Удосконалення та аналіз стійкості алгоритму симетричного шифрування ФБШ

Андрій Лагун[1], Олександр Поліщук[2]

Кафедра безпеки інформаційних технологій,
Національний університет "Львівська політехніка",
УКРАЇНА, м.Львів, вул.С.Бандери, 12, E-mail:
1. Lagun_ae@polynet.lviv.ua,
2. AYPolishchuk@gmail.com

This paper presents the improvements made to block encryption algorithm FBS previously presented in [1] and investigation the its cryptographically strong. This cipher is a four block Feistel network based on simple transformations, such as exclusive or, addition modulo 256 and bit shifts.

The changes primarily made in rounds function and algorithm generation rounds key to increase productivity and simplify investigation and implementation. In addition, some design features intended to protect against some types of knownattacks, such as a slide attack.

In the analysis cryptographically strong of algorithm was conducted his imitation resistance and appearance avalanche effect. To investigate the statistical properties of the algorithm was considered as a generator of pseudorandom numbers, depending on the open text blocks and key. It uses battery of statistical tests NIST and online resources www.cacert.at/random. The algorithm successfully passes all tests.

Ключові слова – криптографія, симетричні алгоритми шифрування, розробка блокових шифрів, схема Фейстеля, стійкість криптографічних алгоритмів, статистичні тести.

I. Вступ

Стрімкий розвиток засобів обчислювальної техніки і відкритих мереж, сучасні методи накопичення, обробки і передачі інформації сприяли появі загроз, пов'язаних з можливістю втрати, розкриття, модифікації даних, що належать різним користувачам. Основу забезпечення інформаційної безпеки в інформаційно-телекомунікаційних системах складають криптографічні методи і засоби захисту інформації.

Визначення ефективності криптографічних алгоритмів, як правило є складнішою задачею, ніж його проектування, оскільки воно вимагає вищого рівня знань у даній сфері і є, по своїй суті, більше науковою, ніж інженерною задачею. Це призводить до того, що існує велика кількість засобів криптографічного захисту, надійність яких не є визначеною та гарантованою, оскільки алгоритми на яких вони базуються є недостатньо або зовсім недослідженими.

Найпоширенішими криптосистемами, які використовуються для прихованого передавання інформації, є симетричні. Вони, як правило, використовують блокові шифри.

Блоковий шифр складається з простих перетворень над відкритим текстом, що виконуються в певній послідовності деяку кількість разів. Ці перетворення чи операції з відкритим текстом, чи його складовими частинами, та ключ шифрування дозволяють досягти основної мети зашифрування – усунути або істотно зменшити статистичну складову інформації та залежності відкритого тексту, тобто підвищити його ентропію, до такого значення коли між тим, що існує на вході криптоалгоритму і тим, що отримується на виході, не спостерігається зв'язку.

В роботі [1] було наведено результати проектування та дослідження алгоритму симетричного шифрування ФБШ. Проте під час подальших досліджень виявлено ряд недоліків цього алгоритму, тому в роботі буде наведено пропозиції по усуненню цих недоліків.

II. Внесені зміни та вдосконалення

У зв'язку з складністю та деякою надлишковістю структури алгоритму, а також наявністю конструктивних особливостей, що були слабкими місцями, було внесено конструктивні зміни у порівнянні з алгоритмом описаним у [1]. На даний момент структура алгоритму представляє собою багатораундове перетворення Фейстеля. Операції зашифрування та розшифрування даних можуть бути описані наступними формулами:

$$E(X)=\begin{pmatrix} X1_i = X4_{i-1} \oplus F2(X3_{i-1}, X2_{i-1}, X1_{i-1}, rK, i) \\ X2_i = X1_{i-1} \oplus F1_1(X4_{i-1}, rK, i) \\ X3_i = X2_{i-1} \oplus F1_2(X4_{i-1}, rK, i) \\ X4_i = X3_{i-1} \oplus F1_3(X4_{i-1}, rK, i) \end{pmatrix} \quad (1)$$

$$E^{-1}(X)=\begin{pmatrix} X1_i = X2_{i-1} \oplus F1(X4_i, rK, i) \\ X2_i = X3_{i-1} \oplus F1_1(X4_i, rK, i) \\ X3_i = X4_{i-1} \oplus F1_2(X4_i, rK, i) \\ X4_i = X1_{i-1} \oplus F2(X3_{i-1}, X2_{i-1}, X1_{i-1}, rK, i) \end{pmatrix} \quad (2)$$

При здійсненні операцій шифрування використовуються функції складної модифікації блоків, що забезпечують заміну та перемішування бітів вхідного блоку. Вони представлені наступним чином:

$$L(rK, X, i)=\begin{cases} i-парне, & (rK \oplus X)+(rK<<i)+(X>>i) \\ i-не\ парне, & (rK \oplus X)+(X<<i)+(rK>>i) \end{cases} \quad (3)$$

$$F1(rK, X, i)=\begin{pmatrix} (L(rK, X, i) \oplus (rK>>i))+X \\ (L(rK, X, i) \oplus (X<<i))+rK \\ (L(rK, X, i)<<i) \oplus rK \oplus X \end{pmatrix} \quad (4)$$

$$F2(rK, X, i)=(X<<i)+(rK \oplus ((rK+X)<<i)>>i) \quad (5)$$

Генерація ключів відбувається з використаням однієї з функцій складного перетворення, що застосовується при зашифруванні та розшифруванні даних, раундовий ключ залежить від вхідного ключа шифрування та номеру раунду для якого він

використовується. Механіз формування раундових ключів описується наступними формулами:

$$J = (i-1) \bmod 4 \quad (6)$$

$$K[J+1] = (X <<< i) + (rK \oplus ((rK + X) <<< i) >>> i) \quad (7)$$

$$rK(K) = K[J+1] \quad (8)$$

В порівнянні з попередньою версією [1], раундові перетворення та функції, які вони використовували були значно спрощені, що дозволяє полегшити аналіз та реалізацію алгоритму. Всі операції циклічного зсуву були замінені на операції бітового зсуву, що унеможливлює провести зворотне перетворення над операндами, оскільки ці операції відбуваються з втратою певної частини інформації.

Поєднання алгоритму формування ключів, який щоразу генерує новий раундовий ключ та операцій зсуву дозволяє запобігти здійсненню слайд атаки на даний алгоритм [3].

III.Аналіз стійкості алгоритму

Для визначення стійкості та інших криптографічних властивостей алгоритму було проведено ряд тестів.

Для атаки на шифр методом повного перебору необхідно перевірити до 2^{256} варіантів ключа.

Перевірка імітостійкості була проведена шляхом визначення впливу зміни одного з бітів у зашифрованому блоці даних на розшифрований блок. Середнє значення різниці між блоками складає близько 50% незалежно від позиції зміненого біта.

Для перевірки наявності лавинного ефекту було досліджено вплив зміни одного з бітів ключа або блоку відкритого тексту на шифротекст. Незалежно від позиції зміненого біта та його розташування (у ключі чи відкритому тексті) середнє значення змін в шифротексті становить близько 50%.

Для перевірки вищеописаних характеристик виконувалися тести з комбінаціями різних типів вхідних даних (блок відкритого тексту та ключ): повністю нульовий вектор, повністю одиничний вектор, вектор згенерований псевдовипадковим чином.

Оскільки будь-який алгоритм шифрування можна розглядати, як псевдовипадкову функцію, що залежить від вхідного тексту та ключа, то для аналізу інших статистичних характеристик шифр було протестовано різними наборами статистичних тестів. Зокрема використовувалися статистичні тести NIST (The National Institute of Standards and Technology), а також результати онлайн-тестування з допомогою ресурсу www.cacert.at/random Результати тестування наведені в Таблиці 1.

Перший тест визначає ентропію (міру невизначеності) кожного з байтів послідовності, отримане значення (7.999985) цілком задовольняє вимоги, йомовірність появи того чи іншого символу становить менше 2×10^{-4}.

Всі інші тести, з обох наборів, є різними статистичними тестами, результат яких трактується згідно методики визначення ймовірності p. При малих значеннях ймовірності послідовність вважається не випадковою, для успішного проходження ймовірність має бути вищою 0,01 [3]. Як бачимо згідно результатів пройдених тестів ймовірність більша 0,05, що є досить хорошим результатом.

ТАБЛИЦЯ 1

РЕЗУЛЬТАТИ ТЕСТУВАННЯ З ДОПОМОГОЮ СТАТИСТИЧНИХ ТЕСТІВ

№	Назва тесту	Результат
www.cacert.at/random		
1	Entropy (->8)	7.999985
2	Birthday Spacing	0.370941
3	Matrix Ranks	0.518000
4	6x8 Matrix Ranks	0.527000
5	Minimum Distance Test	0.212517
6	Random Spheres Test	0.430316
7	The Sqeeze Test	0.406954
NIST STS		
8	Frequency	0.739918
9	CumulativeSums	0.122325
10	Runs	0.122325
11	LongestRun	0.911413
12	Rank	0.350485
13	FFT	0.066882
14	NonOverlappingTemplate	0.350485
15	ApproximateEntropy	0.213309
16	Serial	0.534146
17	LinearComplexity	0.739918

Висновок

Проведені дослідження спроектованого криптографічного алгоритму на основі перетворення Фейстеля показало ефективність алгоритму, який вдало пройшов більшість статистичних тестів.

В подальших дослідженнях даного алгоритму планується більшу увагу звернути на захищеність від криптографічних атак різних типів та вдосконалення алгоритму генерації раундових ключів.

Література

[1] Поліщук О., Лагун А. Проектування блокового шифру (ФБШ) на основі перетворення Фейстеля / Матеріали V Міжнародної конференції молодих вчених CSE-2011. – Львів: Видавництво Львівської політехніки, 2011. - с. 324 - 327.

[2] M. Ciet, G. Piret, J. Quisquater (2002). Related-Key and Slide Attacks: Analysis, Connections, and Improvements.

[3] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, San Vo. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. 2010.