



УКРАЇНА

(19) UA

(11) 18443

(13) U

(51) МПК (2006)  
G09C 1/00МІНІСТЕРСТВО ОСВІТИ  
І НАУКИ УКРАЇНИДЕРЖАВНИЙ ДЕПАРТАМЕНТ  
ІНТЕЛЕКТУАЛЬНОЇ  
ВЛАСНОСТІОПИС  
ДО ПАТЕНТУ  
НА КОРИСНУ МОДЕЛЬвидається під  
відповідальність  
власника  
патенту

## (54) СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

1

2

(21) u200604358

(22) 18.04.2006

(24) 15.11.2006

(46) 15.11.2006, Бюл. № 11, 2006 р.

(72) Білецький Анатолій Якович, Білецький Олександр Анатолійович, Кузнецов Олександр Анатолійович, Юкальчук Андрій Анатолійович

(73) НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

(57) Спосіб криптографічного перетворення інформації, який полягає в тому, що інформаційну послідовність подають у вигляді 128 бітових блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців

(блоків MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв, який **відрізняється** тим, що як S-блок виступає змінна матриця підстановок, що будують отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  з операціями по модулю незвідного багаточлена  $g(x)$  та шляхом виконання афінного перетворення  $y=M \cdot x^{-1} + b$  над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як незвідний багаточлен  $g(x)$  використовують змінні багаточлени, які вибирають відповідно до значення циклового ключа.

Запропонована корисна модель відноситься до галузі криптографічного захисту інформації і може бути використана в засобах шифрування у системах обробки інформації для розширення їх можливостей.

Відомий спосіб криптографічного перетворення [1], який ґрунтується на тому, що інформаційна послідовність подається у вигляді 64 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: перестановка (permutation) - за допомогою блоків перестановок (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв. Ітеративна обробка полягає у багаторазовому виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою P-блоків) та перемішування (за допомогою S-блоків) інформаційних даних.

Недоліком цього способу є те, що для криптографічного перетворення інформації у якості S-блоку виступає фіксована матриця підстановок, що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Найбільш близьким, до запропонованого технічним рішенням, обраним як прототип, є удосконалений спосіб криптографічного перетворення [2], який ґрунтується на тому, що інформаційна

послідовність подається у вигляді 128 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців (блоків MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв. Ітеративна обробка полягає у багаторазовому виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою блоків MixColumn) та перемішування (за допомогою S-блоків) інформаційних даних.

Підстановка

$$x=\{x_0, x_1, \dots, x_7\} \rightarrow y=\{y_0, y_1, \dots, y_7\}$$

представляє собою нелінійну заміну байт, яка виконується незалежно для кожного вхідного байта  $x=\{x_0, x_1, \dots, x_7\}$ . Матриці підстановки, за допомогою яких будуються S-блоки є інвертуємими матрицями, що утворюються із використанням композиції двох перетворень:

1. Отримання мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$ , яке будується за кільцем многочленів з операціями по модулю незвідного многочлену

$$g(x)=x^8+x^4+x^3+x+1; (1)$$

При цьому приймається, що якщо  $x=0$ , то  $x^{-1}=0$ .

2. Виконання афінного перетворення над примітивним двійковим полем Галуа  $GF(2)$ , яке зада-

(19) UA (11) 18443 (13) U

ється виразом:

$$y = M \cdot x^{-1} + \beta, (2)$$

де  $M$  - фіксована матриця восьмого порядку, симетрична відносно допоміжної діагоналі:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix};$$

$\beta$  - восьмиразрядний вектор-стовпець:

$$\beta = [1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 1 \ 0]^T.$$

Недоліком цього способу є те, що для криптографічного перетворення інформації у якості S-блоку виступає фіксована матриця підстановок, яка задається отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  по модулю фіксованого незвідного многочлену (1), що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

В основу корисної моделі поставлена задача створити спосіб криптографічного перетворення інформації, який за рахунок використання у якості S-блоку динамічно змінюємих матриць підстановок, які задаються отриманням мультиплікативно зворотних елементів  $x^{-1}$  над розширеними кінцевими полями Галуа  $GF(2^8)$  по модулю змінних незвідних многочленів  $g(x)$ , які обираються відповідно до значення циклового ключа.

Технічний результат, який може бути отриманий при здійсненні корисної моделі полягає в отриманні можливості гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Сутність запропонованого способу криптографічного перетворення інформації полягає в тому, що інформаційна послідовність подається у вигляді 128 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: мікшування (mix) - за допомогою блоків мікшування стовпців (блоків MixColumn); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 - за допомогою відповідних пристроїв. У якості S-блоку виступає змінна матриця підстановок, що будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  з операціями по модулю незвідного многочлену  $g(x)$  та шляхом виконання афінного перетворення (1) над

примітивним двійковим полем Галуа  $GF(2)$ , при цьому у якості незвідного многочлену  $g(x)$  використовуються змінні многочлени, які обираються відповідно до значення циклового ключа.

Цикловий ключ виробляється із ключа шифрування за допомогою алгоритму вироблення ключів. Довжина циклового ключа дорівнює довжині блоку. Циклові ключі генеруються із ключа шифрування за допомогою розширення ключа. Розширений ключ являє собою лінійний масив 4-х байтових слів. Тобто на кожній ітерації криптографічного перетворення для формування S-блоку використовуються змінні незвідні многочлени  $g(x)$ , які можуть обиратися з 4-х байтових слів розширеного ключа довільним способом, наприклад шляхом використання першого байта циклового ключа. Це надає змогу у процесі криптографічного перетворення гнучко змінювати матрицю підстановки та, відповідно, динамічно керувати процесом перемішування інформаційних даних.

Заміна незвідного многочлену  $g(x)$  приводить до ізоморфного відображення елементів розширеного кінцевого поля Галуа  $GF(2^8)$ . Головний показник ефективності блоків підстановок - показник нелінійності криптографічного перетворення є інваріантним до ізоморфного відображення. Отже показник нелінійності перетворення, що виконується за допомогою сформованих S-блоків, дорівнює показнику нелінійності у способі-прототипі. Отак запропоноване технічне рішення дозволяє виконувати криптографічне перетворення даних гнучко змінюючи таблиці підстановок із фіксованим показником нелінійності та динамічно керувати ітеративною обробкою інформаційних даних.

Таким чином, за рахунок використання змінних незвідних многочленів  $g(x)$  вдається на кожній ітерації криптографічного перетворення інформації застосовувати у якості S-блоку динамічно змінюємі матриці підстановки, що дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних.

Джерела інформації:

1. National Institute of Standards and Technology, "FIPS-46-3: Data Encryption Standard." Oct. 1999. Available at <http://csrc.nist.gov/publications/fips/> <http://csrc.mst.gov/publications/fips/fips46-3/fips46-3.pdf>
2. National Institute of Standards and Technology, "FIPS-197: Advanced Encryption Standard." Nov. 2001. Available at <http://csrc.nist.gov/publications/fips/> <http://csrc.nist.gov/publications/fips/fips197/fips197.pdf>