



УКРАЇНА

(19) **UA** (11) **113464** (13) **U**

(51) МПК (2016.01)

G09C 1/00**H04L 9/06** (2006.01)**H04L 9/14** (2006.01)**G06F 21/72** (2013.01)**G06F 21/60** (2013.01)ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ**(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ**

(21) Номер заявки: u 2016 08327	(72) Винахідник(и): Білецький Анатолій Якович (UA), Навроцький Денис Олександрович (UA)
(22) Дата подання заявки: 28.07.2016	(73) Власник(и): НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, просп. Комарова, 1, м. Київ, 03680 (UA)
(24) Дата, з якої є чинними права на корисну модель: 25.01.2017	
(46) Публікація відомостей про видачу патенту: 25.01.2017, Бюл.№ 2	

(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: перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв. Бітні блоки інформаційної послідовності подають як тривимірні матриці (кубики) i , що як P-блок формують змінну тривимірну матрицю перемішування, 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 матриці M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа. Функціональні операції перемішування не фіксовані, а залежать від стану ключа. Функціональні операції циклічного зсуву не фіксовані, а залежать від стану ключа.

UA 113464 U

Запропонована корисна модель належить до галузі криптографічного захисту інформації і може бути використаною 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 перемішування, а також те, що для функціональної операції циклічного зсуву використовуються фіксовані значення параметрів циклічного зсуву.

Найбільш близьким до запропонованого технічним рішенням, вибраним як найближчий аналог, 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 $GF(2^2)$ та шляхом виконання афінного перетворення $y = M \cdot x^{-1} + \beta$ над примітивним двійковим полем Галуа $GF(2)$, при цьому як матриці 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 способу-найближчого аналога є те, що для криптографічного перетворення інформації як P-блок виступає фіксована матриця перемішування, що не дає змоги гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних, і те, що для криптографічного перетворення інформації параметри перемішування 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 як P-блока динамічно змінюваних матриць перемішування, дасть змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування інформаційних даних у тривимірному просторі, і те, що параметри перемішування динамічно змінюються в залежності від стану ключа, і те, що параметри циклічного зсуву динамічно змінюються в залежності від стану ключа.

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: перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, згідно з корисною моделлю, бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків) і, що як P-блок формують змінну тривимірну матрицю перемішувань, 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 матриці M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, і що функціональні операції перемішування не фіксовані, а залежать від стану ключа, і що функціональні операції циклічного зсуву не фіксовані, а залежать від стану 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 і циклічного зсуву інформаційних даних.

Спосіб криптографічного перетворення інформації реалізується тим, що інформаційну послідовність подають у вигляді 256 бітних блоків, які підлягають ітеративній обробці примітивними криптографічними перетвореннями: перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв. Як P-блок виступає змінна матриця перемішування, 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 перемішування не фіксовані, а залежать від стану ключа, і, що функціональні операції циклічного зсуву не фіксовані, а залежать від стану ключа.

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 вибиратися із великої множини обернених матриць. Це надає змогу у процесі криптографічного перетворення гнучко змінювати матрицю перемішування та, відповідно, динамічно керувати процесом перемішування інформаційних даних і динамічно керувати процесом циклічного зсуву інформаційних даних.

В залежності від стану раундового ключа вибирається параметр перемішування і параметр циклічного зсуву, 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 зсуву вдається на кожній ітерації криптографічного перетворення інформації застосовувати як P-блок динамічно змінювані матриці перемішування і різні величини зсуву, що дає змогу гнучко змінювати параметри криптографічної обробки та динамічно керувати процесом перемішування і циклічним зсувом 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. Спосіб криптографічного перетворення інформації: патент 94189: МПК G09C1/00, Білецький А.Я., Навроцький Д.О.; власник патенту Національний авіаційний університет. - № 201312117; заявл. 16.10.2013; опубл. 10.11.2014, Бюл. № 21. - 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: перемішування (permutation) - за допомогою блоків перемішування кубиків (P-блоків); підстановка (substitution) - за допомогою блоків підстановок (S-блоків); функціональні операції циклічного зсуву і додавання за модулем 2 (ShiftRow) - за допомогою відповідних пристроїв, який **відрізняється** тим, що бітні блоки інформаційної послідовності подають у вигляді тривимірних матриць (кубиків) і, що як P-блок формують змінну тривимірну матрицю перемішування, 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 матриці M афінного перетворення використовують змінні обернені симетричні матриці, які вибирають відповідно до значення циклового ключа, і що функціональні операції перемішування не фіксовані, а залежать від стану ключа, і що функціональні операції циклічного зсуву не фіксовані, а залежать від стану ключа.

Комп'ютерна верстка Д. Шеверун

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

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