© Kudin A., Kovalenko B. Differential analysis of hash functions and block ciphers: generalized approach // Ukrainian Scientific Journal of Information Security, 2015, vol. 21, issue 2, p. 159-164.

ДИФЕРЕНЦІЙНИЙ АНАЛІЗ ФУНКЦІЙ ХЕШУВАННЯ ТА БЛОКОВИХ ШИФРІВ: УЗАГАЛЬНЕНИЙ ПІДХІД

Антон Кудін, Богдан Коваленко

Національний технічний університет України «КПІ», Україна

КУДІН Антон Михайлович, д.т.н.

Рік та місце народження: 1971 рік, м. Київ, Україна.
Освіта: Київське вище інженерне радіотехнічне училище протиповітряної оборони імені Маршала авіації О. І. Покришкіна.
Посада: професор кафедри математичних методів захисту інформації фізико-технічного інституту, НТУУ «КПІ».
Наукові інтереси: теоретична криптографія, теорія інформації, асиметрична криптографія, методи реалізації криптографічних систем.
Публікації: більше 100 статей, 3 монографії, посібники, матеріали та тези доповідей на конференціях.
E-mail: pplayshner@gmail.com.

КОВАЛЕНКО Богдан Анатолійович

Рік та місце народження: 1990 рік, м. Кам'янець-Подільський, Хмельницька область, Україна.
Освіта: Національний технічний університет України «КПІ», 2013 рік.
Посада: аспірант.
Наукові інтереси: криптоаналіз функцій хешування, апаратне прискорення криптоалгоритмів.
Публікації: матеріали та тези доповідей на конференціях.
E-mail: animantbk@gmail.com

Анотація. *Методи диференційного криптоаналізу є потужними методами аналізу блокових шифрів. Для аналізу функцій хешування, зокрема функцій на базі фейстелевських несбалансованих схем, також використовуються схожі методи. У даній статті узагальнюється диференційний криптоаналіз для функцій хешування, що базуються на несбалансованих схемах Фейстеля, та блокових шифрів на основі схем Фейстеля. Отримані результати доводять, що за подібності ідей диференційного аналізу блокових шифрів та функцій хешування, вони мають суттєві відмінності, завдяки яким, однаковим параметрам безпеки відповідають різні стійкості до атак з використанням диференційного аналізу для шифрів та функцій хешування. Дані результати також дозволяють виробляти додаткові обмеження на параметри безпеки при побудові нових функцій хешування.*

Ключові слова: *захист інформації, функція хешування, диференційний аналіз, MD5, схема Фейстеля, бітові умови, метод тунелювання.*

Вступ

У даній статті порівнюються особливості застосування диференційного криптоаналізу до блокових фейстелівських шифрів та функцій хешування, що базуються на незбалансованих схемах Фейстеля.

Сучасна теорія диференційного аналізу блокових шифрів є досить розвиненою в той час як диференційний аналіз функцій хешування наразі є недостатньо обгрунтованим теоретично. Не дивлячись на числені результати в криптоаналізі шифрів, ці результати не можуть бути напряму перенесені у хеш-функції.

В роботі спершу узагальнюються поняття шифрів та хеш-функцій, далі наводяться приклади застосування диференційного аналізу для шифру DES та хеш-функції MD5.

Основне дослідження полягає в спробі узагальнити концепції диференційного аналізу для блокових шифрів та хеш-функцій з метою демонстрації універсальності підходу. Результатом роботи очікується отримати узагальнену модель для опису диференційного аналізу як блокових шифрів, так і хеш функцій. В перспективі така модель може застосовуватися для кількісного порівняння стійкості базових блокових шифрів та хеш функцій на їх основі, що може призвести до появи обгрунтованих критеріїв побудови хеш функцій з заданими параметрами стійкості.

Мета та методи криптоаналізу блокових шифрів та функцій хешування

У даній роботі розглядатимуться блокові

шифри. Усі сучасні блокові шифри використовують ідеї ітеративних шифрів, що описані Шенноном [1] . Зокрема, ця ідея була впроваджена Хорстом Фейстелем у шифрі Люцифер та DES. Наразі, модифікації схеми Фейстеля використовується в більшості криптопримітивах, що застосовуються на практиці. Найбільш відомими прикладами блокових шифрів з використанням схеми Фейстеля є DES, Blowfish, Twofish, IDEA, RC6, MISTY, SEED, KASUMI.

Розглянемо взаємозв'язок блокових шифрів та функцій хешування. Блоковий шифр – це відображення виду:

$$E: X \times K \to Y, \quad (1)$$

де X – простір відкритих текстів, K – простір ключів і Y – простір зашифрованих блоків.

Для шифру також накладаються умови практичної неможливості отримання відкритого повідомлення $x \in X$ з відомого шифртексту $y \in Y$ без знання ключа $k \in K$, а також неможливості отримання ключа з відомих пар відкритого та шифрованого тексту.

Функція хешування – це відображення виду:

$$H: K \to Y, \quad (2)$$

де K – простір повідомлень, Y – простір хеш-значень.

На практиці, функції хешування часто реалізуються на основі блокових шифрів, що і визначає певну спорідненість аналізу шифрів та функцій хешування. Такі функції хешування використовують дві концепції побудови: обробка повідомлення блоками за допомогою односторонніх функцій – функцій стиснення (схема Меркла-Дамгарда [5]) та використання блокового шифру для функції стиснення (роль ключа у цьому випадку відіграє блок повідомлення). Схема Меркла-Дамгарда має вигляд:

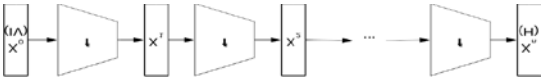

Рис. 1. Схема Меркла-Дамгарда

де X_i – внутрішні стани (стан X_0 – стартовий вектор, стан X_n – хеш-значення), f – функція стиснення.

Було доведено [5] , якщо функція f стійка до побудови колізій, то і уся схема також стійка до побудови колізій.

Прикладами найбільш розповсюджених конструкцій функцій стиснення є:

– $h(X,K) = E_K(X) + X$ – схема Девіса-Мейера,

– $h(X,K) = E_K(X) + K$ – схема Матіаса-Мейера-Осіаса,

– $h(X,K) = E_K(X) + X + K$ – схема Міягучі.

Прикладами таких функцій є функції родини MD (MD4, MD5, SHA-0/1/2), RIPEMD, Skein та багато інших. Особлива увага приділятиметься функціям родини MD через їх широку розповсюдженість та через те, що вони базуються на незбалансованих фейстелівських схемах.

Мови хеш-функцій стискання та блокових шифрів можна задати скінченним розпізнавальним автоматом

$$T =< V, Q, q_0, f_0, \delta >,$$

де V – вхідний алфавіт. У випадку шифру DES алфавітом є $V = \{0,1\}^{48}$ – 48-бітовий фрагмент ключового розкладу, у випадку хеш-функції MD5 алфавітом є $V = \{0,1\}^{32}$ – 32-бітове слово повідомлення, Q – множина станів. Для шифру DES це 64-бітовий блок на виході з раунду, для MD5 це 128-бітовий блок на виході з раунду, q_0 , f_0 – початковий та кінцевий стани. Варто також зазначити, відкриті та зашифровані тексти шифрів, стартовий вектор та хеш-код функції хешування можна вважати фіксованими значеннями оскільки їх завжди можна досягти додаванням необхідної кількості раундів зі спеціально підібраними ключами, δ – функція переходів, $\delta: V \times Q \to Q$. По суті, це є раундове перетворення алгоритму.

Автомат розпізнає мову $L = \{< x, k, E_k(x) > | \, x \in X, k \in K\}$.

На мові можна задати відношення еквівалентності $\langle x, k, E_k(x)\rangle = \langle x', k', E_{k'}(x)\rangle \Leftrightarrow k = k'$,

$L_k = \{< x, E_k(x) > | \, x \in X\}$ – класи еквівалентності.

Отже, для блокового шифру атака пошуку ключа з відомими відкритими текстами є задачею пошуку усіх класів еквівалентності $M = \{L_k \mid L_k \supset l\}$ за заданою множиною $l = \{< x, y > | \, x \in X, y \in Y\}$, де X, Y – множини відкритих та шифрованих текстів відповідно. Необхідність пошуку саме усіх класів витікає з того, що декілька ключів можуть задовольняти усі пари відкритих і зашифрованих текстів з множини l. Проте на практиці множина l перевищує відстань єдиності і лише клас еквівалентності єдиний.

Для функції хешування атака пошуку прообразу є задачею пошуку довільного класу еквівалентності з множини $M = \{L_k \mid L_k \ni l\}$ за заданим $l =< x, y >, x \in X, y \in Y$.

Тож пошук ключа блокового шифру та пошук повідомлення функції хешування є схожими задачами розпізнавання, але випадку шифрів шукається клас мови (часто єдиний) за підмножиною класу, а у випадку функцій хешування будь-який клас (з багатьох можливих), за представником класу. При цьому,

Різниця у методах та особливостях криптоаналізу функцій хешування та блокових шифрів випливає з різних цілей аналізу.

Для блокових шифрів найбільш характерними атаками є:

1. Пошук ключа на основі отриманих зашифрованих текстів (ШТ).

2. Пошук ключа на основі відомих відкритих і відповідних зашифрованих текстів (ВШТ).

3. Пошук ключа на основі вибраних відкритих та відповідних зашифрованих текстів (ВВТ).

4. Розшифрування(зашифрування) будь-яких зашифрованих(відкритих) текстів без знання ключа.

Для алгоритмів хешування найхарактернішими є такі атаки:

1. Атаки побудови колізії:

– пошук слабкої колізії: необхідно знайти такі $k,k' \in K : H(k) = H(k')$,

– пошук колізії з вибраним префіксом: для заданих $x,x' \in X$ знайти $k,k' \in K : h(x,k) = h(x',k')$,

– пошук сильної колізії: для заданого $k \in K$ потрібно знайти $k' \in K : H(k) = H(k')$.

2. Атаки пошуку прообразу:

– пошук прообразу: для заданого $y \in Y$ потрібно знайти таке $k \in K : H(k) = y$,

– пошук псевдопрообразу: для заданого $y \in Y$ потрібно знайти такі $k \in K, x \in X : h(x,k) = y$.

Отже, в загальному випадку, пошук ключа блокового шифру є складнішою задачею, ніж пошук прообразу функції хешування (на базі цього ж блокового шифру). Проте пошуку ключа шифру може суттєво сприяти можливість збору статистики внаслідок використання одного ключа для багатьох різних входів (чого принципово неможливо робити у функціях хешування).

Приклади застосування диференційного криптоаналізу

Отримання ключа DES.

Для ілюстрації методу диференційного аналізу стисло розглянемо диференційний аналіз DES, запропонований Біхамом та Шаміром у 1990 році [2] .

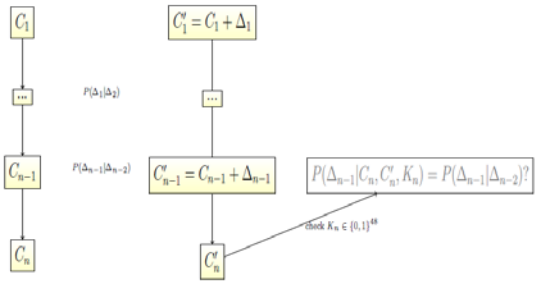

Рис. 2. Ідея диференційного аналізу DES

Основна ідея диференційного аналізу DES полягає в пошуку диференційної характеристики з високою ймовірністю та почергового підбору частин ключа. (див рис. 2).

Атака складається з таких кроків:

1. Пошук диференційної характеристики для шифру.

2. Подача на шифратор пар повідомлень з заданою різницею.

3. Отримання зашифрованих пар повідомлень.

4. Підбір ключа поточного раунду. При цьому відбувається спроба розшифрування на один раунд усіма можливими ключами. У випадку, якщо при розшифруванні різниця відповідає різниці характеристики з заданою ймовірністю, що відповідний ключ розглядається як кандидат на фрагмент повного ключа (їх може бути декілька).

Іншими словами, розшифрування раунду на неправильному ключі еквівалентне зашифруванню на один раунд, що руйнує кореляції між парами відкритих текстів. Найкращі результати для отримання ключа DES – 2^{37} зашифрувань проти 2^{56} для повного перебору.

Диференційний аналіз блокового шифру можна змоделювати множиною класів ймовірніснісних розпізнавальним автоматів:

$$\left\{T_K^{'} = \left\langle Q', q_0', \zeta_k \right\rangle\right\},$$

де Q' - множина станів (диференціали раунду), q_0' - початковий стан (диференціали на вході), ζ_k - функція ймовірності переходів.

Функція ймовірності переходів оцінюється теоретично на основі диференційного шляху, що використовується для атаки (для марківських шифрів це добуток ймовірностей переходу диференціалу через кожний раунд). Рандомізація роботи автомату відбувається шляхом подання на шифр різних пар повідомлень.

Тоді пошук ключа зводиться до задачі розпізнавання належності автомату $T_K^{'}$ до одного з класів $\{L_K\}$.

Побудова колізії для MD5.

Диференційний криптоаналіз функцій хешування дещо відрізняється від дослідження блокових шифрів. У даному випадку принципово неможливо відновлювати ключ частинами оскільки кожному виходу хеш-функції відповідає велика кількість повідомлень.

Основна ідея підбору колізій – побудова диференційного шляху з високою ймовірністю та підбір повідомлень таким чином, щоб вони задовольняли характеристиці.

Побудова колізії складається з таких кроків:

1. Побудова характеристики. Характеристику функції MD5 можна умовно поділити на такі 4 логічні блоки (див. рисунок 3):

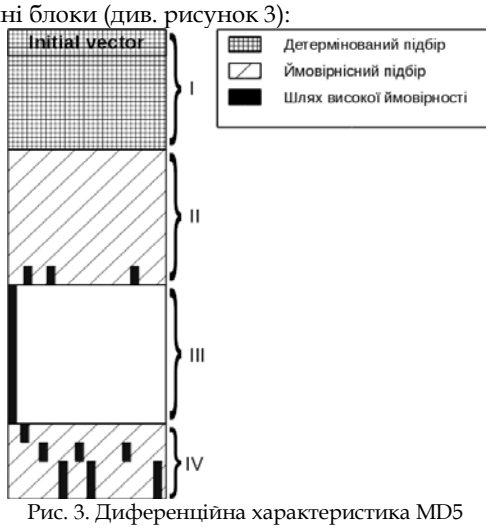

Рис. 3. Диференційна характеристика MD5

(a) Диференціали довільної ймовірності (I). Характеристика задовольняється детерміновано підбором відповідних повідомлень.

(b) Диференційний шлях (II), що поєднує блоки I та III, повинен мати якомога вищу ймовірність, оскільки задовольняється стохастично шляхом модифікації повідомлень [9, 4].

(c) Диференційний шлях (III), проходить через раундову функцію XOR танайстаршийбітстану

(MSB, the most significant bit [6]). Характеристика має фіксовану ймовірність і також задовольняється стохастично.

(d) Диференційний шлях (IV), простягається до виходу хеш-функції. Підбирається також стохастично.

2. Пошук тунелів для отриманого диференційного шляху. Тунелі дозволяють розбити характеристику на області, де ймовірнісний підбір можна проводити незалежно.

3. Власне пошук колізії, що складається з таких кроків:

(a) Вибір повідомлення таким чином, щоб задовольнялася характеристика (I).

(b) Одночасна модифікація повідомлень таким чином, щоб зберігалася характеристика (I). Підбір проводиться доки не задовольниться частина характеристики (II) до раунду дії першого тунелю.

(c) Одночасна модифікація повідомлень таким чином, щоб зберігалася характеристика (I) та (II) до раунду дії першого тунелю. Підбираються повідомлення для задоволення частини характеристики до раунду дії другого тунелю.

(d) Кроки повторюються для усіх тунелів.

(e) У випадку невдачі, усі кроки повторюються.

Максимальна ефективна колізія для алгоритму MD5 була отримана зі складністю 2^{18} (двох блокова) та 2^{41} (одно блокова)[6] .

Узагальнити диференційний пошук колізії функції хешування можна, як у випадку з блоковим шифром, у вигляді задачі розпізнавання класів ймовірнісних автоматів:

$$\left\{T_K^{'} = \left\langle Q', q_0', \zeta_k \right\rangle\right\},$$

де Q' - множина станів (диференціали раунду), q_0' - початковий стан (диференціали на вході), ζ_k - функція ймовірності переходів.

Особливістю моделі для пошуку колізії є те, що клас K відповідає не повідомленню, а лише його частині. Інша частина повідомлення використовується для модифікації та дозволяє рандомізувати роботу автомата.

Функція ймовірності переходів оцінюється теоретично на основі диференційного шляху, що використовується для атаки (для хешів на основі несбалансованих схем Фейстеля це потужність диференційного шляху з бітовими умовами). Рандомізація роботи автомату відбувається шляхом модифікації повідомлень хеш-функції з фіксованою різницею.

Тоді пошук повідомлень, що призводять до колізії, зводиться до пошуку довільного автоматузадачі розпізнавання класу автомату $T_K^{'}$ та, як наслідок, частини повідомлень, що утворюють колізії. Решта фрагментів повідомлень шукається перебором.

Диференційні характеристики хеш функцій та блокових шифрів

Диференційних аналіз блокових шифрів та функцій хешування має певні відмінності:

1. Шифри: для фіксованого невідомого значення $k \in K$ ми можемо отримати підмножину множини $\{x, E(x,k) \mid x \in X\}$ або $\{x_i, E(x_i,k)\}_{i=0..n}, x_i \in X$. Тобто, ми можемо накопичувати інформацію про секретний ключ.

Хеш: для фіксованого відомого значення $x \in X$ ми можемо отримати підмножину множини $\{h(x,k)\}_{k \in K}$. Тобто, повідомлення (ключ базового шифру) використовується один раз, немає можливості проводити накопичення інформації про нього.

2. Шифри: Диференційні характеристики можуть бути довільними, характеристика на заданих повідомленнях досягається стохастично. Задача вибору характеристики – пошук характеристики з якомога більшою ймовірністю.

Хеш: Диференційні характеристики мають обмеження на початку і кінці, досягаються частково детерміновано (метод модифікації повідомлень [9, 4]), частково – стохастично. Задача вибору характеристики – пошук характеристики, що задовольняє задані умови та з якомога більшою ймовірністю частини, що підбирається стохастично.

3. Шифри: диференціали задаються на робочих станах шифру, ключ не впливає на характеристику.

Хеш: Диференціали можуть задаватися не лише для станів хешу (аналог робочих станів шифру), але і для повідомлень (аналог ключів шифру). Тож диференціал ключа є також складовим усієї характеристики.

4. Шифри: ймовірність характеристики для марківських шифрів оцінюється як $P = \prod p_i$, де p_i – ймовірність раундового диференціалу.

Хеш: загалом, ймовірність характеристики оцінюється так само, проте з'являються області, де диференційний шлях може досягатися детерміновано шляхом модифікації повідомлень. Також з'являється можливість використання так званих "тунелів", що також підвищують ймовірність характеристики. Тоді ймовірність стохастичної частини характеристики можна оцінити як $P = \prod_i \rho_{t_i}$, де $\rho_{t_i} = 1 - (1 - \prod_{j=t_i}^{t_{i+1}} p_j)^{2^n_i}$, $\{t_i\}$ – раунд, з якого діє тунель i потужності n .

5. Шифри: атаки пошуку ключа найчастіше будуються як атаки розпізнавання відмінності від випадкового оракулу. Основна їх ідея в тому, що для окремих частин ключа накопичується інформація про те, чи є конкретне значення ключем розшифрування.

Хеш: для кожного хеш значення принципово існує велика кількість (для одноблокового MD5 це $\approx 2^{512-64-128} = 2^{320}$) прообразів, кожен з яких задовольняє аналітика. Тож атаки розпізнавання повідомлення (ключа базового шифру) не працюють. Натомість, застосовуються метод модифікації повідомлень, тунелювання [7] , зустрічі посередині для характеристик 0 та інші.

Диференціали та бітові умови

Основне мета побудови диференційного шляху (як для блокових шифрів так і для функцій

хешування) – позбавитися залежності від ключа (або повідомлення для хеш-функції). Далі спробуємо дещо формалізувати поняття "позбавлення залежності".

Якщо розглядати модель блокового шифру чи хеш-функції у вигляді автомату, то задача пошуку $M_l = \{L_k \mid L_k \supset l\}$ за множиною $l = \{x, y \mid x \in X, y \in Y\}$ є доволі складною. Іноді цю задачу можна звести до простішої з використанням диференційного аналізу. Розглянемо відкриті тексти $A, B \in X$ на вході шифру чи хешу. Після і-го раунда отримуємо певні значення $Q_i(A) \oplus k_i$ $Q_i(B) \oplus k_i$. При цьому, якщо операція $\oplus$ комутативна, ми можемо визначити операцію ! та розглядати диференціал $Q_i(A)!Q_i(B)$. Зрозуміло, що при цьому неможливо точно визначити значення $Q_{i+1}(A)!Q_{i+1}(B)$, але іноді це вдається зробити з високою ймовірністю. При цьому ми позбавляємося залежності від ключів.

Основна ідея введення диференціалу в тому, що множина найбільш ймовірних станів набагато менша ніж Q . Біль того, на вхід автомату більше не подається послідовність зв'язаних між собою символів, що іноді значно спрощує задачу розпізнавання.

Вперше бітові умови згадуються у роботі Ванга [8] присвяченій побудові колізій для функцій хешування MD5 та RIPEMD. Потім метод був узагальнений Стівенсом [4] . Для шифрів та функцій хешування, що базуються на схемі Фейстеля часто нескладно визначити ймовірності проходів диференціалів через нелінійну функцію. Наприклад блок підстановки приймає на вхід 6-бітовий вектор, тож нескладно підрахувати можливі диференціали на виході. Проте у випадку незбалансованих модифікацій, як наприклад у функції MD5, на вхід нелінійної функції подаються $32 \times 3 = 96$ бітів. Більш того, якщо на нелінійну функцію потрапляють значення зі станів i , $i+1$ та $i+2$, то відомо, що на наступному раунді туди потраплять знову стани $i+1$ та $i+2$. Тож бітові умови накладаються на ці стани, таким чином ми маємо гарантію того, що різниці на сусідніх нелінійних функціях не будуть несумісними. Отже, метод бітових умов є універсальним для незбалансованих фейстелівських схем як для функцій хешування так і для шифрів.

Характерною особливістю застосування диференційних шляхів для побудови слабких колізій для функцій хешування є наявність так званих "тунелів" [7] .

Нехай уже існує певна диференційна характеристика $\{\Delta_i\}_{i=0..n}$ та підібрані повідомлення K та K' так, що задовольняється характеристика до раунду j . Тоді іноді можна знайти таку множину пар повідомлень $\{(K_i, K_{i'})\}_{i>1}$, за якої також задовольняється характеристика $\{\Delta_i\}_{i=0..j}$. У цьому випадку, можна досягати характеристики на раундах після j ймовірнісним шляхом, при цьому не впливати на уже отримані різниці на раундах до j .

Висновки

У даній статті були досліджені відмінності та особливості застосування диференційного аналізу до фейстелівських шифрів та функцій хешування.

В роботі запропоновано узагальнення блокових шифрів та функцій хешування, як скінченних автоматів Мілі. Також запропоновані узагальнені якісні моделі атак, зокрема диференційного аналізу, для блокових шифрів та функцій хешування через задачі розпізнавання класів ймовірнісних автоматів

В результаті дослідження було показано:

1. Метою диференційного аналізу як блокових шифрів так і функцій хешування є позбавлення залежності від ключа (для шифру) та повідомлення (для хеш-функції) на раунді.

2. Головною задачею диференційного аналізу шифрів є отримання та накопичення інформації про ключ та відновлення його частинами. Задачею диференційного аналізу функцій хешування є отримання обмежень на повідомлення за яких відбувається колізія.

3. Ключ блокового шифру є, в теорії, є випадковою рівномірно розподіленою величиною. В той же час, повідомлення функції хешування часто маюсь нерівномірний розподіл (фрази природної мови, паролі, коди програм, архіви, публічні ключі сертифікатів тощо), що з одного боку зменшує кількість інформації в повідомлення (внаслідок чого зменшується простір перебору), а з іншого боку – накладає додаткові умови на диференційні шляхи (внаслідок чого доводиться відкидати характеристики високої ймовірності).

4. Метод бітових умов є універсальним методом побудови диференційної характеристики (жадібний алгоритм) для криптопримітивів, що базуються на незбалансованих схемах Фейстеля та у якості нелінійної функції використовуються бітові перетворення. Даний метод використовується для оцінки ймовірності диференціалу наступного раунду як у блокових шифрах, так і у функціях хешування на базі незбалансованої схеми Фейстеля.

5. Тунелювання є специфічний для функцій хешування метод, що дозволяє підбирати бітові умови частинами.

Література

[1] Claude E. Shannon. Communication theory of secrecy systems. The Bell System Technical Journal, 28(4):656–715, October 1949.

[2] Eli Biham & Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '90, pages 2–21, London, UK, UK, 1991. Springer-Verlag.

[3] Kazumaro Aoki and Yu Sasaki. Selected areas in cryptography. chapter Preimage Attacks on One-Block MD4, 63-Step MD5 and More, pages 103–119. Springer-Verlag, Berlin, Heidelberg, 2009.

[4] Marc Stevens, Arjen K. Lenstra & Benne de Weger. Chosen-prefix collisions for md5 and applications. IJACT, 2(4):322–359, 2012.

[5] Ralph Charles Merkle. Secrecy, authentication, and public key systems. PhD thesis, Stanford, CA, USA, 1979. AAI8001972.

[6] Tao Xie Fan, Bao Liu Deng, Guo Feng. Could the 1-msb input difference be the fastest collision attack for md5 ? Cryptology ePrint Archive, Report 2008/391, 2008. http://eprint.iacr.org/.

[7] Vlastimil Klima. Tunnels in hash functions: Md5 collisions within a minute. Cryptology ePrint Archive, Report 2006/105, 2006. http://eprint.iacr.org/.

[8] Xiaoyun Wang & Hongbo Yu. How to break md5 and other hash functions. In In EUROCRYPT. Springer-Verlag, 2005.

УДК 003.26 (045)

Кудин А.М., Коваленко Б.А. Диференциальный анализ функций хеширования и блочных шифров: обобщенный подход

Аннотация. *Методы дифференциального криптоанализа – мощные методы анализа блочных шифров. Для анализа функций хеширования, в частности функций на базе фейстелевских несбалансированных схем, также используются похожие методы. В данной статье обобщается дифференциальный анализ функций хеширования, основанных на несбалансированных схемах Фейстеля и блочных шифров на основе схем Фейстеля. Полученные результаты доказывают, что при схожести идей дифференциального анализа для блочных шифров и функций хеширования, они имеют существенные различия, благодаря которым, одинаковым параметрам безопасности отвечают разные стойкости к атакам с использованием дифференциального анализа для шифров и функций хеширования. Данные результаты также позволяют вырабатывать дополнительные ограничения на параметры безопасности при построении новых функций хеширования.*

Ключевые слова: *защита информации, функция хеширования, дифференциальный анализ, MD5, схема Фейстеля, битовый условия, метод тунелирования.*

Kudin A., Kovalenko B. Differential analysis of hash functions and block ciphers: generalized approach

Abstract. *Differential analysis approaches are powerful block cipher analysis methods. Similar methods are used for hash function analysis. This paper generalizes differential analysis of unbalanced Feistel scheme based hash functions and Feistel block ciphers. Obtained results demonstrate, despite on some similarity of differential analysis for cipher and hash functions, they have crucial differences, so the same security parameters may belong to different resistances to differential analysis of cipher and hash functions. These results allow generate additional constrictions on security parameters in hash functions which are under development now.*

Key words: *information security, hash function, differential analysis, MD5, Feistel scheme, bitconditions, tuneling method.*

Отримано *20 травня 2015 року*, затверджено редколегією *4 червня 2015 року*