УДК 004.056.55

В. І. Руженцев
Харківський національний університет радіоелектроніки,
кафедра безпеки інформаційних технологій

ПРО ОСОБЛИВОСТІ УСІЧЕНИХ ДИФЕРЕНЦІАЛІВ, ЩО ВИКОРИСТОВУЮТЬСЯ В КОЛІЗІЙНИХ АТАКАХ НА АЛГОРИТМИ ҐЕШУВАННЯ З RIJNDAEL-ПОДІБНИМИ ПЕРЕТВОРЕННЯМИ

Проаналізовано вимоги до усічених диференціалів, які використовуються в колізійних атаках на алгоритми ґешування, що використовують Rijndael-подібні шифри. Продемонстровано відмінності цих вимог та вимог до усічених диференціалів, що використовуються в атаках на блокові шифри.

Ключові слова: усічений диференціал, усічена диференційна характеристика, колізія, алгоритм ґешування, складність атаки.

The requirements to truncated differential paths used in collision attacks on hash algorithms with Rijndael-like transformations are considered. The difference between these requirements and requirements to truncated differential paths in attacks on block ciphers is demonstrated.

Key words: truncated differential, truncated differential characteristic, collision, hash algorithm, complexity of attack, rebound attack.

Вступ

Після прийняття алгоритму Rijndael як стандарту шифрування AES (FIPS-197) Rijndael-подібні шифри та окремі перетворення цього алгоритму стали поширеними елементами у багатьох нових криптопримитивах. Не є в цьому плані винятком і алгоритми ґешування. Алгоритм Whirlpool [1] є алгоритмом ґешування, прийнятий як стандарт ISO/IEC (ISO/IEC 10118-3) та використовує 512-бітний Rijndael-подібний шифр. Два алгоритми з п’яти фіналістів конкурсу SHA-3 [2]: ґеш-функції Groestl та ECHO також використовують Rijndael-подібні шифри. У межах конкурсу SHA-3 було проаналізовано криптографічні властивості подібних алгоритмів ґешування та виявлено найефективніші шляхи організації атак на алгоритми, що використовують Rijndael-подібні шифри [3–9]. У роботах [3–9] запропоновано та вдосконалено атаку “зміни напрямку” (rebound attack).Основний елемент, що використовується в усіх цих запропонованих атаках на спрощені ґеш-алгоритми, – це усічені диференційні характеристики (УДХ) (truncated differential paths) та усічені диференціали (УД) (truncated differentials).

У роботі [10] було проаналізовано УДХ та УД з погляду їх використання в диференційних атаках на блокові шифри, що мають Rijndael-подібні перетворення. Визначено структуру найефективніших УДХ та УД. Метою цієї роботи є визначення критеріїв ефективності та структури УД та УДХ, що можуть бути застосовані в колізійних атаках на алгоритми ґешування, в яких використовуються Rijndael-подібні шифри.

1. Rijndael-подібні шифри

Під Rijndael-подібними шифрами розумітимемо алгоритми шифрування, які побудовані за принципом Substitution-Permutation Network (SPN) та мають у кожному циклі аналогів перетворень шифру Rijndael чотири види перетворень: ByteSub (BS), ShiftRow(SR), MixColumns (MC) и AddKey. Ці перетворення обробляють блок даних, який представлений у вигляді матриці, де кожна клітинка - це один байт. Залежно від розміру блоку можуть змінюватися кількість та розмірність колонок цієї матриці.

BS виконує підстановку для кожного байту блоку. SR виконує циклічний зсув кожної строки матриці блоку. MC виконує множення кожного стовпця матриці на фіксовану квадратну матрицю відповідного розміру. AddKey додає цикловий ключ за допомогою операції XOR.

На рис. 1 пояснено принцип дії перетворення SR. На рис. 1 m – кількість рядків у блоці, n – кількість колонок. Коли $n \geq m$, то SR виконує циклічний зсув кожного рядка на відмінну кількість байтів. Цей вид перетворення використовується у всіх варіантах шифру Rijndael. У випадку $m > n$ деякі рядки зсуваються на однакову кількість байтів (див. рис. 1). Таку схему перетворення використано в шифрі “Калина” [12].

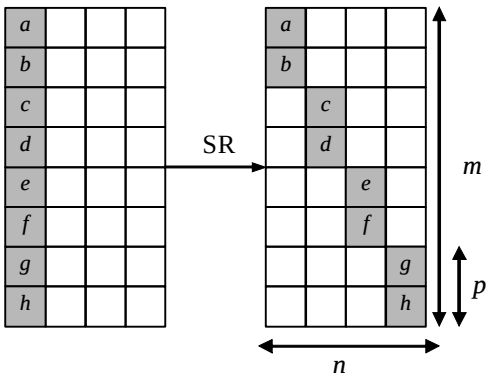

Рис. 1

2. Вимоги до УД та УДХ, що можуть бути використані в диференційних атаках на блокові шифри

Методику реалізації атаки усічених диференціалів запропонував Л. Кнудсен [11]. Відмінність від звичайної диференціальної атаки полягає в тому, що через цикли проводиться не повна різниця, а деяка її частина. Для байт-орієнтованих шифрів природним вважається вивчення усічених диференціалів особливого виду, для яких усічення полягає не у виключенні з розгляду окремих бітів вхідної чи вихідної різності, а в розгляді активності S-блоків. Оскільки S-блоки (S-підстановки), що використовуються в сучасних шифрах, найчастіше є відображеннями байт-в-байт, то диференціали, що характеризують активність S-блоків, часто називають байтовими диференціалами. У байтових диференціалах різність представляється у вигляді послідовності бітів, яку називають *вектором активізації*. Кожен біт цього вектора характеризує активність одного S-блоку (байта) (1– ненульова різниця – S-блок активний; 0 – S-блок неактивний). Надалі у цій роботі під усіченими диференціалами або диференційними характеристиками розумітимемо саме байтові диференціали або диференційні характеристики.

У літературі існує опис атак усічених (байтових) диференціалів на послаблені варіанти шифрів SAFER, E2. З цих робот можна з’ясувати, що наявність r-циклового ефективного УД дає змогу організувати атаку на r-цикловий, а в деяких випадках – і на r+1-цикловий шифр.

Основна вимога до УДХ чи УД, що використовуються в атаках на блокові шифри, – це їх ймовірність. УДХ чи УД вважаються ефективними, коли їх імовірність $P_{УДХ}$ або $P_{УД}$ більша ніж імовірність одержання на виході того самого вектора активізації за довільного (випадкового) вектора активізації на вході:

$P_{УДХ} > p_{сл}$ или $P_{УД} > p_{сл}$,

випадковий вхідний вектор активізації припускає однакову ймовірність усіх значень вихідної різниці, тобто $p_{сл} \approx \left(2^{-8}\right)^u$, де u – кількість неактивних байтів у вихідній різності або кількість нульових бітів у вихідному векторі активізації.

3. Вимоги до УД та УДХ, що можуть бути використані в колізійних атаках на алгоритми гешування

У цьому розділі на основі аналізу робіт [3–9] наведено головні вимоги до УД та УДХ, що можуть бути використані в колізійних атаках.

3.1. Умова отримання колізії з врахуванням загальної структури функції стиснення

Структура функції стиснення визначає вимоги, які буде висунуто до УД або УДХ. Наприклад, в алгоритмі Whirlpool використовується схема Miyaguchi-Preneel, яку наведено на рис. 2.

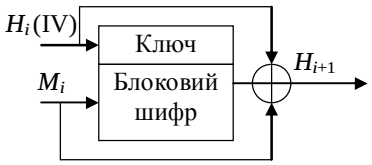

Рис. 2

У цьому випадку для побудови колізії потрібно знайти два блоки тексту M_1 та M_2, які мають однакову різність на вході і виході блокового шифру: $M_1 \oplus M_2 = E_{IV}(M_1) \oplus E_{IV}(M_2)$. Тоді ці обидва блоки матимуть однакове значення H_{i+1}, отже, їх можна додати на початку двох однакових текстів – отримані повідомлення створять колізію.

У роботі [3] описано колізійну атаку на алгоритм Whirlpool з 4 циклами перетворень у блоковому шифрі. Автори використали УДХ з такою кількістю активних байтів на межах циклів: $1 \xrightarrow{1цикл} 8 \xrightarrow{2цикл} 64 \xrightarrow{3цикл} 8 \xrightarrow{4цикл} 1$. З погляду розглянутої умови важливо, що однаковою є кількість та позиція активних байтів на вході та виході. У цій роботі ми розглянемо можливість використання УДХ зі схемою $25 \xrightarrow{1цикл} 25 \xrightarrow{2цикл} 25 \xrightarrow{3цикл} 25 \xrightarrow{4цикл} 25$, яка, як зазначено в [10], є ефективнішою в атаках на блокові шифри, адже має більшу ймовірність.

3.2. Обчислення кількості колізійних пар, що можуть бути побудовані

Для обчислення кількості колізійних пар потрібно, по-перше, визначити загальну кількість пар, яку для обраної вхідної різності можна побудувати, по-друге, помножити цю кількість на ймовірність УД чи УДХ. Докладніше цей процес описано в [4].

Загальна кількість пар, яку для обраної вхідної різності можна побудувати, визначається кількістю активних байтів на вході та розміром блоку. Для УДХ з [3] ця кількість становить $2^{8(64+1)} = 2^{520}$. Для нової УДХ: $2^{8(64+25)} = 2^{712}$.

Порядок розрахунку ймовірності УДХ для Rijndael-подібних перетворень представлено в роботах [5]. УДХ з [3] має ймовірність 2^{-512}, нова УДХ – 2^{-384}.

Також потрібно ще врахувати ймовірність повного збігу початкової та вихідної різності. Ця ймовірність визначається кількістю активних байтів у вхідній або вихідній різності. Для УДХ з [3] ця ймовірність 2^{-8}, для нової УДХ – $2^{-8*25} = 2^{-200}$.

Отже, кількість колізійних пар, що може бути побудована для відомої УДХ, 1, для нової – 2^{128}.

3.3. Обчислення складності побудови колізійної пари

Найбільші відмінності між відомою та новою УДХ стають зрозумілі саме на цьому етапі.

У роботі [3] описано спосіб побудови колізій, який названо атакою перескерування, або зміни напрямку (rebound attack). Основна ідея – починати пошук правильної пари для обраного шляху зміни різності не з початку або з кінця, а з середини багатоциклового перетворення – з місця, де відповідно до УДХ відбувається найбільше зменшення ймовірності. Це дає можливість побудувати правильну пару з меншою складністю.

У відомій УДХ найбільше зменшення ймовірності відбувається у 3-му циклі при переході 64 активних байтів у 8. Починаючи побудову правильної пари з цього місця, автори роботи [3] отримують загальну складність 2^{120}. У новій УДХ ймовірність зменшується поступово протягом усіх циклів, і побудувати правильну пару виявляється значно важче. Запропонувати алгоритм зі складністю, меншою за 2^{256}, нам не вдалося.

4. Визначення потрібної кількості циклів для блокового шифру, який використовується в алгоритмі гешування, для забезпечення захищеності від колізійної атаки "зміни напрямку" (rebound attack)

Задача визначення потрібної кількості циклів для блокового шифру, який використовується в алгоритмі гешування, для забезпечення захищеності від колізійної атаки "зміни напрямку" (rebound attack) має дуже багато деталей, серед яких розмір блоку шифру, розмір геш-коду, вигляд функції стиснення та інші. Отже, дуже складно подати розв'язок цієї задачі у загальному вигляді. Тому в цьому розділі окреслимо лише можливі шляхи вирішення окремих складових цієї задачі.

Атака "зміни напрямку" [3] використовує УДХ, яка має внутрішню (inbound) та зовнішню (outbound) частини. Розглянемо, чим визначається максимальна кількість циклів для цих частин.

4.1. Внутрішня (inbound) частина УДХ

На основі аналізу відомих робіт [3–9] можна зробити висновок, що максимальна кількість циклів, яку може покрити внутрішня (inbound) частина, становить 3 цикли. При цьому, ґрунтуючись на матеріалах тих самих робіт, побудова пар, які відповідають inbound частині, розглядається як попередній етап та не збільшує загальної складності атаки. Важливо, аби було сформовано достатню кількість пар, щоб хоча б одна задовольнила усю УДХ.

4.2. Зовнішня (outbound) частина УДХ

Значно складніше визначити обмеження за кількістю циклів для зовнішньої (outbound) частини УДХ. При цьому можна використати результати роботи [10]. Так, згідно із теоремою 2 ([10]), для Rijndael-подібних шифрів з трьома та більше циклами та зі структурою блоку, коли рядків не менше ніж стовпців ($m \geq n$) (див. рис. 1), не існує УД, ймовірність яких вища ніж $p_{сл} \approx \left(2^{-8}\right)^u$, де u – кількість неактивних байтів у вихідній різності або кількість нульових бітів у вихідному векторі активізації. Отже, ні до, ні після inbound частини УДХ не можна додати понад трьох циклів. Тобто загальна довжина УДХ не може бути більшою за 9 циклів. Але ця оцінка переважно є дуже завищеною, і у відомих атаках outbound частина складається з одного циклу на початку та одного циклу наприкінці УДХ, а загальна довжина УДХ – 5 циклів .

Висновок

У роботі розглянуто основні вимоги до усічених диференційних характеристик, що використовуються в колізійних атаках на алгоритми ґешування, в яких використовуються Rijndael-подібні перетворення. Виявлено суттєві відмінності між цими вимогами та вимогами до диференційних характеристик в атаках на блокові шифри. Продемонстровано, що найефективніші усічені диференційні характеристики в атаках на блокові шифри не є ефективними в відомих колізійних атаках. Також в роботі окреслено можливі шляхи розв'язання задачі визначення потрібної кількості циклів для блокового шифру, який використовується в алгоритмі гешування, для забезпечення захищеності від колізійної атаки "зміни напрямку" (rebound attack).

1. Paulo S. L. M. Barreto and Vincent Rijmen. The Whirlpool Hashing Function. Submitted to NESSIE, September 2000. Revised May 2003. Available online at http://www.larc.usp.br /~pbarreto/WhirlpoolPage.html (2008/12/11). 2. National Institute of Standards and Technology. Announcing Request for Candidate Algorithm Nominations for a New Cryptographic Hash Algorithm (SHA-3) Family. Federal Register, 27(212):62212-62220, November 2007. Available: http://csrc.nist.gov/ groups/ ST/hash/documents/FR_Notice_Nov07.pdf (2008/10/17). 3. Florian Mendel, Christian Rechberger, Martin Schlaffer, and Soren S. Thomsen. The Rebound Attacks: Cryptanalysis of Reduced

Whirlpool and Grostl. In Josef Pieprzyk, editor, CT-RSA, volume 5985 of LNCS, pages 350-365. Springer, 2010. 4. M. Schlaffer. Updated Differential Analysis of Grøstl. Grøstl website, January, 2011. 5. Kota Ideguchi, Elmar Tischhauser, and Bart Preneel. Improved collision attacks on the reduced-round Grostl hash function. In Information Security Conference, 2011. To appear. 6. Florian Mendel, Thomas Peyrin, Christian Rechberger, and Martin Schlaffer. Improved Cryptanalysis of the Reduced Grostl Compression Function, ECHO Permutation and AES Block Cipher. In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, Selected Areas in Cryptography, volume 5867 of LNCS, pages 16-35. Springer, 2009. 7. Thomas Peyrin. Improved Differential Attacks for ECHO and Grostl. In Tal Rabin, editor, CRYPTO, volume 6223 of LNCS, pages 370-392. Springer, 2010. 8. Gilbert, H., Peyrin, T.: Super-Sbox cryptanalysis: Improved attacks for AES-like permutations. In Hong, S., Iwata, T., eds.: Preproceedings of FSE 2010. (2010) 368–387. 9. Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta. Non-full-active Super-Sbox Analysis: Applications to ECHO and Grostl. In Masayuki Abe, editor, ASIACRYPT, volume 6477 of LNCS, pages 38–55. Springer, 2010. 10. Руженцев, В. И. Доказуемая стойкость Rijndael-подобных шифров к атаке усеченных дифференциалов. // Науково-технічний журнал: Радіоелектронні і комп'ютерні системи. – 2012. № 5. – С. 51–55. 11. 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. 12. І. Д. Горбенко, В. І. Долгов, Р. В. Олійников, В. І. Руженцев та ін. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікація // Прикладная радиоэлектроника. Тематический выпуск, посвященный проблемам обеспечения безопасности информации. – Харьков. – 2007 – Т. 6. – №2. – С. 195–208.

УДК 004.(056.53: 932)

С.М. Кущ, Д.О. Прогонов
Національний технічний університет України
"Київський політехнічний інститут"
Фізико-технічний інститут,
кафедра фізико-технічних засобів захисту інформації

АЛГОРИТМ ФОРМУВАННЯ СТЕГАНОГРАМ НА ОСНОВІ LSB-МЕТОДУ ТА ЙОГО ВИКОРИСТАННЯ ДЛЯ ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ МЕТОДІВ АКТИВНОГО СТЕГОАНАЛІЗУ

Розроблено алгоритм формування стеганограм у цифрових зображеннях на основі LSB-методу. Алгоритм дає можливість у широких межах варіювати параметри методу приховання стегоданих. Розглянуто використання запропонованого алгоритму для розроблення нових методів активного стегоаналізу.

Ключові слова: стеганографія, LSB-метод, активний стегоаналіз.

The paper discusses the development of an algorithm for data embedding into digital images according to LSB method. The algorithm allows changing the parameters of the embedding method. Application of the proposed algorithm for creating new methods of active stegoanalysis is considered.

Key words: steganography, LSB method, active stegoanalysis.

Вступ

Забезпечення надійного захисту інформації з обмеженим доступом (ІзОД), зокрема конфіденційних даних організацій та підприємств від несанкціонованого доступу сьогодні є особливо актуаль-