и линейных характеристик.

В соответствии с практическим критерием [5], шифр считается стойким к соответствующей атаке (дифференциального либо линейного криптоанализа) если

справедливо неравенство

$$P_{\text{upb}}^{(r)} \leq 2^{-n}, \quad (1)$$

где  $r$  – число циклов шифра,  $n$  – размер блока в битах,  $P_{\text{upb}}^{(r)}$  – верхняя граница вероятности  $r$ -циклового дифференциальной или линейной характеристики.

Рассмотрим ослабленные варианты шифра Торнадо.

Поскольку цикловая функция шифра биективна, то в соответствии с [5]

$$P_{\text{upb}}^{(r)} = \begin{cases} \left(P_{\text{max}}^{(1)}\right)^{2t}, & \text{если } r = 3t \text{ или } r = 3t + 1, \\ \left(P_{\text{max}}^{(1)}\right)^{2t+1}, & \text{если } r = 3t + 2, \end{cases} \quad (2)$$

где  $P_{\text{max}}^{(1)}$  – максимальная вероятность отличной от нуля дифференциальной или линейной характеристики цикловой функции. Для вычисления верхней границы этого значения необходимо определить минимально возможное число активных S-блоков в активной цикловой функции.

Активная цикловая функция ослабленного шифра Торнадо содержит не менее 9 активных S-блоков. Справедливость этого утверждения следует из свойства MDS-преобразования, в соответствии с которым число ветвей активизации равно 9. Следовательно

$$P_{\text{max}}^{(1)} = (p_s)^9 = \left(2^{-6}\right)^9 = 2^{-54}, \quad (3)$$

где  $p_s = 2^{-6}$  – максимальная вероятность отличной от нуля линейной/дифференциальной характеристики отдельного S-блока шифра Торнадо.

Используя формулы (2) и (3) были рассчитаны верхние границы вероятностей дифференциальных/линейных характеристик  $P_{\text{upb}}^{(r)}$  для ослабленных вариантов шифра Торнадо и для различного числа итераций цепи Фейстеля  $r$ . Результаты представлены в табл. 1 (в скобках указано минимальное число активных S-блоков  $a$ , соответствующее дифференциальной/линейной характеристике).

Таблица 1

$r$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$P_{\text{upb}}^{(r)}$	1	$2^{-54}$	$2^{-108}$	$2^{-108}$	$2^{-162}$	$2^{-216}$	$2^{-216}$	$2^{-270}$	$2^{-324}$	$2^{-324}$	$2^{-378}$	$2^{-432}$	$2^{-432}$	$2^{-486}$	$2^{-540}$
$a$	(0)	(9)	(18)	(18)	(27)	(36)	(36)	(45)	(54)	(54)	(63)	(72)	(72)	(81)	(90)

Учитывая возможность применения NR-атаки [2], в ходе которой может быть отброшено до двух итераций цепи Фейстеля, неравенство (1) следует записать как:

$$P_{\text{upb}}^{(r-2)} \leq 2^{-n}. \quad (4)$$

Как видно из результатов, представленных в табл. 1, для ослабленных вариантов шифра даже без IT- и FT-преобразований выполняется неравенство (4), а значит ослабленные Торнадо-128, Торнадо-256 и Торнадо-512 являются практически стойкими к дифференциальному и линейному криптоанализу. Использование полного набора преобразований в этих шифрах увеличит их стойкость.

### 3 Атака усеченных дифференциалов

Одна из разновидностей дифференциальных атак была предложена в середине 90-х годов Л. Кнудсенем [6]. В своей работе он показал, что для организации атаки иногда эффективнее предсказывать не полную разность, а лишь некоторую ее часть. Такая методика получила название криптоанализ усеченных дифференциалов. Считается, что для байт-ориентированных шифров естественным является изучение усеченных дифференциалов особого вида, для которых усечение заключается не в исключении из рассмотрения отдельных битов входной или выходной разности, а в рассмотрении факта активности S-блоков. Поскольку используемые в современных шифрах S-блоки чаще всего задают закон

отображения байт в байт, то дифференциалы, рассматривающие активность S-блоков, часто называют байтовыми дифференциалами. В таких дифференциалах вместо разности рассматривается прохождение через преобразования шифра двоичных векторов, каждый бит которых отражает активность одного S-блока (1 – ненулевая разность – S-блок активный; 0 – S-блок пассивный). Двоичный вектор, описывающий активность всех байтов блока (полублока) будем называть вектором активизации. В литературе существует описание атак усеченных (байтовых) дифференциалов на ослабленные варианты байт-ориентированных шифров SAFER и E2 [7, 8]. В дальнейшем под усеченными будем понимать байтовые дифференциалы.

Существует мнение, что рассмотрение усеченных (байтовых) дифференциалов для байт-ориентированных шифров позволяет получить более точную оценку стойкости к дифференциальному криптоанализу, чем при стандартном подходе, т.е. при рассмотрении дифференциальных характеристик [9, 10]. Рассмотрим стойкость к атаке усеченных дифференциалов ослабленных вариантов шифра.

Оценка стойкости БСШ к атаке усеченных дифференциалов выполняется путем поиска байтовых дифференциалов, покрывающих достаточное для построения атаки число циклов и обладающих достаточно высокой вероятностью. Известные методы выполнения такого поиска [10, 11] были предложены для 128-битных шифров и не могут быть применены в явном виде для оценки стойкости фейстель-подобных шифров с размером блока 256 и более битов. Для того, чтобы произвести поиск байтовых дифференциальных характеристик для всех вариантов шифра Торнадо был предложен метод, который позволяет значительно сократить вычислительные затраты на реализацию такого поиска для фейстель-подобных шифров с rijndael-подобной шифрующей функцией по сравнению с методом из [11]. В основе этого подхода лежит идея сокращения числа рассматриваемых на каждой итерации выходных векторов активизации.

Изложим коротко основную идею предлагаемого метода. Как было выяснено, среди всех векторов активизации с одинаковой комбинацией активных колонок (активная колонка содержит хотя бы один активный байт) на выходе одного цикла наиболее перспективным является тот, который содержит максимальное число активных байтов в каждой из активных колонок. Исключая из рассмотрения остальные возможные выходные вектора активизации, число рассматриваемых вариантов на каждом цикле не будет превосходить число комбинаций активных колонок  $N_{комб}$ , которое может вычислено по следующей формуле

$$N_{комб} = \sum_{i=1}^{n_c-1} C_{n_c}^i,$$

где  $C_{n_c}^i$  - число сочетаний из  $i$  по  $n_c$ ,  $n_c$  – число колонок в полублоке. Значение  $N_{комб}$  зависит от числа колонок и обычно не превосходит нескольких десятков, и, следовательно, становится возможным тестирование шифров с большим размером блока. Более подробно предлагаемый метод планируется рассмотреть в одной из следующих статей.

Поиск дифференциальных байтовых характеристик, на основе которых возможна эффективная атака усеченных дифференциалов на ослабленный вариант Торнадо-128, был проведен с использованием известного [11] и предлагаемого методов. В обоих случаях одинаковым было максимальное число циклов, для которого были найдены эффективные байтовые характеристики. Применение метода из [11] позволило найти гораздо больше эффективных характеристик. В то же время, лучшие по вероятностным показателям, а значит, и наиболее эффективные байтовые характеристики были найдены в обоих случаях, что свидетельствует о работоспособности предлагаемого метода для фейстель-подобных шифров с "rijndael-подобной" шифрующей функцией.

Предлагаемый метод позволил также протестировать ослабленные варианты шифра Торнадо с размером блока 256 и 512 битов. Полученные результаты сведены в табл. 2.

Таблица 2

	Размер блока, байты (биты)	Макс. число полуциклов	Вер. усеч. дифф. хар., $P_{усд}$	Вер. обычн. диффер., $P_{диф}$
Торнадо-128	16 (128)	2	1	$2^{-72}$
Торнадо-256	32 (256)	4	$2^{-32.11}$	$2^{-232.11}$
Торнадо-512	64 (512)	6	$2^{-176.42}$	$2^{-496.42}$

В таблице приведены также вероятности обычных дифференциалов, вычисленные в соответствии с представленными в работе [10] соотношениями между вероятностями обычных  $P_{диф}$  и усеченных дифференциалов  $P_{усд}$ :

$$P_{диф}^{(i)}(a, b) = p^{h(c(b))} P_{усд}^{(i)}(c(a), c(b)),$$

где  $h(f)$  – вес Хемминга аргумента  $f$ ;  $c$  – функция-характеристика, которая преобразует разность в вектор активизации, т.е. ставит 1 на месте активных  $S$ -блоков в аргументе и 0 – в противном случае;  $p = \frac{1}{255}$  – вероятность получения на выходе активного  $S$ -блока

определенного значения разности;  $a$  и  $b$  есть, соответственно, входная и выходная разности.

Исходя из полученных результатов и учитывая возможность использования NR-атаки [2], в ходе которой может быть отброшено до двух итераций цепи Фейстеля, можно заключить, что ослабленные варианты шифров Торнадо-128 с 5 и более полуциклами, Торнадо-256 с 7 и более полуциклами и Торнадо-512 с 9 и более полуциклами являются стойкими к дифференциальной атаке и атаке усеченных дифференциалов.

Версии шифра Торнадо с полным набором операций будут обладать, в первую очередь за счет использования начальных и конечных преобразований, более хорошими показателями стойкости к рассматриваемому виду атак.

#### 4 Атака невозможных дифференциалов

Впервые техника выполнения данного вида дифференциальных атак была предложена для ослабленных вариантов шифров Skipjack [12], IDEA [13]. Данная атака строится на использовании дифференциалов специального вида – тех, которые не могут выполняться, то есть имеющих нулевую вероятность.

Методика атаки заключается в следующем: на некотором цикле (обычно первом или последнем) делается предположение о примененном подключе или о его части (выполняется перебор цикловых ключей), а на остальных циклах предполагается выполнение “невозможного” дифференциала. Если на проверяемом цикловом ключе-кандидате возможно получение разностей определенных “невозможным” дифференциалом, то этот ключ отбрасывается как ошибочный. В результате такого перебора остается ограниченное множество цикловых ключей-кандидатов.

В работе [13] показано, что если в фейстель-подобном шифре используется биективная шифрующая функция, то всегда существует 5-цикловый невозможный дифференциал, который имеет вид  $(a, 0) \rightarrow (a, 0)$  для любой ненулевой разности  $a$ . В силу того, что шифр Торнадо построен с использованием цепи Фейстеля, а шифрующая функция биективна, то существует 2,5-цикловый (5 итераций цепи Фейстеля) невозможный дифференциал. Невозможных дифференциалов, покрывающих большее число циклов, найдено не было. В подтверждение их отсутствия может служить и тот факт, что не было найдено дифференциалов с вероятностью 1 для более, чем 1 цикла шифра, а невозможный дифференциал, основываясь на материалах работы [13], обычно получается путем “стыковки” двух дифференциалов с вероятностями 1.

Возможно, с помощью 2,5-циклового невозможного дифференциала может быть организована атака на шифр с 6-ю итерациями цепи Фейстеля без начальных и конечных преобразований. Варианты шифра Торнадо с начальными и конечными преобразованиями и со стандартным числом циклов будут неуязвимы для атаки невозможных дифференциалов.

## 5 Бумеранг-атака

Впервые бумеранг-атака была представлена в работе [14]. Эта атака во многом схожа с дифференциальным криптоанализом, так как использует дифференциалы. В отличие от дифференциального криптоанализа, где используется один дифференциал, покрывающий почти все циклы шифра, для организации бумеранг-атаки требуется два "более коротких" дифференциала, которые вместе покрывают все циклы шифра и обладающие высокими вероятностями  $p_1$  и  $p_2$ . При этом, условие эффективности бумеранг-атаки может быть записано как [14, 15]

$$p_1 \times p_2 \geq 2^{-n/2}, \quad (5)$$

где  $n$  – длина блока в битах.

Легко убедиться, что среди найденных в пунктах 1 и 2 дифференциалов и дифференциальных характеристик (табл. 1, табл. 2) нет таких, которые бы покрывали все циклы шифра и удовлетворяли неравенству (5). Поэтому есть основания считать все варианты шифра Торнадо стойкими к этой атаке.

## 6 Интерполяционная атака и атака линейных сумм

Атака предложена Якобсеном и Кнудсеном [16]. Для проведения этой атаки криптоаналитик выполняет построение полиномов на основе известных пар "открытый–шифрованный текст". Эта атака эффективна против шифров, позволяющих описать процедуру шифрования некоторым сравнительно простым алгебраическим выражением. Принцип интерполяционной атаки состоит в том, что если шифртекст может быть представлен как полином (или рациональное выражение) от открытого текста в котором количество неизвестных (ключезависимых) коэффициентов равно  $N$ , то этот полином (или рациональное выражение) может быть восстановлен с использованием  $N$  пар "открытый–шифрованный текст", полученных на искомом ключе  $K$ . Для восстановления неизвестных коэффициентов обычно используется какая-либо интерполяционная формула. Выражение, определяемое полученным полином, будет эквивалентно зашифрованию на искомом ключе. Для защиты от этой атаки необходимо максимизировать величину  $N$ .

В работе [17] предложен алгоритм, позволяющий оценить стойкость шифра к атаке линейных сумм и интерполяционной атаке. На практике этот алгоритм реализуем для случая, когда строящийся полином связывает значения одного байта открытого текста с одним байтом шифртекста. В этом случае строящийся полином имеет вид

$$f_k(x) = \sum_{i=1}^{2^8} a_i(k)b_i(x),$$

где  $x \in GF(2^8)$  – байт открытого текста,  $a_i(k) \in GF(2^8)$  – ключезависимые коэффициенты,  $\{b_i(x)\}$  – множество линейно независимых полиномов с коэффициентами из  $GF(2^8)$  (атака линейных сумм эквивалентна интерполяционной атаке, когда  $b_i(x) = x^{i-1}$ ).

Атака линейных сумм эффективна, когда число неизвестных ключезависимых коэффициентов  $a_i(k)$  меньше, чем  $2^8$ . В соответствии с предложенным в [17] алгоритмом был произведен поиск соотношений над  $GF(2^8)$  между каждым байтом открытого текста и каждым байтом криптограммы. Результаты тестирования шифра Торнадо представлены в табл. 3.

Таблица 3

Число циклов	Торнадо	Торнадо без ИТ- и ФТ-преобразований
0	1	–
1	256	1
1,5	256	255
$\geq 2$	256	256

Представленные в табл.3 данные свидетельствуют о стойкости шифра Торнадо без ИТ- и ФТ-преобразований с 5 и более итерациями цепи Фейстеля к интерполяционной атаке и атаке

линейных сумм. Из таблицы также видно, что использование ИТ- и ФТ-преобразований увеличивает стойкость шифра к этим видам атак.

В соответствии с [17, Теорема 3] шифр, стойкий к атаке линейных сумм, является также стойким к атаке высших дифференциалов и Square-атаке. Поэтому есть основания считать Торнадо стойким и к этим видам атак.

### **7 Атака дифференциалов высших порядков**

Данная атака применима к шифрам представимым в виде булевого полинома малой степени. Применение такой атаки к БСШ было продемонстрировано Кнудсенем [6, 16]. Необходимый для проведения криптоанализа порядок дифференциала определяют по степени булевых полиномов, определяющих значения битов криптограммы как функцию от битов открытого текста. Так если биты выхода  $(r-1)$ -го цикла могут быть выражены через биты открытого текста в виде полиномов степени не выше  $d$ , то порядок дифференциала высшего порядка будет  $d+1$ , так как любой дифференциал  $(d+1)$ -го порядка становится равным 0 [6]. Если обозначить через  $b$  длину используемого на последнем цикле ключа, то существует дифференциальная атака порядка  $d+1$ , со сложностью по времени  $2^{b+d}$ , требующая  $2^{d+1}$  подобранных открытых текстов и соответствующих им криптограмм, которая позволит получить ключ последнего цикла [16, Теорема 1].

Для того, чтобы оценить стойкость шифра к атаке высших дифференциалов следует найти порядок полиномов, связывающих биты на выходе предпоследнего цикла с битами открытого текста. В шифре Торнадо единственный нелинейный элемент – это S-подстановки. Порядок полиномов, отражающих значения битов на выходе S-подстановки как функции от битов на входе, максимален для подстановки 8 в 8 битов и равен 7. Каждая следующая S-подстановка существенно увеличивает порядок булевых полиномов. Например, после четырех уровней S-подстановок порядок булевых полиномов будет  $7^4 = 2401$ . Поскольку 2401 больше, чем 128, 256 и 512, то ожидается, что все варианты шифра будут стойкими к атаке высших дифференциалов. Подтверждением этому могут служить и результаты, полученные в пункте 6.

### **8 Интегральный криптоанализ**

Данная атака первоначально была предложена под названием square для одноименного шифра [18], который имеет байт-ориентированную структуру. Этой атаке подвержены и другие шифры, имеющие “слово”-ориентированную структуру, т.е. состоящие из последовательности линейных и нелинейных преобразований над выровненными битовыми кортежами фиксированной длины [1, 19]. В интегральной атаке используется множество подобранных открытых текстов. В результате суммирования (интегрирования) принадлежащих множеству текстов в битовых кортежах фиксированной длины получают определенные значения. Если возможно с высокой вероятностью предсказать значение суммы в одном или нескольких битовых кортежах после  $r$  циклов шифра, то может быть организована атака на  $(r+1)$ -цикловый шифр. В ходе атаки перебираются возможные подключения последнего цикла и для каждого варианта производится дешифрование одного цикла для всего множества имеющихся криптограмм. Если в результате суммирования информационных блоков, полученных при одноцикловом дешифровании, в определенном битовом кортеже будет получено нужное значение, то с высокой вероятностью проверяемый подключ последнего цикла верный. Более подробно методика интегрального криптоанализа описана в работах [1, 19].

Преобразования шифра Торнадо, за исключением битовой перестановки  $CP_{bit}$ , являются байт-ориентированными и во многом похожи на преобразования, используемые в шифрах Square, Rijndael, поэтому важно исследовать возможность организации интегральной атаки на Торнадо. Особенности прохождения интегралов через большинство преобразований рассматриваемого шифра известны из работ [1, 18, 19]. Рассмотрим прохождение различных интегралов через битовую перестановку. Для этого будем использовать введенные в работе [19] обозначения. Символ 'C' на определенной позиции говорит о том, что значения слов на

этой позиции во всех рассматриваемых текстах равны. Символ 'A' означает, что все слова на этой позиции в коллекции рассматриваемых текстов различны. 'S' обозначает то, что сумма всех слов на этой позиции в коллекции рассматриваемых текстов имеет определенное значение. '?' – значение суммы неизвестно.

Операция  $CP_{bit}$  преобразует 64-битные блоки так, что каждый байт после преобразования содержит по одному биту из каждого байта до преобразования. Поэтому если побитовая сумма по модулю 2 во всех 64 битах равна 0, то такой же она и останется после преобразования. Естественно, если в каждом из восьми байтов в множестве рассматриваемых текстов находятся одинаковые значения, т. е. каждый из 8-ми байтов обозначается символом 'C', то одинаковыми они останутся и после перестановки. Однако, если перед перестановкой наряду с 'C'-байтами имеется один или несколько байтов со значениями 'A' или 'S', то на выходе будут получены значения 'S' на всех восьми позициях. С учетом особенностей используемых в шифре Торнадо преобразований, могут быть построены интегралы, покрывающие 3-итерации цепи Фейстеля для вариантов шифра с различным размером блока (рис. 1).

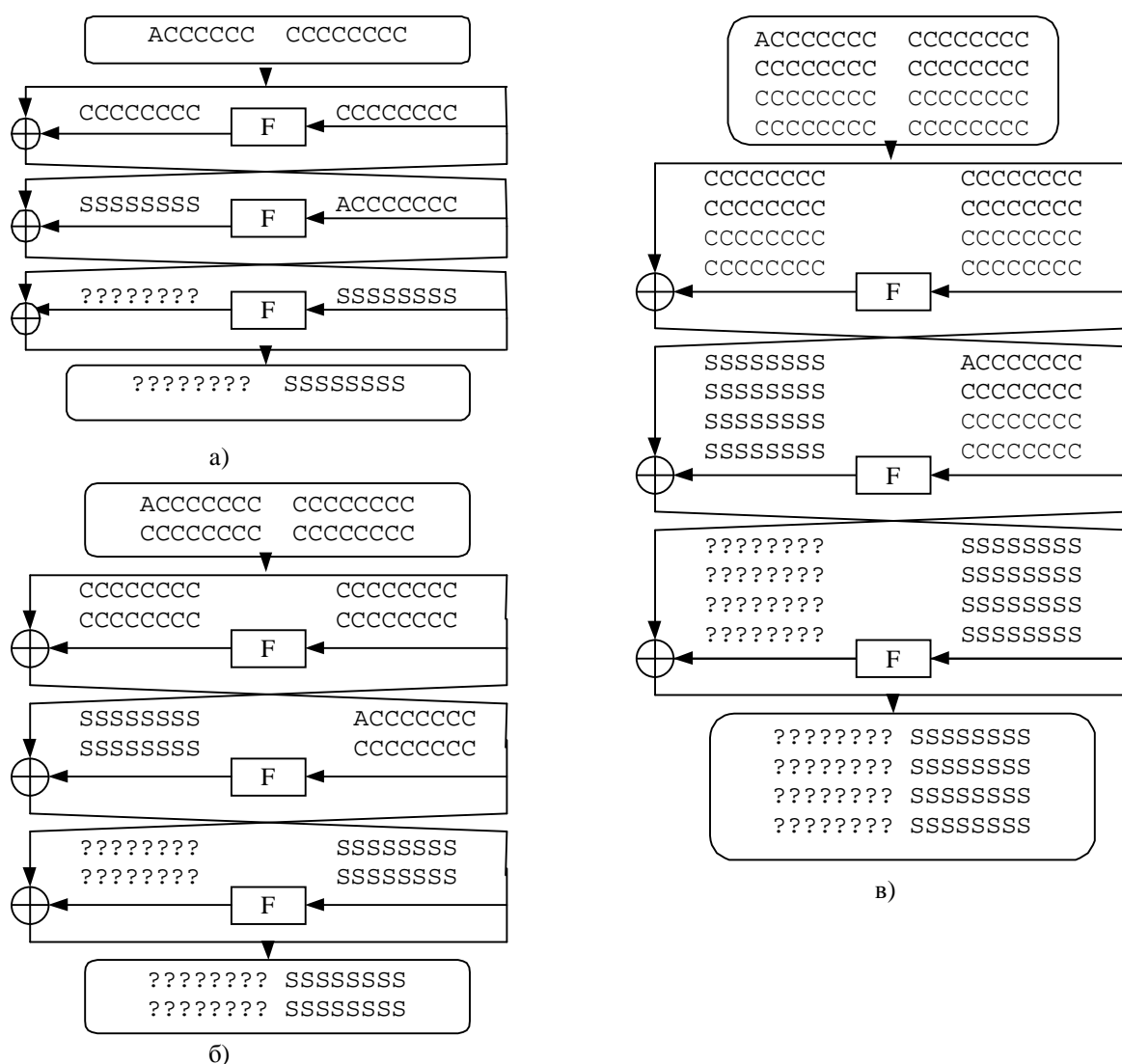


Рис. 1

С помощью представленных интегралов, вероятно, может быть организована эффективная атака на ослабленные варианты шифра Торнадо, содержащие 4 полуцикла (2 цикла). Шифры Торнадо-128, Торнадо-256 и Торнадо-512 со стандартным числом циклов являются стойкими к интегральному криптоанализу, что подтверждается и результатами, полученными в пункте 6.

**Список литературы:** 1. *J. Daemen, V. Rijmen*. AES Proposal Rijndael, AES Round 1 Technical Evaluation CD-1: Documentation, National Institute of Standards and Technology, Aug 1998. See <http://www.nist.gov/aes>. 2. *E. Biham, A. Shamir*. Differential Cryptanalysis of DES-like Cryptosystem, *Journal of Cryptology*. Vol. 4. P. 3-72. 1991. 3. *E. Biham, A. Shamir*. Differential Cryptanalysis of the full 16-round DES. Technical Report - Computer Science Department, Technion, Israel, 1993. 4. *M. Matsui*. Linear Cryptanalysis Method for DES Cipher, EUROCRYPT'93, pp. W112-W123, May 1993. 5. "Supporting Document on E2", Nippon Telegraph and Telephone Corporation, June 14, 1998. 6. *L. R. Knudsen*. Truncated and Higher Order Differentials. In B. Preneel, editor, *Fast Software Encryption — Second International Workshop*, Volume 1008 of *Lecture Notes in Computer Science*, pp. 196–211. Springer-Verlag, Berlin, Heidelberg, New York, 1995. 7. *L. R. Knudsen, T. A. Berson*. Truncated differentials of SAFER, <http://www.iu.uib.no/~larsr/>. 8. *M. Matsui, T. Tokita*. Cryptanalysis of reduced version of the block cipher E2, in proceedings of *Fast Software Encryption'99*, pp. 70-79, 1999. 9. *K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita*. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms, *Selected Areas in Cryptography – 7<sup>th</sup> Annual International Workshop, SAC2000, Lecture Notes in Computer Science* 2012, pp. 39-56, Springer-Verlag, Berlin, 2001. 10. *M. Sugita, K. Kobara*. Relationships among differential, truncated differential, impossible differential cryptanalyses against word-oriented block cipher like Rijndael, E2 // National Institute of Standards and Technology, <http://www.nist.gov/aes>. 11. *S. Moriai*. Security of E2 against truncated differential cryptanalysis, <http://www.nist.gov/aes>. 12. *E. Biham, A. Biryukov, A. Shamir*. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials, proceedings of EUROCRYPT'99, *lecture notes in computer science* 1592, pp. 12-23, 1999. 13. *E. Biham, A. Biryukov, A. Shamir*. Miss in the Middle Attacks on Idea and Khufu, proceedings of FSE'99, *lecture notes in computer science* 1636, pp. 124-138, 1999. 14. *D. Wagner*. The Boomerang Attack. In *L. R. Knudsen*, editor, *Fast Software Encryption — 6th International Workshop, FSE'99, Volume 1636 of Lecture Notes in Computer Science*, pp. 156–170, Berlin, Heidelberg, New York, 1999. 15. *E. Biham, O. Dunkelman, N. Keller*. New Results on Boomerang and Rectangle Attacks, available from <http://eprint.iacr.org/2001/070.ps>. 16. *T. Jakobsen, L. R. Knudsen*. The Interpolation Attack on Block Cipher. In *E. Biham*, editor, *Fast Software Encryption — 4th International Workshop, FSE'97, Volume 1267 of Lecture Notes in Computer Science*, pp. 28–40, Berlin, Heidelberg, New York, 1997. Springer-Verlag. 17. *K. Aoki*. Practical Evaluation of Security against Generalized Interpolation Attack. *IEICE Transactions Fundamentals of Electronics, Communications and Computer Sciences (Japan)*, Vol. E83-A, No. 1, pp. 33–38, 2000. (A preliminary version was presented at SAC'99). 18. *J. Daemen, L.R. Knudsen, V. Rijmen*. The block cipher Square, *Fast Software Encryption, LNCS 1267*, *E. Biham, Ed.*, Springer-Verlag, 1997, pp. 149–165. 19. *L. R. Knudsen*. Integral Cryptanalysis, NESSIE internal report NES/DOC/UIB/WP5/015/1, 2001.