Розгортання Ключа для Блокових Шифрів з Псевдонедетермінованою Послідовністю Криптопримітивів

Аліна Остапенко-Боженова
кафедра захисту інформації
ВНТУ
Вінниця, Україна
asja87@gmail.com

Валентина Каплун
кафедра захисту інформації
ВНТУ
Вінниця, Україна
Chair.information.protection.vntu@gmail.com

Key expansion of pseudo non-determined block ciphers

Alina Ostapenko-Bozhenova
dept. of chair Information Protection
Vinnitsa National Technical University,
Vinnitsa, Ukraine
asja87@gmail.com

Valentyna Kaplun
dept. of chair Information Protection
Vinnitsa National Technical University,
Vinnitsa, Ukraine
Chair.information.protection.vntu@gmail.com

***Анотація*—Робота присвячена створенню методу та програмного засобу для реалізації процедури розгортання ключової інформації для блокових шифрів, що використовують псевдонедетерміновані послідовності криптопримітивів та розбиття вхідного повідомлення на блоки змінної довжини.**

***Abstract*—This work is devoted to the creation of a method and a software for procedure for key expansion for pseudo non-determined block ciphers which use breaking the input message into blocks of variable length**

Ключові слова—криптографія; блокові шифри; секретний ключ;

Keywords— cryptography; block ciphers; secret key.

I. Вступ

Одним із сучасних напрямів розробки симетричних блокових шифрів (СБШ) підвищеної швидкості є створення недетермінованих шифрів де формування алгоритмів шифрування відбувається під керуванням секретного ключа [1, 2]. Але запропоновані підходи до побудови таких СБШ мають недоліки з точки зору складності процедур передобчислень.

При розробці нових підходів до побудови СБШ для покращення їх основних характеристик проводяться дослідження процедури розгортання ключа, режимів блокового шифрування та операцій, що використовуються у функціях раундового перетворення [1, 2]. При цьому, для збільшення або підтримання заданого рівня криптостійкості СБШ практикується використання складних математичних рішень, що в свою чергу можуть збільшувати вимогу шифру до ресурсів комп'ютерної системи та зменшувати швидкість шифрування.

Змінити залежність криптографічної стійкості від складності обчислень або кількості ітерацій можливо шляхом застосування гнучких структур СБШ. Властивості яких, за використання простих та швидких операцій перетворення, дозволяють будувати блокові шифри підвищеної швидкості, що підтримують заданий світовими стандартами рівень криптографічної стійкості.

Тому у роботі [3] було запропонована модель блокових шифрів, що дозволить вносити ефект недетермінованості в складові криптографічного перетворення СБШ.

Одним з головних етапів формування криптографічного перетворення для блокових шифрів з псевдонедетермінованою послідовністю крипто примітивів (ПНБШ) є формування ознак з ключової інформації [4].

II. Основні складові криптографічного перетворення блокових шифрів

Базовим для всіх видів СБШ є підхід до шифрування блоку даних: вхідна інформація розбивається на блоки деякої розрядності які в свою чергу оброблюються функцією раунду перетворення за допомогою раундового ключа шифрування певну кількість ітерацій. Розглядаючи процес шифрування СБШ в цілому можна виділити кілька його етапів:

1. Розгортання секретного ключа.
2. Забілювання ключовою інформацією.
3. Розбиття вхідної інформації на блоки.
4. Раундові перетворення блоку даних.

Набір операцій для обробки інформації різної складності та структури утворюють функцію раундового перетворення (ФРП) СБШ. При цьому функція раунду має забезпечувати розсіювання та перемішування даних (підстановки та перестановки) згідно Шеннону [5].

Для впровадження ефекту недетермінованості в процес конструювання СБШ доцільно розглянути основні складові елементи блокового шифру. Основними з них є: оброблювана інформація, набір операцій для обробки інформації, ключ шифрування.

Тому, будь який блоковий шифр можна охарактеризувати :

- ознакою структури блоку.
- ознакою функції раунду перетворення.

Структура блоку характеризується кількістю підблоків на які розбивається блок і розрядністю цих підблоків.

Центральним поняттям для процесу перетворення інформації є блок. Вхідна інформація представлена у вигляді блоку розбивається на певну кількість частин (підблоків).

Для СБШ, раундові перетворення яких побудовані на основі мереж Фейстеля блок складається із двох або із чотирьох підблоків (мережі на дві та чотири гілки), для SP-мереж розбиття на підблоки не є очевидним, але при перетворенні (S та P блоки) блок також оброблюється частинами – підблоками, для байт-орієнтованих структур основні операції виконуються над базовими елементами – байт, рядок або стовпчик байт, для СБШ що використовують операції за модулем може бути використано розбиття блоку на підблоки, або ж блок є одним підблоком.

Виходячи з цього можна казати, що поняття блоку не є основним поняттям процесу перетворення інформації, він скоріш є інтервалом певної розмірності для зчитування інформації який вже під час основних перетворень розбивається на базові елементи СБШ – підблоки.

Отже, блок в СБШ – це набір базових елементів (підблоків) певної розмірності.

Позначимо q – кількість підблоків розрядності l. Тоді розрядність блоку M:

$$M = q \times l.$$

Наприклад:

M (мережа Фейстеля)=2×32=64 (біт);

M (мережа Фейстеля)=2×64=128 (біт);

M (розширена мережа Фейстеля)=4×32=128 (біт).

ФРП характеризується послідовністю застосувань деяких операцій із набору базових операцій. Структура блоку та ФРП можуть бути постійними або змінними в процесі шифрування.

Набір операцій, що формують ФРП СБШ загально позначимо як Q_{vp} – вид раундового перетворення. Представляючи ФРП у вигляді набору операцій недетермінованість можливо застосовувати і до її наповнення.

Ключова інформація для перетворень поточного раунду отримується з процедури розгортання секретного ключа.

Усі етапи обробки блоку даних для конкретного СБШ є строго визначеними та задаються при конструюванні, що вносить певні обмеження до його використання для комп'ютерних систем з різними параметрами ресурсів (об'ємами енергонезалежної пам'яті, обчислювальними можливостями). Таким чином бачимо, що існує кілька базових ознак побудови СБШ, деякі з них є змінними, а деякі не змінюються. Це означає, що не повною мірою використовує потенційні можливості ідей блокового шифрування для забезпечення характеристик швидкості та криптостійкості.

Базовим для всіх видів СБШ є підхід до шифрування блоку даних: вхідна інформація розбивається на блоки деякої розрядності які в свою чергу оброблюються функцією раунда перетворення за допомогою ключа відповідного раунду певну кількість ітерацій.

III. Етап формування ключової інфірмації

Одним з головних етапів формування криптографічного перетворення для блокових шифрів з псевдонедетермінованою послідовністю крипто примітивів (ПНБШ) є формування ознак з ключової інформації [4] Рис.1.

Як інструмент для процесу розгортання секретного ключа K у ПНБШ використовуються генератори псевдовипадкових послідовностей побудовані на основі регістра зсуву з лінійними зворотними зв'язками [5]. Секретний ключ K визначає не лише початковий стан регістру зсуву, а і його структуру, задаючи твірний поліном.

Формування криптографічного перетворення для раунду ПНБШ передбачає використання трьох видів ознак [3]:

- кількість підблоків Q_{pb};
- розрядність підблоку Q_{rb} (біт);
- вид структури перетворення Q_{vp},

набір конкретних значень яких характеризує вигляд раундового перетворення.

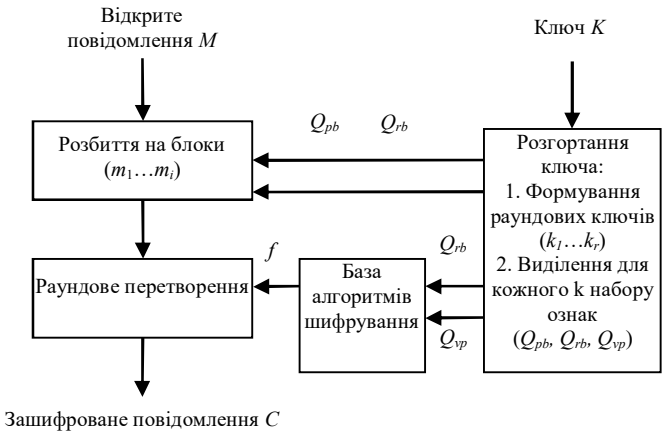

Рис. 1. Схема криптографічного перетворення ПНБШ.

Отже, можна казати що раунд перетворення блоку даних блокового шифру може бути однозначно заданий сукупністю розглянутих показників:

$$P = \{k, Q_{pb}, Q_{rb}, Q_{vp}\}.$$

Виділення ознак на кожному етапі відбувається з використанням ключа k відповідного раунду, що був сформований як поточний стан регістру зсуву побудованого на основі K.

Наприклад, для ключа $k = 128$ біт ця процедура може бути представлена послідовністю дій:

1. Раундовий ключ k розбивається на підблоки по 8 біт $(K1 \ldots K16)$. Код ознаки виду перетворення Q_{vp} обраховується шляхом використання так званої «процедури згортки»:

$$Q_{vp} = (K1 + K2 + \ldots + K16) \bmod 256.$$

В результаті, значення отриманого блоку (8 біт) визначає номер $(0 \div 255)$ алгоритму шифрування із бази, що містить перелік алгоритмів, відповідних до кількості підблоків Q_{pb} формованого блоку.

2. Блок Q_{vp} в свою чергу розбивається на підблоки по 2 біта $(Q1 \ldots Q4)$. Використовуючи вищеописану методику, визначається код ознаки кількості підблоків Q_{pb}:

$$Q_{pb} = (Q1 + \ldots Q4) \bmod 4.$$

Визначення кількості підблоків відповідно до отриманого коду ознаки Q_{pb} наведено в табл.1.

ТАБЛИЦЯ I. ВІДПОВІДНІСТЬ КІЛЬКОСТІ ПІДБЛОКІВ КОДУ ОЗНАКИ КІЛЬКОСТІ ПІДБЛОКІВ

Код ознаки Q_{pb}	00	01	10	11
Кількість під блоків (шт)	2	3	4	5

3. Шляхом циклічного зсуву на 1 біт вліво отриманого у п.п. 1 блоку Q_{vp} утворюється блок $\overrightarrow{Q_{vp}}$, що додається до Q_{vp} за mod 2 в результаті чого формується Q^*:

$$Q^* = Q_{vp} \oplus \overrightarrow{Q_{vp}}.$$

4. Отриманий блок Q^* розбивається на підблоки по 2 біта $(Q^*1 \ldots Q^*4)$ та визначається код ознаки розрядності підблоку Q_{rb}:

$$Q_{rb} = (Q^*1 + \ldots + Q^*4) \bmod 4.$$

Значення розрядності підблоку відповідно до коду ознаки Q_{rb} наведено у табл.2.

ТАБЛИЦЯ II. ВІДПОВІДНІСТЬ РОЗРЯДНОСТІ ПІДБЛОКУ КОДУ ОЗНАКИ РОЗРЯДНОСТІ ПІДБЛОКУ

Код ознаки Q_{rb}	00	01	10	11
Розрядність підблоку (біт)	8	16	32	64

Можливі значення ознаки Q_{pb} та Q_{rb} є рівноймовірними і забезпечують формування блоків різної довжини для різних раундів шифрування.

Діапазон значення ознак дозволяють представити 16 можливих комбінацій структур блоку. Так мінімальне значення розрядності блоку $m_{b\min}$, при структурі із 2 підблоків розрядністю 8 біт:

$$m_{b\min} = 2 \times 18 = 36 \text{ (біт)},$$

а максимальне значення розрядності блоку $m_{b\max}$, структура 5 підблоків розрядністю по 64 біта:

$$m_{b\max} = 5 \times 64 = 320 \text{ (біт)}.$$

Враховуючи діапазон значень ознаки виду криптографічного перетворення Q_{vp} ПНБШ, для одного раунду може бути побудовано 4096 різних модифікацій алгоритмів шифрування.

В результаті виконання розглянутого етапу криптографічного перетворення було отримано набір ознак для формування раунду ПНБШ.

IV. ПРОГРАМНИЙ ЗАСІБ ДЛЯ ГЕНЕРУВАННЯ КЛЮЧОВОЇ ІНФОРМАЦІЇ

Метою створення програмного засобу є практична реалізація одного з етапів криптографічного перетворення

запропонованої моделі ПНБШ [3], проведення тестування з формуванням ознак для ключової інформації різного розміру.

Таким чином проектований програмний засіб має розв'язувати такі задачі:

- генерування вхідних даних (секретний ключ різної довжини 64-1024 біт);
- формування генератора псевдовипадкових послідовностей на основі K;
- формування множини раундових ключів k;
- виділення набору ознак для побудови перетворення раундуПНБШ;
- побудова криптоперетворення блокового шифру (візуалізація результату).
- тестування отриманих результатів.

Вихідними результатами роботи програми є:

- «k» – набір раундових ключів;
- «Набір ознак Q_{pb}, Q_{rb}, Q_{vp}» – визначені ключові параметри для відповідного перетворення;
- «Вигляд перетворення ПНБШ» та «Мнемонічний опис перетворення ПНБШ» – відповідне графічне та мнемонічне представлення опису раунду перетворення.

Висновки

Було розглянуто формування ключових ознак раунду перетворення блокових шифрів для впровадження ефекту недетермінованості в процес конструювання нового виду СБШ, модель яких представлена у роботі [3].

Алгоритм шифрування таких блокових шифрів складається з відомих операцій, але порядок їх застосування та структура оброблюваних ним блоків визначається секретним ключем.

В той же час можливість створення ПНБШ великої кількості модифікацій алгоритмів шифрування для кожного раунду криптоперетворення, теоретично робить неможливим попередні статистичні дослідження.

На основі отриманих теоретичних результатів розроблено програмний засіб для генерування ключової формації, що може бути використано як базовий модуль програмної реалізації запропонованого методу блокового шифрування (ПНБШ).

Література References

[1] B.Schneier. Applied Cryptography.- John Wiley & Sons Inc., N.Y. 1996.-757 p.

[2] Молдовян Н.А. Скоростные блочные шифры.- СПб, СПбГУ, 1998.- 212 с.

[3] Лужецький В. А. Блочний шифр на основі псевдонедетермінованих послідовностей криптопримітивів / В .А. Лужецький, А. В. Остапенко // Наукові праці ВНТУ. – № 4 (2010). – Режим доступу до статті: http://www.nbuv.gov.ua

[4] Остапенко А. В. Криптографічне перетворення ПНБШ Тези доповідей П'ятої Міжнародної науково-практичної конференції «Інформаційні технології та комп'ютерна інженерія» м. Івано-Франківськ, 27-29 травня 2015 року. – Івано-Франківськ: Супрун В.П., 2015. – С. 187-188.

[5] Шеннон К. Работы по теории информации и кибернетики. – М., 1963. – 829 с.

[6] Иванов М.А. Теория, применение и оценка качества генераторов / М.А. Иванов, И.В. Чугунков – М.:КУДИЦ-ПРЕСС, 2003. – 240 с.