Дослідження криптографічного алгоритму на основі тюрмітів на відповідність лавинному критерію

Лілія Олександрівна Фадєєва, Павло Володимирович Мерзликін[0000-0002-0752-411X]

Криворізький державний педагогічний університет,
пр. Гагаріна, 54, м. Кривий Ріг, 50086, Україна
fadeyevaliliya@gmail.com, linuxoid@i.ua

Анотація. Досліджується запропонований криптографічний алгоритм на відповідність лавинному критерію. Представлено модифікацію алгоритму, що дозволяє задовольнити цей критерій без втрати інших властивостей алгоритму.

Ключові слова: криптографія, мураха Ленгтона, лавинний критерій.

The avalanche criterion satisfaction research of the turmite-based cryptographic algorithm

Liliia O. Fadieieva and Pavlo V. Merzlykin[0000-0002-0752-411X]

Kryvyi Rih State Pedagogical University, 54, Gagarin Ave., Kryvyi Rih, 50086, Ukraine
fadeyevaliliya@gmail.com, linuxoid@i.ua

Abstract. The proposed cryptographic algorithm's avalanche criterion satisfaction is examined. The algorithm's modification to satisfy the criterion without algorithm's features loss is introduced.

Keywords: cryptography, Langton's ant, avalanche criterion.

1 Вступ

Тюрмітами називають один з двовимірних різновидів машини Тюринга, найбільш відомим з яких є Мураха Ленгтона [1]. Це клітинний автомат із дуже простими правилами. Кожна квадратна клітинка двовимірного поля може мати два стани (кольори): чорний і білий. В одній із клітинок знаходиться «мураха», яка на кожному кроці може рухатися в одному з чотирьох напрямків (у клітинку, що має спільну сторону з поточною). В чорній клітинці мураха повертає на 90° вліво, змінює колір клітинки на білий і робить крок до наступної клітинки. В білій

клітинці повертає на 90° вправо, змінює колір клітинки на чорний і робить крок до наступної клітинки. Інші варіанти тюрмітів можуть мати дещо відмінні правила руху. Незважаючи на простоту правил руху, такі системи демонструють досить складну поведінку й з ними пов'язаний ряд досі відкритих математичних проблем, що виходять за рамки цієї роботи. Однак можливість застосування таких алгоритмів в криптографічних цілях (завдяки їх здатності генерувати псевдовипадкові паттерни) лишається майже поза увагою дослідників. В цьому полягає актуальність роботи.

Якщо припустити, що в ролі початкового поля виступають певні дані (наприклад, фрагмент файлу), де двом кольорам відповідають значення бітів «0» і «1»), можна зашифрувати, а згодом розшифрувати дані, знаючи кількість кроків і кінцеве положення мурахи.

Одна з найбільш успішних реалізацій криптографічного алгоритму з використанням тюрмітів [2] має такі недоліки, як обмеженість лише шифруванням зображень, а також більшу ймовірність модифікації молодших бітів, ніж старших, що може потенційно знижувати криптостійкість. З урахуванням цього, нами було запропоновано альтернативний криптографічний алгоритм з використанням тюрмітів. Його детальний огляд, оцінка швидкодії, оцінка потенційної стійкості до частотного аналізу та оптимізація параметрів алгоритму здійснені в роботі [3]. Як було показано, при достатньо великій кількості кроків одержується псевдоповипадкова послідовність байтів з рівномірним розподілом, що ускладнює можливі атаки на основі частотного аналізу.

2 Методологія

Алгоритм, представлений у даній роботі, має таку схему:

- розбиваємо файл з вхідними даними на блоки однакового розміру;
- обираємо стартові позиції тюрмітів;
- далі, згідно правил руху мурахи Ленґтона, виконуємо побітове шифрування даних.

Даний алгоритм має циклічні граничні умови, тобто, якщо тюрміт наближається до границі блоку, то переходить на протилежну сторону.

Дана робота присвячена оцінці відповідності алгоритму лавинному критерію. Для того, аби криптографічний алгоритм відповідав цьому критерію, потрібно, щоб при зміні одного біту у вхідному файлі змінювалось близько половини бітів у вихідному.

3 Обговорення результатів

На рис. 1 подано матрицю різниці бітів для двох зашифрованих файлів, що відрізнялися на один біт. Чорні клітинки позначають ті біти, що відрізняються

після застосування нашого алгоритму. Можемо бачити, що у схожих файлах після шифрування відрізняється 92 біти, що становить 18 %. Це пов'язано насамперед зі способом розбиття вихідного файлу на блоки [3]. Оскільки блоки шифруються незалежно, модифікація одного біту вплине лише на розподіл бітів у відповідному блоці. Очевидно також, що відсоток відмінних бітів буде зменшуватися зі збільшенням розміру вихідних файлів.

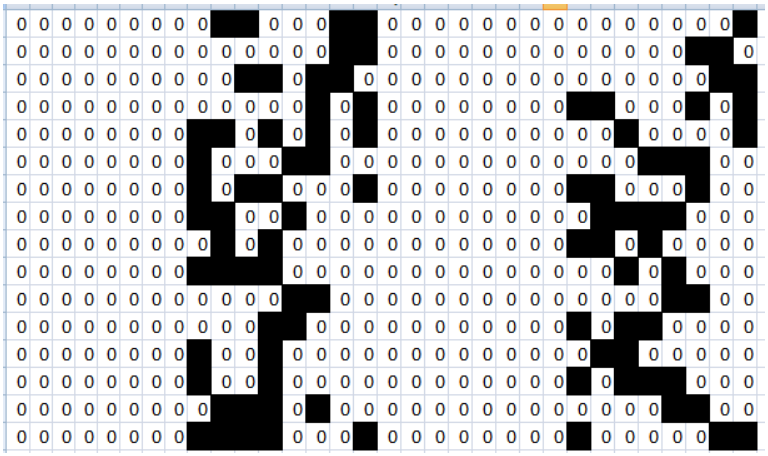

Рис. 1. Матриця різниці бітів у вихідній реалізації алгоритму

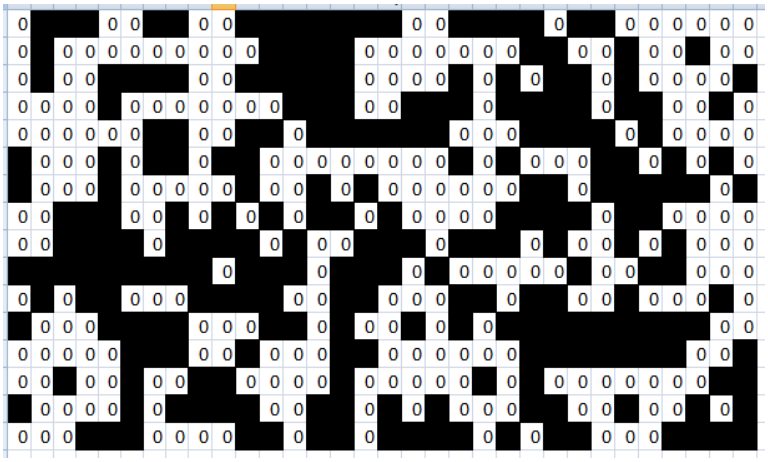

Рис. 2. Матриця різниці бітів для модифікованого алгоритму

Для вирішення цієї проблеми було внесено певні зміни в ініціалізацію початкових станів блоків. У вихідній версії алгоритму спосіб розбиття на блоки та початкове положення мурахи визначалися ключем користувача. Тобто зміна одного байту вихідного файлу впливала лише на один блок в зашифрованому

файлі. Запропонована модифікація полягає в тому, що ключ користувача впливає лише на спосіб розбиття на блоки, тоді як початкове положення й орієнтація мурахи в просторі визначаються випадково. Цей підхід видається цілком прийнятним, позаяк алгоритм є асиметричним і для дешифрування важливе кінцеве, а не початкове положення мурахи й кількість пройдених кроків. Тобто модифікація не призводить до збільшення довжини ключа й не впливає на характер розподілів бітів чи швидкодію.

Матриця різниці бітів для тих самих вихідних файлів показана на рис. 2. В зашифрованих файлах відрізняється 239 бітів, що становить 47 %. Це ілюструє відповідність алгоритму лавинному критерію. Додаткові тести на різних типах вхідних файлів показали аналогічні результати.

4 Висновки

Таким чином, запропонована модифікація алгоритму дозволяє задовольнити лавинний критерій без втрати інших його властивостей. В майбутньому планується розширити алгоритм для тюрмітів з різними правилами руху та створити модифікацію алгоритму для роботи в реальному часі, наприклад, для шифрування трафіку.

Список використаних джерел

1. Langton C. G. Studying Artificial Life with Cellular Automata / Crystopher G. Langton // Physica D: Nonlinear Phenomena. – 1986. – Vol. 22. – Iss. 1-3. – P. 120-149. – DOI : 10.1016/0167-2789(86)90237-X.
2. Wang X. A novel image encryption scheme using chaos and Langton's Ant cellular automaton / Xingyuan Wang, Dahai Xu // Nonlinear Dynamics. – 2015. – Volume 79. – Issue 4. – P. 2449-2456. – DOI : 10.1007/s11071-014-1824-0.
3. Мерзликін П. В. Криптографічний алгоритм на основі системи тюрмітів / П. В. Мерзликін, Л. О. Фадєєва, В. Ю. Іваницька, Є. Є. Іваницька // Актуальні питання забезпечення кібербезпеки та захисту інформації. – Київ : Видавництво Європейського університету, 2018. – С. 97-102.

References (translated and transliterated)

1. Langton, C.G.: Studying Artificial Life with Cellular Automata. Physica D: Nonlinear Phenomena. **22**(1–3), 120–149. (1986). doi:10.1016/0167-2789(86)90237-X
2. Wang X., Xu, D.: A novel image encryption scheme using chaos and Langton's Ant cellular automaton. Nonlinear Dynamics. **79**(4), 2449–2456 (2015). doi:10.1007/s11071-014-1824-0
3. Merzlykin, P.V., Fadieieva, L.O., Ivanytska, V.Yu., Ivanytska, Ye.Ye.: Kryptohrafichnyi alhorytm na osnovi systemy tiurmitiv (Turmites System Based Cryptography Algorithm). In: Aktualni pytannia zabezpechennia kiberbezpeky ta zakhystu informatsii, pp. 97–102. Vydavnytstvo Yevropeiskoho universytetu, Kyiv (2018)