



УКРАЇНА

(19) **UA** (11) **144137** (13) **U**  
(51) МПК (2020.01)  
**G09C 1/00**  
**G06F 21/60** (2013.01)  
**G06F 21/72** (2013.01)  
**H04L 9/00**

МІНІСТЕРСТВО РОЗВИТКУ  
ЕКОНОМІКИ, ТОРГІВЛІ ТА  
СІЛЬСЬКОГО ГОСПОДАРСТВА  
УКРАЇНИ

## (12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: <b>u 2020 00526</b>	(72) Винахідник(и): <b>Білецький Анатолій Якович (UA),</b> <b>Навроцький Денис Олександрович (UA)</b>
(22) Дата подання заявки: <b>29.01.2020</b>	(73) Власник(и): <b>НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ</b> <b>УНІВЕРСИТЕТ,</b>
(24) Дата, з якої є чинними права на корисну модель: <b>11.09.2020</b>	просп. Комарова, 1, м. Київ, 03058 (UA)
(46) Публікація відомостей про видачу патенту: <b>10.09.2020, Бюл.№ 17</b>	

## (54) СПОСІБ КРИПТОГРАФІЧНОГО ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

### (57) Реферат:

Спосіб криптографічного перетворення інформації полягає в тому, що інформаційну послідовність подають у вигляді бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, підстановка (substitution) - за допомогою блоків підстановок (S-блоків); перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); функціональні операції ковзного кодування (SlidCode) - за допомогою змішаних кодів Грея. Бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків), як S-блок формують змінну тривимірну матрицю підстановок, що будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення  $y=M \cdot x^{-1} + \beta$  над примітивним двійковим полем Галуа  $GF(2)$ . Як матрицю M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа. Ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).

UA 144137 U

UA 144137 U

Корисна модель належить 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 багатократному виконанні однакових груп перетворень, що забезпечують необхідні умови стійкості криптографічного перетворення: розсіювання (за допомогою P-блоків) та перемішування (за допомогою S-блоків) інформаційних даних.

Недоліками цього способу є те, що для криптографічного перетворення інформації як S-блок виступає фіксована матриця підстановок, що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних, а також те, що для функціональної операції перемішування використовуються фіксовані значення параметрів зсуву.

Найближчим аналогом до запропонованої корисної моделі є удосконалений спосіб криптографічного перетворення [2], який ґрунтується на тому, що інформаційну послідовність подають у вигляді бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: перемішування (permutation) - за допомогою блоків перемішування кубиків (блоків Permut3D); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв. При цьому бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків) і як S-блок формують змінну тривимірну матрицю підстановок, і будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення  $y = M \cdot x^{-1} + \beta$  над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як матрицю M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, і функціональні операції циклічного зсуву не фіксовані, а залежать від стану ключа.

Недоліками найближчого аналога є те, що для криптографічного перетворення інформації як S-блок виступає фіксована матриця підстановки, що не дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом підстановки інформаційних даних, і те, що для криптографічного перетворення інформації параметри підстановки фіксовані, і те, що для криптографічного перетворення інформації параметри циклічного зсуву фіксовані.

В основу корисної моделі поставлена задача створити спосіб криптографічного перетворення інформації, який за рахунок використання чотирьох тривимірних криптографічних перетворень (підстановки, перемішування, циклічного зсуву і ковзного кодування) дасть змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом ковзного кодування та підстановки інформаційних даних у тривимірному просторі, і що функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа, і що ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).

Поставлена задача вирішується за рахунок того, що у способі криптографічного перетворення інформації, який полягає в тому, що інформаційну послідовність подають у вигляді бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, підстановка (substitution) - за допомогою блоків підстановок (S-блоків); перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); функціональні операції ковзного кодування (SlidCode) - за допомогою змішаних кодів Грея, згідно з корисною моделлю, бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків), і що як S-блок формують змінну тривимірну матрицю підстановки, що будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення  $y = M \cdot x^{-1} + \beta$  над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як матрицю M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до

значення циклового ключа, і що функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа, і що ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).

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

Спосіб криптографічного перетворення інформації реалізується тим, що інформаційну послідовність подають у вигляді 256 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, підстановка (substitution) - за допомогою блоків підстановок (S-блоків); перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); функціональні операції ковзного кодування (SlidCode) - за допомогою змішаних кодів Грея. Як S-блок виступає змінна матриця підстановок, яку будують отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення (1) над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як симетричну матрицю M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, і що функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа, і що ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).

Цикловий ключ виробляють із ключа шифрування за допомогою алгоритму вироблення ключів. Довжина циклового ключа дорівнює довжині блока. 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 використовується відповідна симетрична матриця M, яка за допомогою циклового 4 байтового ключа може обиратися із великої множини обернених матриць. Це надає змогу у процесі криптографічного перетворення гнучко змінювати матрицю перемішування та динамічно керувати процесом перемішування, підстановки, циклічного зсуву і ковзного кодування інформаційних даних.

В залежності від стану раундового ключа вибирається параметр перемішування, підстановки, циклічного зсуву і ковзного кодування, шляхом складання за модулем 2 всіх байтів ключа, встановлення 1 в молодший розряд результату складання (для утворення непарного значення) і позбавлення від старшого розряду результату складання (залишається 7 з 8 значущих біт). Остаточне значення визначає величину зсуву у поточному раунді.

Таким чином, за рахунок використання змінних обернених симетричних матриць і змінної (залежного від раундового ключа) функції підстановки вдається на кожній ітерації криптографічного перетворення інформації застосовувати як S-блок динамічно змінювані матриці підстановок і різні величини ковзного кодування, що дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом ковзного кодування та підстановки не фіксованих інформаційних даних у тривимірному просторі.

Джерела інформації:

1. "FIPS PUB 46-3" FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION. DATA ENCRYPTION STANDARD (DES) 1999 Oktober 25. - P. 26. <http://www.everyspec.com/NIST/NIST-FIPS/download.php?spec=FIPS PUB 46-3.030171.pdf>.

2. Патент України на корисну модель № 99696, МПК G09C 1/00 (2015.01). Спосіб криптографічного перетворення інформації/ Білецький А.Я., Навроцький Д.О.; заявник і патентовласник Національний авіаційний університет. - № u201404060; заявл. 16.04.2014; опубл. 25.06.2015, Бюл. № 12. - 5 с.

#### ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб криптографічного перетворення інформації, який полягає в тому, що інформаційну послідовність подають у вигляді бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, підстановка (substitution) - за допомогою блоків підстановок (S-блоків); перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); функціональні операції ковзного кодування (SlidCode) - за

допомогою змішаних кодів Грея, який **відрізняється** тим, що бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків), як S-блок формують змінну тривимірну матрицю підстановок, що будується отриманням мультиплікативно зворотного елемента  $x^{-1}$  над розширеним кінцевим полем Галуа  $GF(2^8)$  та шляхом виконання афінного перетворення  $y = M \cdot x^{-1} + \beta$  над примітивним двійковим полем Галуа  $GF(2)$ , при цьому як матрицю  $M$  афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, функціональні операції ковзного кодування та підстановки не фіксовані, а залежать від стану ключа, ітеративна обробка примітивними криптографічними перетвореннями відбувається у такій послідовності: функціональні операції ковзного кодування (SlidCode), перемішування (permutation), підстановка (substitution), функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow).

---

Комп'ютерна верстка В. Мацело

---

Міністерство розвитку економіки, торгівлі та сільського господарства України,  
вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

---

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601