УДК 004.056.55

О. М. Бевз
М. В. Барабан
Б. В. Кримчук

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ РЕАЛІЗАЦІЇ ОБЧИСЛЕННЯ НЕЛІНІЙНОГО ПЕРЕТВОРЕННЯ БЛОЧНИХ ШИФРІВ В КОМПЮТЕРНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

Запропоновано спосіб підвищення швидкодії блочного шифру. Метод базується на використанні паралельних обчислень блоків підстановки на основі високонелінійних булевих функцій.

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

Abstract

The mode of increasing produce block cipher is presented. This method is based on parallel thread for finding the result of substitution box for a block cipher.

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

Вступ

У сучасних умовах захист інформації стає все більш складною і одночасно гострою проблемою. Це пов'язано з масовим поширенням методів і засобів несанкціонованого доступу до інформації. У зв'язку з цим необхідно застосовувати підходи, які дозволяють уникнути отримання конфіденційних даних сторонніми особами. Одним з перевірених засобів захисту інформації є блочний шифр. Сучасний блочний шифр представляє собою перетворення з певною кількістю ітерацій. Кожне з таких перетворень, що відбуваються в одній ітерацій має відповідати концепції Шеннона – забезпечувати розповсюдження та розсіювання.

Результати дослідження

Реалізація розсіювання виконується блоками підстановки (Substitution box – S-бокс)[1]. Нелінійні бульові функції у випадку застосування в S-боксах забезпечують ефективну протидію проти лінійного та диференційного аналізу. По тій причині, що сучасні комп'ютерні системи базуються на багатоядерних процесорах, а кожне ядро можна умовно представити як окремий процесор, доцільно виконати обчислення результату нелінійної бульової функції з використанням декількох потоків. Кожний такий потік має бути виконаний на окремому ядрі процесора комп'ютерної системи.

Одним з варіантів нелінійної булевої функції, що може бути використана у S-боксах є функція наступного виду (1).

$$Y = X_0 \oplus X_1 \oplus (X_1 \oplus X_2)(X_1 \oplus X_3) \oplus (X_1 \oplus X_4)(X_1 \oplus X_5) \oplus (X_1 \oplus X_6) \\ (X_1 \oplus X_7)(X_1 \oplus X_3) \oplus (X_1 \oplus X_5)(X_1 \oplus X_7) \quad (1)$$

Провівши аналіз даної функції визначено, що певні її складові не залежать один від одного, і тому можуть бути обраховані окремо один від одного, тобто паралельно на різних процесорах. Провівши

аналіз за допомогою теорії графів було визначено, що для паралельного обчислення найбільш ефективний паралельний розрахунок має бути виконаний на комп'ютерній системі з кількістю процесорів не меншою за 8 [2].

Після проведених розрахунків було визначено, що ефективність обчислення S-боксу, який базується на наведеній вище високонелінійній булевій функції (1), на комп'ютерній системі з кількістю процесорів 8 буде підвищена на 19-50%, а прискорення буде підвищено на 50-90% в порівнянні з комп'ютерною системою, яка буде складатися з одного процесора і виконувати послідовне обчислення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. 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.

2. Б. В. Кузьменко, О.А.Чайковська. Технологія розподілених систем та паралельних обчислень. Навчальний посібник. – К.: Видавничий центр КНУКІМ, 2011 – 126 с.

Кримчук Богдан Валерійович — магістрант групи 1АКІТ-17М, факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, Вінниця, e-mail: krymchuk.bogdan@gmail.com.

Барабан Марія Володимирівна канд. техн. наук., старший викладач кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, Вінниця, Україна.

Науковий керівник: ***Бевз Олександр Миколайович*** — канд. техн. наук. доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця

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

Baraban M. V. — Cand. Sc. (Eng), Assistant Professor of automation and information-measuring equipment, Vinnytsia National Technical University, Vinnytsia.

Supervisor: ***Bevz O. M.*** Cand. Sc. (Eng), Assistant Professor of automation and information-measuring equipment, Vinnytsia National Technical University, Vinnytsia.