УДК 681.3.06

О. М. Бевз
Б. В. Кримчук

ПІДВИЩЕННЯ ШВИДКОСТІ РОБОТИ БЛОЧНИХ ШИФРІВ

Вінницький національний технічний університет

Анотація

Запропоновано спосіб підвищення швидкості роботи блочних шифрів, який використовує паралельні обчислення для визначення результатів роботи блоків підстановки.

Ключові слова: Блочний шифр, блоки підстановки (S-бокси), високонелінійна булева функція, паралельні обчислення, потоки операційної системи, час виконання перетворення.

Abstract

The mode of increasing produce block cipher is presented. This method exploit parallel thread for finding result of substitution box for block cipher.

Keywords: Block cipher, substitution box, high-level-non-linear Boolean function, parallel computation, threads of operation system, time of working function.

Вступ

Сучасний стан розвитку інформаційних систем характеризується зростанням об`єму передавання інформації та зростанням швидкості передавання інформації в локальних та глобальних мережах. З іншого боку, кількість несанкціонованих спроб доступу до конфіденційної інформації також зростає. По цій причині формування та реалізація в комп`ютерних системах та мережах блочних шифрів, які мають високу криптостійкість та швидку реалізацію є актуальною задачею.

Метою роботи є розроблення способу реалізації криптографічного перетворення (блоків підстановки), що характеризується високою криптостійкістю та швидкою реалізацію.

Результати дослідження

Перевіреним способом унеможливлення спроб несанкціонованого доступу - є використання блочних шифрів. Одним з компонентів блочних шифрів є блоки підстановки (S-бокси) [1]. Головним та критичним фактором S-боксу, що забезпечує криптостійкість, є високий ступінь нелінійності. Використання високоненелінійних булевих функцій дає можливість задовольнити цю вимогу. В роботі пропонується використовувати в якості високонелінійної функції комбінацію бент-функції від шести змінних та афінної функції від двох змінних [2]. Розмір вхідних блоків сучасних блочних шифрів складає 64, 128, 192 та 256 біт. При роботі блочних шифрів виконується розподілення вхідного блоку на підблоки, розмір яких становить у сучасних шифрах 8 біт. Далі ці підблоки перетворюються S-боксами. Обчислення результатів роботи одного S-боксу не залежить від обчислення результатів роботи інших S-боксів. Тому обчислення результатів роботи кожного S-боксу може бути виконано незалежно від результатів інших S-боксів з використанням окремого потоку операційної системи. Кількість таких потоків буде дорівнювати кількості S-боксів. Проведені комп`ютерні експерименти продемонстрували, що необхідний час для перетворення вхідного блоку, що складається з восьми S-боксів на основі високонелінійної булевої функції, в середньому становить 6,4 мілісекунд у випадку використання восьми потоків, що працюють паралельно. Якщо перетворення такого блоку виконується послідовно одним потоком то час перетворення складає 10,3 мілісекунд. Комп`ютерні експерименти були проведені в 64-ох розрядній операційній системі Windows 10 Pro на процесорі Intel Core i5-3230M з обсягом оперативної пам`яті 6 ГБ.

Висновки

Запропонований спосіб паралельного обчислення, який реалізується восьмома паралельними потоками, для здійснення перетворень S-боксів на основі високонелінійних бульових функцій дає можливість збільшити швидкодію в середньому на 30% в порівнянні з послідовним виконанням перетворень таких S-боксів одним потоком.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайер – М.: Триумф, 2002. – 816 с.

2. Бевз О. М. Кореляційні та диференційні властивості S-боксів на основі високонелінійних функцій / О. М. Бевз // Інформаційні технології та комп'ютерна інженерія. № 1(5). – 2006. – С. 154-158.

Кримчук Богдан Валерійович — студент групи 1СІ-13б, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця.

Науковий керівник: ***Бевз Олександр Миколайович*** — доцент кафедри автоматики та інформаційно-вимірювальної техніки, Вінницький національний технічний університет, м. Вінниця

Krymchuk B. V. — student group 1SI-13b, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Bevz O. M.*** associate Professor, Department of automation and information-measuring equipment, Vinnytsia National Technical University, Vinnytsia.