Криптографічне перетворення псевдонедетермінованих блокових шифрів

Остапенко А. В.

Асист. кафедри Захисту інформації, Вінницький національний технічний університет
Хмельницьке шосе 95, м. Вінниця, Україна, asja87@gmail.com

***Анотація* — Обґрунтовано актуальність розробки симетричних блокових шифрів підвищеної швидкості. Запропоновано застосування псевдонедетермінованої послідовності перетворення даних для побудови блокових шифрів. Визначено основні етапи побудови криптографічного перетворення для блокових шифрів, що використовують псевдонедетерміновану послідовність криптопримітивів. Запропоновано схему формування функцій раундового перетворення для досліджуваних блокових шифрів.**

Ключові слова: шифрування, блоковий шифр, криптографічне перетворення.

Cryptographic transformation pseudo non-determined block ciphers

Ostapenko A.V.

Asist., Information Protection Chair , Vinnytsia national technical university
95 Khmelnytske shose, Vinnytsia, Ukraine, asja87@ gmail.com

***Abstract* — Application actuality development symmetric block ciphers speed boos. Proposed use of pseudo non-determined sequence data conversion for the construction of block ciphers. The basic steps for building a cryptographic transformation of block ciphers that use pseudo non-determined sequence of crypto primitives. The scheme forming conversion functions for researched block ciphers**

Keywords: encryption, block cipher,cryptographic transformation.

I. Вступ

Актуальність розробки симетричних блокових шифрів (СБШ) підвищеної швидкості полягає в можливості вирішити проблему створення високоефективних засобів захисту інформації працюючих в масштабі реального часу [1].

Результати проведеного аналізу відомих СБШ [2], розкривають проблему взаємозв'язку їх основних характеристик, яка полягає в тому, що методи забезпечення необхідного рівня криптографічної стійкості призводять до зменшення швидкості шифрування. Для вирішення даної задачі при розробці СБШ, пропонуються використовувати псевдонедетерміновану послідовність перетворень даних [3].

II. Криптографічне перетворення

Будь який блоковий шифр можна охарактеризувати :

1. Ознакою структури блоку.
2. Ознакою функції раунда перетворення (ФРП).

Структура блоку характеризується кількістю підблоків на які розбивається блок і розрядністю цих підблоків. ФРП характеризується послідовністю застосувань операцій із набору базових операцій. Структура блоку та ФРП можуть бути постійними або змінними в процесі шифрування.

У роботі [3] запропоновано модель блокових шифрів, що дозволяє вносити ефект недетермінованості в значення вищенаведених ознак при шифруванні даних. Перетворення блокових шифрів, що використовують псевдонедетерміновану послідовність криптопримітивів (ПНБШ) будуються на елементарних операціях, які найбільш просто та швидко реалізуються в сучасних мікропроцесорах, що обумовлює швидкість їх виконання. В той же час можливість створення ПНБШ великої кількості модифікацій алгоритмів шифрування теоретично робить неможливим попередні статистичні дослідження.

Побудову криптографічного перетворення для ПНБШ можна розділити на 3 етапи:

1. Етап формування ознак з ключової інформації:
   - розгортання секретного ключа K та виділення раундових ключів $(k_1 \dots k_r)$;
   - виділення з раундового ключа k відповідного набору ознак: кількість підблоків Q_{pb}; розрядність підблоку Q_{rb} (біт); Q_{vp} вид ФРП.
2. Етап формування структури блоку:

- розбиття вхідного повідомлення (M) на блоки $(m_1 \dots m_i)$ розрядністю (N_b), що визначається ознаками Q_{pb}, Q_{rb} :

3. Етап вибору виду ФРП:

- вибір за ознакою Q_{vp} функції раундового перетворення із бази, відповідної Q_{pb}.

Етапи формування ознак та структури блоку детально розглянуті у роботі [3]. Запропонований діапазон можливих значень ознак [3] дозволяє будувати блокові шифри із змінною довжиною блоку та розбивати блок на непарну кількість підблоків, на відміну від загальновідомих СБШ.

Етап вибору виду функції раундового перетворення передбачає попереднє формування наборів алгоритмів шифрування відповідно до можливих значень кількості підблоків (визначених значенням Q_{pb}), що включає :

- формування набору базових операцій;
- формування механізму комбінування базових операцій у алгоритми шифрування;
- тестування алгоритмів шифрування;
- формування бази алгоритмів шифрування.

Алгоритми шифрування будуються на основі набору базових операцій, що сформована та детально описана в роботі [3].

Вимоги до побудови алгоритмів шифрування випливають із поняття стійкості шифру, яка забезпечується принципами розсіювання та перемішування [4]. Для досягнення збільшення швидкості шифрування, із збереженням властивості розсіювання, запропоновано використовувати послідовне виконання трьох операційних шарів. Шар перестановки PR є обов'язковим для кожного сформованого алгоритму. Процес побудови шару алгоритмів шифрування складається із двох фаз: фази вибору структури шару (Str); фази наповнення структури базовими операціями. Представимо загальну схему формування алгоритмів шифрування (рис.1).

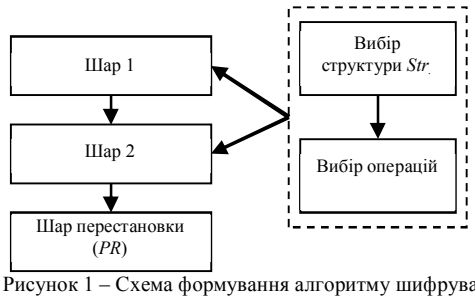

Рисунок 1 – Схема формування алгоритму шифрування

Для множини базових операцій ПНБШ запропоновано використання двох видів операцій: двоопераднді (виконуються над двома підблоками даних) та одноопераднді (виконуються над одним підблоком даних). Тому, задача вибору структури шару полягає у виборі комбінації одно- та двоопераднди операцій для відповідного значення ознаки Q_{pb}. Для цього значення Q_{pb} (N) представимо як:

$$N = 2 \cdot D + 1 \cdot O,$$

$$D = \left\lceil \frac{N}{2} \right\rceil, D = 0 \div \left\lceil \frac{N}{2} \right\rceil,$$

$$O = N - 2 \cdot D,$$

де D - двоопераднді операції; O - одноопераднді операції.

Визначення структур перетворення та запропонований варіант їх мнемонічного опису дозволяє створити механізм для формування великої кількості алгоритмів шифрування. В подальшому сформовані алгоритми проходять тестування на відповідність вимогам стійкості.

В результаті виконання попереднього етапу відбувається формування бази алгоритмів шифрування, що складається із наборів ФРП для кожного значення ознаки кількості підблоків.

III. Висновки

Застосування псевдонедетермінованих перетворень даних для побудови блокових шифрів дозволяє досягти рівня криптографічної стійкості сучасних СБШ. Стійкість таких шифрів забезпечується, на відміну від існуючих, не складністю ФРП, а невизначеним порядком їх застосування (з точки зору зловмисника) та змінною структурою оброблюваної інформації, тому зникає потреба у використанні складних обчислень. Перетворення будуються на базі елементарних операцій, які найбільш просто та швидко реалізуються в сучасних мікропроцесорах, що обумовлює швидкість їх виконання. При цьому можливість створення ними великої кількості модифікацій алгоритму шифрування теоретично робить неможливим попередні статистичні дослідження, які є базовими для найпотужніших методів криптографічного аналізу.

[1] Молдовян Н. А. Скоростные блочные шифры / Н. А. Молдовян. – СПб.:Издательство СПбГУ, 1998. – 230 с.

[2] Лужецький В. А. Аналіз алгоритмів симетричного блокового шифрування / В .А. Лужецький, А. В. Остапенко // Інформаційні технології та комп'ютерна інженерія. – 2012. – № 3. – С. 55-64.

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

[4] Шеннон К. Работы по теории информации и кибернетике / К. Шеннон ; пер. с англ. – М.: Изд-во иностранной литературы, 1963. – 830 с.