УДК 621.3.06

М.Ю. РОДІНКО

ОЦІНКА СТІЙКОСТІ СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУ «КИПАРИС» ДО ДИФЕРЕНЦІЙНОГО КРИПТОАНАЛІЗУ

Вступ

В останні роки все більшого розвитку набуває малоресурсна криптографія, метою якої є створення симетричних примітивів (блокових та потокових шифрів, функцій гешування) для застосування у нересурсоємних пристроях. Висока зацікавленість у розробці таких примітивів спостерігається і з боку Національного Інституту Стандартів і Технологій США, який у 2018 році оголосив про конкурс з розробки малоресурсних алгоритмів для застосування у простих електронних пристроях [1].

Відповідно до світових тенденцій в Україні розроблений перспективний малоресурсний симетричний блоковий шифр «Кипарис» [2]. Метою розробки малоресурсного алгоритму було забезпечення високої швидкодії перетворень зі збереженням високого рівня криптографічної стійкості, прийнятної для застосування шифру у постквантовий період. Блоковий шифр «Кипарис» оперує 256- та 512-бітовими блоками даних із використанням ключа шифрування аналогічної довжини.

У попередніх роботах [2, 3] були представлені результати досліджень лавинних та статистичних показників блокового шифру «Кипарис», його швидкісних характеристик, а також результати щодо оцінки диференційних властивостей алгоритму. Оскільки, диференційний криптоаналіз (ДК) [4] є найбільш розповсюдженим серед відомих методів криптоаналізу симетричних блокових шифрів, обґрунтування стійкості до ДК є невід'ємною частиною оцінки будь-якого блокового шифру.

В основі блокового шифру «Кипарис» лежить ARX-перетворення (складається з операцій додавання за модулем, циклічного зсуву та побітового додавання), яке знайшло широке застосування у малоресурсних алгоритмах (ChaCha [5], SPECK [6], TEA [7] і т.д.). Однак, не дивлячись на простоту застосовуваних операцій, розробники ARX-шифрів стикаються з проблемами при оцінці верхньої границі диференційної ймовірності шифру через відсутність загального теоретичного підходу до оцінки стійкості ARX-шифрів до ДК. У роботі [3] запропоновані евристичні методи пошуку найбільш ймовірних одноциклових диференційних характеристик блокового шифру «Кипарис», за допомогою яких знайдено одноциклові характеристики з ймовірністю 1/4 та 1/8.

Метою роботи є оцінка практичної стійкості блокового шифру «Кипарис» до диференційного криптоаналізу, що визначається ймовірністю кращої знайденої диференційної характеристики. Для досягнення цієї мети у роботі пропонуються методи пошуку багатоциклових диференційних характеристик для блокового шифру «Кипарис».

1. Диференційний криптоаналіз блокових шифрів

В основі диференційного криптоаналізу [4] блокових шифрів лежить аналіз проходження різниці між двома відкритими текстами крізь цикли шифрування та оцінка ймовірності перетворення вхідної різниці a у вихідну різницю b. Максимальне значення диференційної ймовірності визначається як [8, 9]

$$\mathrm{MEDP}(a,b) = \max_{a\neq 0,b} \mathrm{EDP}(a,b), \tag{1}$$

де $\mathrm{EDP}(a,b)$ – середня за ключами ймовірність диференціалу.

Значення MEDP(a,b) називається теоретичною стійкістю блокового шифру до диференційного криптоаналізу [10]. Однак, як правило, при аналізі блокових шифрів, користуються

оцінкою практичної стійкості [10], яка визначається верхньою границею ймовірності диференційної характеристики, або

$$\mathrm{MEDP}(\Omega) = \max_{\Omega \in (a,b)} \mathrm{EDP}(\Omega(a,b)). \tag{2}$$

де $\mathrm{EDP}(\Omega(a,b))$ – середня за ключами ймовірність диференційної характеристики.

Як правило, сучасні ітеративні блокові шифри є марковськими. Для марковського шифру ймовірність багатоциклової характеристики може бути апроксимована добутком ймовірностей одноциклових характеристик [8].

Нехай задано ітеративний блоковий шифр $E_k^{(r)}(x)$ з розміром ключа κ, що складається з r ітерацій циклової функції $f(x)$. Для успішної атаки на блоковий шифр необхідно знайти $(r-1)$ -циклову диференційну характеристику з ймовірністю [8]

$$P(E_k^{(r-1)}(x) + E_k^{(r-1)}(x+a) = b) = p >> 2^{-n}. \tag{3}$$

Для традиційних блокових шифрів, що базуються на S-блоках, максимальна ймовірність ДХ для одного циклу перетворення визначається максимумом таблиці розподілу різниць S-блока та мінімальною кількістю гілок активізації лінійного перетворення [9]. Подібний підхід є застосовуваним до шифрів, побудованих згідно зі стратегією широкого сліду, таких як AES, Калина, Camellia та ін., завдяки тому, що нелінійна та лінійна складові цих алгоритмів побудовані із застосуванням прозорого математичного апарату, а значить мають теоретично обґрунтовані криптографічні властивості [11].

2. Оцінка стійкості ARX-шифрів до диференційного криптоаналізу

У якості нелінійної операції в ARX-шифрах виступає додавання n-бітових слів за модулем 2^n, а циклові ключі, як правило, вводяться за допомогою операції XOR, тому, диференційна ймовірність шифру визначається ймовірностями перетворення різниць (обчислених за допомогою операції XOR) на модульних суматорах [12]. Розмір модуля є достатньо великим у порівнянні з розмірністю S-блоків (як правило, 32-64 біти), що з точки зору обчислювальної складності унеможливлює побудування повної таблиці розподілу різниць.

Визначення мінімальної кількості гілок активізації також є складною задачею, оскільки перемежування простих (нелінійних та лінійних) операцій, що не підпорядковується чіткому математичному обґрунтуванню, є складним з точки зору аналізу його криптографічних властивостей.

Часто один цикл перетворення ARX-шифру містить декілька нелінійних та лінійних операцій, що чергуються між собою, при цьому ключове забілювання застосовується лише на початку кожного циклу. Згідно з класичною теорією [8] такий шифр не є марковським, оскільки вхідні значення нелінійних операцій, починаючи з другої, не рандомізуються ключем. Тим не менше, в сучасних роботах з диференційного криптоаналізу ARX-шифрів робиться припущення, що шифр є марковським, і ймовірність ДХ для одного циклу перетворення обчислюється як добуток ймовірностей перетворення різниць при проходженні крізь нелінійні операції [12]. Таке припущення не матиме суттєвого впливу на результат оцінки, проте значно спростить процес оцінювання (хоча, поодинокі приклади випадків, коли шифр поводить себе як немарковський, також наведені в літературі [13]). В будь-якому разі, на поточний момент невідомо, як розраховувати диференційну ймовірність у разі припущення про «немарковість» шифру. Викладені у цій статті результати також базуються на припущенні, що «Кипарис» є марковським шифром.

Вперше підхід до проектування ARX-шифрів, які є доказово стійкими до для диференційного (лінійного) криптоаналізу, представлений в [14]. Якщо для блокових шифрів, побудованих на основі S-блоків, застосовується стратегія широкого сліду, то для ARX-шифрів

пропонується так звана стратегія довгого сліду (англ. long trail strategy). Нова стратегія пропонує використовувати S-блоки разом з простими лінійними операціями [14]. Застосування запропонованого підходу при розробці шифру SPARX дозволило отримати оцінку верхньої границі диференційної ймовірності для цього шифру.

Що стосується оцінки стійкості існуючих ARX-шифрів, на сьогоднішній день не існує універсального теоретичного методу оцінки верхньої границі ймовірності ДХ для ARX-шифрів. Існуючі методи оцінки, як правило, базуються на результатах застосування евристичних алгоритмів пошуку кращих диференційних характеристик [12, 13]. До найбільш відомих таких методів можна віднести наступні:

- модифікований алгоритм Мацуї із застосуванням часткових таблиць розподілу різниць [12], найбільш розвинутий з існуючих методів;
- метод, заснований на пошуку ймовірносних нейтральних бітів (англ. probabilistic neutral bits) [15], наразі застосований до потокових шифрів Salsa та ChaCha;
- метод, заснований на задачі здійснимості булевих формул (англ. SAT solvers) [13], який також запропонований для криптоаналізу шифру Salsa.

Найбільшого застосування набув метод пошуку на основі часткових таблиць розподілу різниць, запропонований А. Бірюковим та В. Вєлічковим [12].

Таблиця розподілу різниць (TPP) для додавання n-бітових слів за модулем 2^n містить ймовірності перетворення двох вхідних різниць у вихідну після проходження крізь операцію модульного додавання.

Означення 1 [12, 16]. Нехай α, β та γ – фіксовані n-бітні різниці (за операцію XOR). Диференційна ймовірність додавання за модулем 2^n (xdp^+) – це ймовірність, з якою вхідні різниці α та β переходять у вихідну різницю γ після проходження через операцію додавання, обчислена для всіх пар n-бітових вхідних текстів (x, y):

$$\mathrm{xdp}^+(\alpha,\beta\to\gamma)=2^{-2n}\cdot\#\{(x,y):((x\oplus\alpha)+(y\oplus\beta))\oplus(x+y)\}=\gamma. \quad (4)$$

Як можна помітити з формули (4), розрахунок значення ймовірності прямим шляхом перебирання усіх вхідних пар навіть для одного переходу є обчислювально складною задачею. Ефективний алгоритм для практичного обчислення значення xdp^+ представлений в [17].

У зв'язку з великим розміром модуля n, навіть із застосуванням ефективного алгоритму, побудування повної таблиці розподілу різниць є нездійсненною на практиці задачею. У свою чергу в [12] пропонується будувати так звану часткову TPP, що містить диференціали $(\alpha,\beta\to\gamma)$ з ймовірністю, що дорівнює або перевищує заданий поріг p_{thres} [12]:

$$(\alpha,\beta,\gamma)\in D\Leftrightarrow(\alpha,\beta\to\gamma)\geq p_{thres}. \quad (5)$$

Далі пропонується побудувати таку часткову таблицю для усієї циклової функції та, використовуючи модифікований алгоритм Мацуї, здійснити пошук диференційних характеристик. Цей метод був успішно застосований до блокових шифрів заснованих на мережі Фейстеля з ARX-подібною цикловою функцією, а саме таких як SPECK, TEA, XTEA та ін.

Можна відмітити, що описаний метод найбільше підходить до шифрів з достатньо простою цикловою функцією, в якій не передбачається поділу вхідного значення на слова. Це пояснюється тим, що коли операції додавання та зсуву застосовуються до цілого вхідного значення, побудувати часткову TPP для такої циклової функції достатньо просто.

3. Функція шифрування блокового шифру «Кипарис»

Блоковий шифр «Кипарис» оперує блоками даних розміром l біт, із використанням ключа шифрування довжиною k біт, $l,k\in\{256,512\}$, $l = k$. Операції циклової функції виконуються над s-бітними словами, $s\in\{32,64\}$. Загальні параметри шифру наведені в табл. 1 [2].

Таблиця 1

Загальні параметри блокового шифру «Кипарис»

Параметр	Кипарис-256	Кипарис-512
Розмір блока (l), біт	256	512
Довжина ключа (k), біт	256	512
Довжина слова (s), біт	32	64
Кількість циклів (t)	10	14

Схематичне зображення функції зашифрування наведено на рис. 1. Як видно з рисунку, шифр «Кипарис» представляє собою мережу Фейстеля з ARX-перетворенням у якості циклової функції, що містить 8 додавань за модулем 2^s, 8 додавань за модулем 2 та 8 циклічних зсувів.

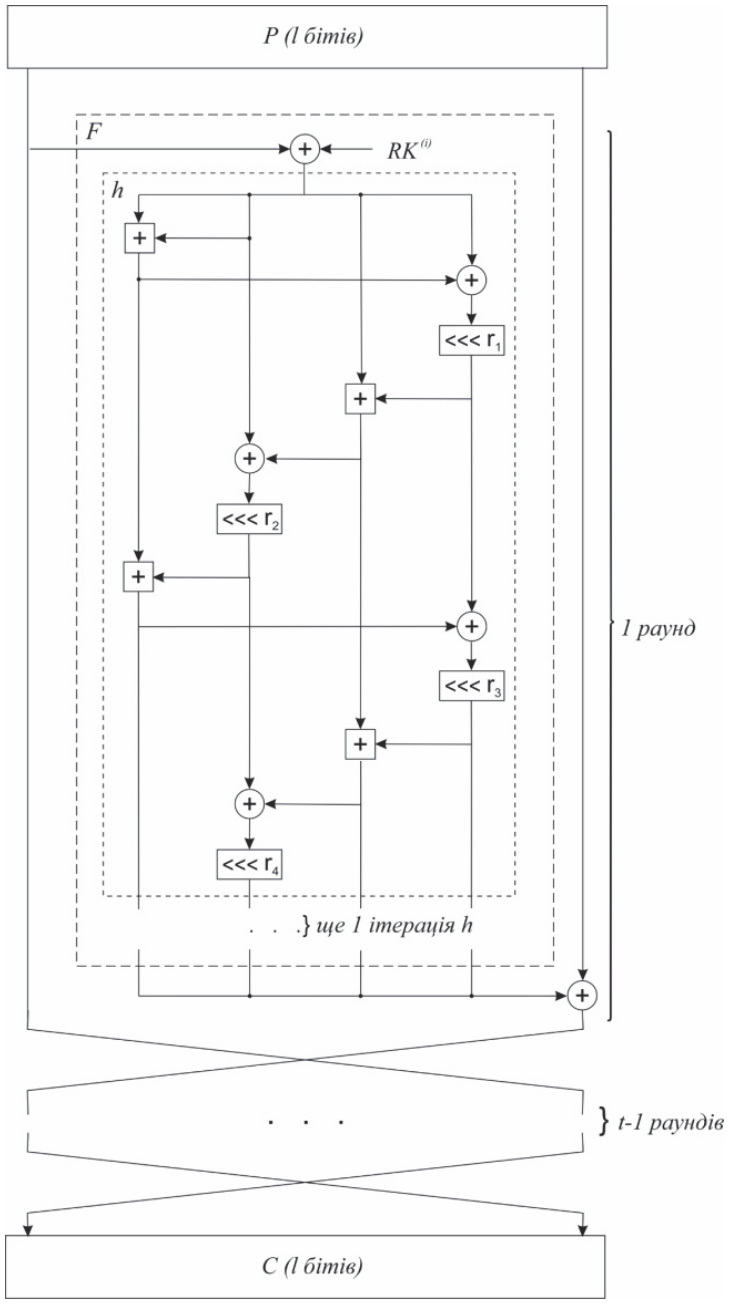

Рис. 1. Функція зашифрування шифру «Кипарис»

4. Математична модель оцінки стійкості блокового шифру «Кипарис» до диференційного криптоаналізу

Нехай $\oplus$ (XOR) є операцією, що визначає різницю між парою текстів, а $\boxplus$ є операцією додавання за модулем 2^s, для якої диференційна ймовірність $\mathrm{xdp}^+ \le 1$. Введемо наступні припущення.

Припущення 1. Блоковий шифр «Кипарис» є марковським шифром, тому:

1) Середня за ключами ймовірність одноциклової ДХ $\mathrm{EDP}^{(1)}(\Omega)$ дорівнює добутку ймовірностей перетворення вхідних різниць на восьми модульних суматорах:

$$\mathrm{EDP}^{(1)}(\Omega) = \prod_{i=1}^{8} \mathrm{xdp}^+(\alpha_i, \beta_i \to \gamma_i), \tag{6}$$

де (α_i, β_i) – різниці на вході *i*-го суматора, γ_i – різниця на виході *i*-го суматора.

2) Середня за ключами ймовірність *r*-циклової ДХ визначається добутком ймовірностей одноциклових ДХ [8].

Нехай $(\Omega_1, \Omega_2, ..., \Omega_r)$ – множина одноциклових ДХ таких, що $\Omega_1 = (\alpha, \beta_1), \Omega_2 = (\beta_1, \beta_2), ..., \Omega_r = (\beta_{r-1}, \beta_r)$ та $\Omega = (\alpha, \beta_1, ..., \beta_r)$. Тоді ймовірність $\mathrm{EDP}^{(r)}(\Omega)$ може бути апроксимована як

$$\mathrm{EDP}^{(r)}(\Omega) = \prod_{i=1}^{r} \mathrm{EDP}^{(1)}(\Omega_i). \tag{7}$$

Припущення 1 витікає із загальноприйнятих припущень, що робляться з метою спрощення отримання оцінок для ARX-шифрів [12, 13].

Припущення 2. При обчисленні вихідної різниці γ, в яку перетворюються вхідні різниці α та β після проходження крізь операцію модульного додавання, обирається вихідна різниця, що має максимальну ймовірність:

$$\gamma = \boxplus(\alpha, \beta), \mathrm{xdp}^+(\alpha, \beta \to \gamma) = \max \Gamma, \tag{8}$$

де Γ – множина усіх можливих вихідних різниць для (α, β).

У багатьох випадках для пари вхідних різниць (α, β) існує декілька вихідних різниць з максимальною ймовірністю. Якщо таких різниць небагато (≈5-10), тоді обчислюються диференційні шляхи для усіх можливих варіантів. У разі, коли значення $\max \Gamma$ є достатньо малим, кількість вихідних різниць з максимальною ймовірністю може бути дуже великою (тисячі та десятки тисяч). Тоді робиться випадкова вибірка (random sampling) з множини різниць, що мають максимальну імовірність, та будуються диференційні шляхи лише для них.

Припущення 3. У високоймовірнісних одноциклових ДХ шифру «Кипарис» вхідні різниці мають малу вагу Хемінга, а саме 3-7 активних бітів (при цьому, активні біти рознесені по різним словам). Таке припущення пояснюється тим, що вхідні різниці найбільш ймовірних переходів в таблиці розподілу різниць для модульного додавання мають малу кількість активних бітів. Обґрунтуємо припущення 3 більш детально.

Означення 2. Кількістю активних біт *b* у різниці (α, β), яка поступає на вхід суматора, називається число одиниць, що міститься у доданку $\alpha \oplus \beta$.

Розглянемо часткову ТРР для додавання за модулем 2^{32}, що містить переходи з ймовірністю $\mathrm{xdp}^+(\alpha, \beta \to \gamma) \ge 1/2$. Для переходів з ймовірністю $\mathrm{xdp}^+(\alpha, \beta \to \gamma) = 1$, яких у ТРР

всього чотири, кількість активних біт у вхідній різниці дорівнює $b \le 1$. Зазначимо, що це справедливо для будь-якого значення n (табл. 2).

Для переходів з ймовірністю $\mathrm{xdp}^+\left(\alpha, \beta \to \gamma\right) = 1/2$ (для $n = 32$ таких всього 744), кількість активних біт у вхідній різниці обмежується двома, $b \le 2$.

У [16] наводиться вираз, що описує зв'язок між позиціями бітів вхідної та вихідної різниць й імовірністю, а саме верхня границя диференційної ймовірності операції модульного додавання визначається як $\Pr\left[\alpha, \beta \to \gamma\right] \le 2^{-k}$, де $k = \#\left\{i : \neg\left(\alpha[i] = \beta[i] = \gamma[i]\right), 0 \le i \le n-2\right\}$, тобто кількість бітових позицій, за виключенням найбільш значущого біта, на яких біти різниць α, β, γ не є рівними.

Таблиця 2

Переходи в TPP для додавання за модулем 2^n з ймовірністю $\mathrm{xdp}^+\left(\alpha, \beta \to \gamma\right) = 1$

№	α	β	γ
1	0	0	0
2	$1\underbrace{0\ldots0}_{n-1}$	0	$1\underbrace{0\ldots0}_{n-1}$
3	0	$1\underbrace{0\ldots0}_{n-1}$	$1\underbrace{0\ldots0}_{n-1}$
4	$1\underbrace{0\ldots0}_{n-1}$	$1\underbrace{0\ldots0}_{n-1}$	0

Таблиця 3

Результати щодо розповсюдження активних бітів для циклової функції блокового шифру «Кипарис»

128-бітова вхідна різниця (1 позначає слово, в якому є активні біти)	Кількість активних бітів на виході циклової функції	
	Нижня границя	Верхня границя
1000	14	14
0100	19	19
0010	7	7
0001	10	10
1100	5	33
0110	12	26
0011	3	17
0101	9	29
1010	7	21
1001	4	24
1110	2	40
1101	5	43
1011	3	21
0111	2	36

Таким чином, мінімізація кількості активних бітів у різниці на вході модульних суматорів підвищує загальну ймовірність ДХ. У шифрі «Кипарис» перші три слова різниці, що подається на вхід циклової функції, попадають на вхід модульного суматора одразу, а четверте – після застосування операцій побітового додавання та циклічного зсуву, тому припущення про малу кількість активних біт на вході циклової функції є цілком обґрунтованим. Враховуючи вплив лінійних операцій на процес розповсюдження активних бітів, припускається, що 1-2 активних біти на вході циклової функції добре розповсюдяться по різним словам на виході. Експерименти показали, що 1 активний біт на вході циклової функції переходить щонайменше у 7 активних бітів на виході (див. табл. 3). У свою чергу, декілька активних бі-

тів у різних словах можуть знищитись за рахунок застосування лінійних операцій. Таким чином, приблизно 3-7 активних бітів на вході циклової функції, які розподілені між різними словами, дозволять отримати високоймовірну ДХ, оскільки забезпечать оптимальне розповсюдження активних бітів для максимізації ймовірності перетворення різниць на суматорах.

5. Методи пошуку багато циклових диференційних характеристик блокового шифру «Кипарис»

Як зазначалось вище, найбільш відомим методом пошуку диференційних характеристик є модифікований метод Мацуї із застосуванням часткових ТРР [12], який добре підходить до шифрів з простими цикловими функціями з невеликим розміром входу, що послідовно обробляється декількома операціями додавання та зсуву. У випадку шифру «Кипарис», де 128/256-бітове вхідне значення циклової функції ділиться на 32/64-бітові слова, які проходять крізь велику кількість операцій додавання, часткова ТРР повинна містити диференціали з достатньо низькою ймовірністю. Крім того, кількість диференційних шляхів зростає з кожним суматором. Все це призводить до того, що обсяг часткової ТРР стає значно великим для обчислення за прийнятний час. Тому вважатимемо, що при побудуванні диференційних характеристик для шифру «Кипарис» краще обчислювати значення ймовірностей на суматорах на льоту, користуючись швидким алгоритмом, запропонованим Ліпмою та Моріарі [17].

У [3] представлено три методи пошуку кращих диференційних характеристик для одного циклу перетворень шифру «Кипарис». Оптимізований метод дозволив знайти одноциклову характеристику, що має ймовірність ¼. У цьому розділі пропонуються методи пошуку багатоциклових диференційних характеристик та результати їх застосування.

5.1. Метод пошуку багатоциклових ДХ, заснований на побудуванні множини високоймовірнісних одноциклових ДХ

Нагадаємо, що пошук диференційних характеристик проводиться з метою знаходження високоймовірнісних диференційних шляхів та підтвердження, що ймовірність найкращої знайденої (r-1)-циклової ДХ $\mathrm{EDP}^{(r-1)}(\Omega) < 2^k$, де k – довжина ключа шифрування. Для виконання цієї задачі, по-перше, пропонується побудувати достатньо велику множину одноциклових ДХ та виконати пошук можливих комбінацій одноциклових ДХ у двоциклові (багатоциклові) ДХ. В загальному вигляді ***метод*** складається з наступних кроків.

1) Згідно з Припущенням 3, сформувати множину вхідних різниць Ξ, для яких буде побудовано одноциклові ДХ. До множини Ξ включити усі можливі комбінації $l/2$ – бітових рядків з вагою Хемінга 1-7 бітів ($l/2$ – довжина напівблока, що подається на вхід циклової функції). Оскільки нас цікавитимуть не лише найбільш ймовірні ДХ, до множини включено й різниці з вагою Хемінга 1-3 бітів.

2) Побудувати одноциклові ДХ для вхідних різниць з множини Ξ. Вихідні різниці після проходження крізь операцію модульного додавання обчислювати згідно з Припущенням 2, а ймовірність одноциклової ДХ $\mathrm{EDP}^{(1)}(\Omega)$ згідно з пунктом 1 Припущення 1. Зазначимо, що для однієї вхідної різниці, як правило, буде існувати декілька ДХ.

3) Враховуючи, що довжина ключа дорівнює k, а кількість циклів шифрування дорівнює t, з усіх обчислених ДХ до множини Ψ включити ДХ, що мають ймовірність $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-k/t}$.

4) Якщо для вхідних різниць з деякою вагою Хемінга обчислення всіх ДХ потребує значних обчислювальних ресурсів, зменшити значення $\mathrm{EDP}^{(1)}_{thres}(\Omega)$ для ДХ, побудованих для вхідних різниць з цією вагою Хемінга.

5) Здійснити пошук комбінацій одноциклових ДХ з множині Ψ у двоциклові (багатоциклові) ДХ.

Запропонований метод був застосований до шифру «Кипарис-256». У зв'язку з обмеженням обчислювальних ресурсів, до множини Ψ були додані ДХ:

- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-26}$ для вхідних різниць з вагою Хемінга 1-4 бітів;
- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-18}$ для вхідних різниць з вагою Хемінга 5 бітів;
- з ймовірністю $\mathrm{EDP}^{(1)}_{thres}(\Omega) \geq 2^{-10}$ для вхідних різниць з вагою Хемінга 6 бітів.

Результати побудування множини високоймовірнісних одноциклових ДХ наведені в табл. 4.

Таблиця 4

Характеристики множини високоймовірнісних одноциклових ДХ

Вага Хемінга вхідної різниці	$\mathrm{EDP}^{(1)}_{thres}(\Omega), \log_2 n$	$\mathrm{MEDP}^{(1)}(\Omega), \log_2 n$	$\lvert\Psi\rvert$
1	-26	> -26	0
2	-26	-14	2986
3	-26	-12	10357
4	-26	-6	28392
5	-18	-2	1446
6	-10	-3	343

Як і було припущено у математичній моделі (див. Припущення 3), ДХ, побудовані для вхідних різниць з вагою Хемінга 4-6 бітів, мають високу ймовірність. Деякі з отриманих ДХ представлені у табл. 5.

Таблиця 5

Найбільш ймовірні одноциклові диференційні характеристики блокового шифру «Кипарис»

Вхідна різниця у 32-бітових словах, hex	Вихідна різниця у 32-бітових словах, hex	$\mathrm{EDP}^{(1)}(\Omega), \log_2 n$
0 80000000 800000 80008080	80000000 4000 80 80	-2
80000 80080000 80000000 80000000	800 4040040 80080000 80000	-3
0 80000000 1800000 80008080	80000000 4000 80 80	-3
180000 80080000 80000000 80000000	800 4040040 80080000 80000	-4
80000 80000 80800000 8080	80000800 4044040 80080080 80080	-5
80000000 0 80000000 80008000	88000000 40404404 808088 800088	-6
80000000 80000000 80800000 80	8000000 40400404 808008 800008	-6
80 80 80000080 8000	8 40040440 80800800 80000800	-7
8000 8000 8080 800000	800 4044040 80080080 80080	-7
80000000 80000800 800 800	800000 40040040 80000800 80000000	-7
0 80 80000000 808080	80 400000 8000 8000	-7
0 800000 8000 80800080	800000 40 80000000 80000000	-7
80000000 80000000 81800000 80	8000000 40400404 808008 800008	-7
0 100 1 1010100	100 800000 10000 10000	-8
0 200 2 2020200	200 1000000 20000 20000	-8
0 800 8 8080800	800 4000000 80000 80000	-8
0 1000 10 10101000	1000 8000000 100000 100000	-8
0 2000 20 20202000	2000 10000000 200000 200000	-8
0 4000 40 40404000	4000 20000000 400000 400000	-8
0 8000 80 80808000	8000 40000000 800000 800000	-8
180 80 80000080 8000	8 40040440 80800800 80000800	-8
80 80 80000180 8000	8 40040440 80800800 80000800	-8
100 80 80000000 808080	80 400000 8000 8000	-8
80001000 80000800 800 800	800000 40040040 80000800 80000000	-8
8000 8000 8180 800000	800 4044040 80080080 80080	-8
80000000 40000000 400000 40004040	40000000 2000 40 40	-8
0 40 c0000000 404040	40 200000 4000 4000	-8
0 800000 18000 80800080	800000 40 80000000 80000000	-8
0 40000000 80400000 40004040	40000000 2000 40 40	-8

Не дивлячись на те, що деякі ДХ мають вихідну різницю, яка співпадає з вхідною різницею інших ДХ, жодних комбінацій одноциклових ДХ у двоциклові виявлено не було (див. пункт 5 запропонованого методу). Це означає, що отримані ДХ, вихідні різниці яких мають малу вагу Хемінга, не можуть бути продовжені для побудування багатоциклових ДХ з високою ймовірністю.

5.2. Пошук існуючих найбільш ймовірних багатоциклових ДХ та оцінка стійкості блокового шифру «Кипарис-256»

Наступний крок на шляху пошуку багатоциклових ДХ полягає у продовженні одноциклових ДХ з множини Ψ на декілька циклів. Відмітимо, що особливість архітектури мережі Фейстеля дозволяє підбирати вхідну різницю таким чином, щоб «пропустити» один цикл шифрування, тобто створити таку ситуацію, коли на певному циклі на вхід циклової функції подається значення $\Delta X = 0$, ймовірність перетворення якого дорівнює 1. З метою максимізації ймовірності ДХ для перших трьох циклів шифрування, в якості лівої половини різниці пропонується подати значення ΔX, а в якості правої – $\Delta Y = F(\Delta X)$. Завдяки цьому ймовірність ДХ для 1-го та 3-го циклів буде однаковою, а для 2-го – дорівнюватиме 1. Шлях проходження вхідної різниці для чотирьох циклів шифрування зображено на рис. 2.

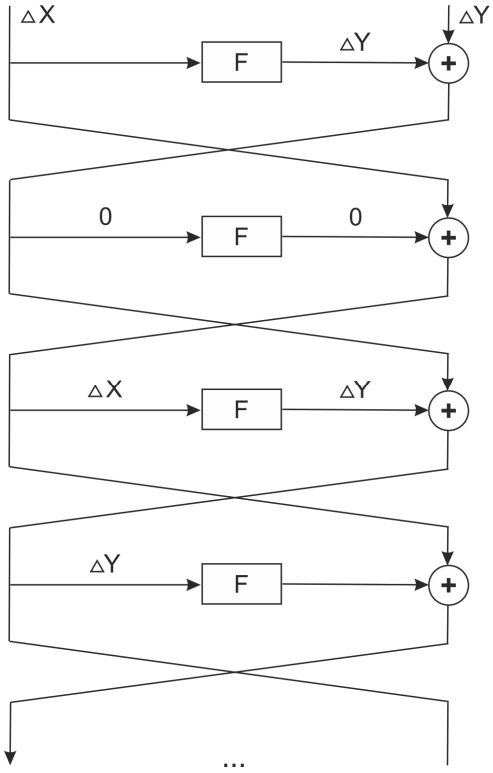

Рис. 2. Шлях проходження вхідної різниці для 4-х циклів шифрування

Пошук найбільш ймовірних багатоциклових ДХ складається з наступних кроків.

1) Визначити l-бітову вхідну різницю як таку, що складається з двох $l/2$ – бітових половин ΔX та ΔY.

2) Сформувати множину Z l-бітових вхідних різниць для пошуку багатоциклових ДХ наступним чином. Визначити вхідну різницю ζ_i з множини Z як $\zeta_i = (\Delta X_i \,|\, \Delta Y_i)$, де ΔX_i та ΔY_i – значення вхідної та вихідної різниць i-ї ДХ з множини Ψ відповідно.

3) Для кожної вхідної різниці ζ_i з множини Z побудувати ДХ для j циклів за умови, що $\mathrm{EDP}^{(j)}(\Omega) > 2^{-256}$. ДХ для кожного циклу будувати згідно пунктів (2) – (4) методу, представленого у розд. 5.1.

У табл. 6 представлені параметри однієї з найбільш ймовірних ДХ, знайденої за допомогою описаного вище методу. Зазначимо, що за рахунок застосування механізму випадкової вибірки 1) при обчисленні значень вихідних різниць для операції модульного додавання та 2) при обранні виходу з циклової функції між циклами шифрування, значення $\mathrm{EDP}^{(j)}(\Omega)$ є апроксимованим (обчислення всіх існуючих диференційних шляхів навіть для одного значення вхідної різниці є обчислювально складною задачею).

Таблиця 6

Параметри однієї з найбільш ймовірних знайдених багатоциклових ДХ для блокового шифру «Кипарис»

Номер циклу, j	ДХ $\Omega(a,b)$ для j-го циклу, hex	$\mathrm{EDP}^{(1)}(\Omega), \log_2 n$	$\mathrm{EDP}^{(j)}(\Omega), \log_2 n$
1	a = (00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080), b = (00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000)	-10	-10
2	a = (00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080), b = (00000000 00000000 00000000 00000000 00000000 80008000 00800080 00800080)	0	-10
3	a = (00000000 80008000 00800080 00800080 00000000 00000000 00000000 00000000), b = (00000000 80008000 00800080 00800080 80008000 40004000 00800080 00800080)	-10	-20
4	a = (80008000 40004000 00800080 00800080 00000000 80008000 00800080 00800080), b = (80008000 40004000 00800080 00800080 c0204020 90009000 00a000a0 00800080)	-27	-47
5	a = (c0204020 90009000 00a000a0 00800080 80008000 40004000 00800080 00800080), b = (c0204020 90009000 00a000a0 00800080 5208d204 40444044 08820882 0a800a80)	-74	-121
6	a = (5208d204 40444044 08820882 0a800a80 c0204020 90009000 00a000a0 00800080), b = (5208d204 40444044 08820882 0a800a80 266e7071 a74313f2 0088e7e0 10fa6fd2)	-102	-223

Таким чином, знайдена найбільш ймовірна ДХ для шести циклів шифрування має ймовірність

$$\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}.$$

Отримане значення $\mathrm{MEDP}^{(6)}(\Omega)$ будемо називати практичною стійкістю блокового шифру «Кипарис» до диференційного криптоаналізу. Через застосування механізму випадкової вибірки, значення $\mathrm{MEDP}^{(6)}(\Omega)$ може дещо відрізнятися у різних експериментах, проте це суттєво не впливає на загальний результат оцінки, оскільки

$$\mathrm{MEDP}^{(7)}(\Omega) << 2^{-256}, 7 < (r-1).$$

Таким чином, блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

Висновки

1. Найбільшу ймовірність мають одноциклові диференційні характеристики блокового шифру «Кипарис», вхідна різниця яких містить приблизно 3 – 7 активних бітів, які розподілені між різними словами. Це пояснюється оптимальним розповсюдження активних бітів, що призводить до максимізації ймовірності перетворення різниць на суматорах.

2. Застосування запропонованого методу пошуку багатоциклових диференційних характеристик, заснованого на побудуванні множини високоймовірнісних одноциклових диференційних характеристик, до блокового шифру «Кипарис-256» показало, що побудовані одноциклові ДХ, вихідні різниці яких мають малу вагу Хемінга (а значить і достатньо високу ймовірність), не можуть бути продовжені для побудування багатоциклових ДХ з високою ймовірністю.

3. Одна зі знайдених найбільш ймовірних багатоциклових диференційних характеристик для блокового шифру «Кипарис-256» може бути побудована лише для шести циклів шифрування з ймовірністю $\mathrm{MEDP}^{(6)}(\Omega) \approx 2^{-223}$, що дає підстави стверджувати, що блоковий шифр «Кипарис-256» є практично стійким до диференційного криптоаналізу.

Список літератури:

1. Lightweight Cryptography. Project Overview. URL: https://csrc.nist.gov/projects/lightweight-cryptography.

2. Родінко М.Ю., Олійников Р.В. Постквантовий малоресурсний симетричний блоковий шифр «Кипарис» // Радіотехніка. – 2017. – Вип. 189. – С. 100-107.

3. Родінко М.Ю., Олійников Р.В. Методи пошуку диференційних характеристик циклової функції симетричного блокового шифру «Кипарис» // Радіотехніка. – 2017. – Вип. 191. – С. 47-51.

4. Biham, E. Differential Cryptanalysis of DES-like Cryptosystem / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – Vol. 4. – P. 3-72.

5. Bernstein D. J. ChaCha, a Variant of Salsa // Workshop Record of SASC: The State of the Art of Stream Ciphers.

6. Beaulieu R. et al. The SIMON and SPECK lightweight block ciphers // Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. – IEEE, 2015. – С. 1-6.

7. Wheeler D. J. and Needham R. M. TEA, a Tiny Encryption Algorithm // International Workshop on Fast Software Encryption, Springer, Heidelberg, 1995. – P. 363–366.

8. Lai X., Massey J. L. and Murphy S. Markov ciphers and differential cryptanalysis // Workshop on the Theory and Application of of Cryptographic Techniques, Springer, Berlin, Heidelberg, 1991. – P. 17-38.

9. Canteaut, Anne, and Joëlle Roué. Differential Attacks Against SPN: A Thorough Analysis // International Conference on Codes, Cryptology, and Information Security. Springer, Cham, 2015.

10. Kanda M., Takashima Y., Matsumoto T., Aoki K., Otha K. A strategy for constructing fast round functions with practical security against differential differential and linear cryptanalysis // Selected Areas in Cryptography. – SAC 1998, Proceedings. – Springer Verlag, 1999. – P. 264 – 279.

11. Daemen, Joan, and Vincent Rijmen. The wide trail design strategy // IMA International Conference on Cryptography and Coding. Springer, Berlin, Heidelberg, 2001.

12. Biryukov A., Velichkov V. Automatic Search for Differential Trails in ARX Ciphers // CT-RSA. – 2014. – Т. 8366. – С. 227-250.

13. Mouha, Nicky and Bart Preneel. Towards finding optimal differential characteristics for ARX: Application to Salsa20. Cryptology ePrint Archive, Report 2013/328, 2013.

14. Dinu D. et al. SPARX: A Family of ARX-based Lightweight Block Ciphers Provably Secure Against Linear and Differential Attacks // Proceedings of ASIACRYPT'16. – P. 1-21, 2016.

15. Aumasson J. P. et al. New features of Latin dances: analysis of Salsa ChaCha and Rumba // Lecture Notes in Computer Science. – 2008. – Vol. 5086. – P. 470-488.

16. Lipmaa, Helger, Johan Wallén, and Philippe Dumas. On the additive differential probability of exclusive-or. // International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2004.

17. Lipmaa H. and Moriai S. Efficient algorithms for computing differential properties of addition // International Workshop on Fast Software Encryption, Springer, Berlin, Heidelberg, 2001. – P. 336-350.

Харківський національний
університет імені В.Н. Каразіна

Надійшла до редколегії 25.10.2018