УКРАЇНА

(19) UA (11) 103726 (13) C2

(51) МПК (2013.01)
H04L 12/00
H04L 9/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВИНАХІД

(21) Номер заявки: **a 2012 11995**

(22) Дата подання заявки: **18.10.2012**

(24) Дата, з якої є чинними права на винахід: **11.11.2013**

(41) Публікація відомостей про заявку: **13.05.2013, Бюл.№ 9**

(46) Публікація відомостей про видачу патенту: **11.11.2013, Бюл.№ 21**

(72) Винахідник(и):
Горбенко Іван Дмитрович (UA),
Олійников Роман Васильович (UA),
Руженцев Віктор Ігорович (UA),
Казимиров Олександр Володимирович (UA),
Горбенко Юрій Іванович (UA)

(73) Власник(и):
АКЦІОНЕРНЕ ТОВАРИСТВО "ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ",
вул. Бакуліна, 12, м. Харків, 61166 (UA)

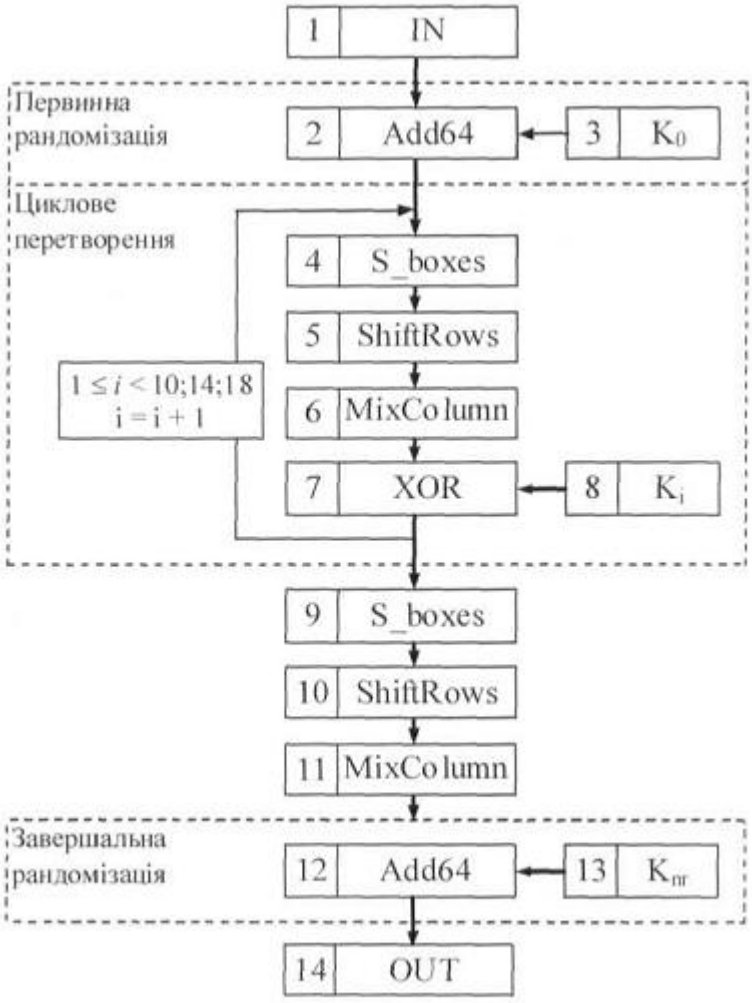
(56) Перелік документів, взятих до уваги експертизою:
US 2012201374 A1; 09.08.2012
WO 2010132130 A1; 18.11.2010
KR 20090037366 A; 15.04.2009
CN 101409616 A; 15.04.2009
JP 2009276458 A; 26.11.2009
JP 2009206593 A; 10.09.2009
JP 2008040244 A; 21.02.2008
EP 1379023 A1; 07.01.2004

(54) СПОСІБ ШИФРУВАННЯ ДВІЙКОВИХ БЛОКІВ ДАНИХ

(57) Реферат:

Спосіб шифрування двійкових блоків даних належить до області обчислювальної техніки, а саме до способів криптографічного перетворення даних. Спосіб містить формування сукупності циклових ключів із ключа шифрування, початкове та завершальне забілювання ключа, циклові перетворення, а саме операцію додавання ключа за модулем, заміну байтів відповідно до фіксованих таблиць підстановок, лінійне перетворення результату байтової заміни, яке представлене циклічними зсувами байтових рядків у межах блока даних та побайтовим множенням на фіксовану матрицю у скінченному полі. У блоці байтової заміни SBox використовують чотири різні таблиці підстановок для різних груп байтів блока даних, а циклічні зсуви лінійного перетворення ShiftRows залежать від розмірів вхідного блока даних, додавання циклових ключів відбувається за модулями 2^{64} та за модулем 2. Спосіб забезпечує високий рівень стійкості, швидкодію, що не поступається аналогам, та оптимальні вимоги до обсягу необхідної пам'яті.

UA 103726 C2


1
IN
Первинна рандомізація
2
Add64
3
K0
Циклове перетворення
4
S_boxes
5
ShiftRows
1 ≤ i < 10;14;18
i = i + 1
6
MixColumn
7
XOR
8
Ki
9
S_boxes
10
ShiftRows
11
MixColumn
Завершальна рандомізація
12
Add64
13
Knr
14
OUT

Фіг. 1

Винахід належить до області обчислювальної техніки, а саме до способів криптографічного перетворення даних.

Відомий спосіб криптографічного перетворення даних AES Rijndael (див. J. Daemen, V. Rijmen. "AES Proposal: Rijndael", AES Round 1, National Institute of Standards and Technology, Aug 1998. http://www.nist.gov/aes). Шифрування з використанням даного способу полягає у виконанні багатоциклової процедури криптографічних перетворень, що виконуються за допомогою на бору циклових підключів. Вказана процедура включає первинне забілювання вихідного блока даних шляхом додавання за модулем 2 першого підключа, а також наступні ітеративні циклові перетворення. AddRoundKey - перетворення, що здійснює додавання циклового підключа до масиву State (проміжного результату шифрування блока даних). ShiftRows - перетворення, що здійснює циклічний зсув рядків масиву State на різну кількість байт. SubBytes - перетворення, що реалізується нелінійною таблицею байтової підстановки. MixColumn - лінійне перетворення представлене множенням байтових рядків на фіксовану матрицю та складається з операцій XOR (виключна диз'юнкція), множення багаточленів за модулем x^4+1 і множення у скінченному полі. Процедура розгортання ключів використовує перетворення RotWord, що оброблює чотирибайтове слово шляхом здійснення підстановки кожного байта, додавання константи та виконання циклічного зсуву отриманого слова на 1 байт.

Описаний спосіб має порівняно високу швидкодію процедури шифрування, проте сучасні умови застосування шифрів висувають додаткові вимоги: збільшення розміру блока даних, що оброблюється, без втрати продуктивності симетричного шифрування, а також підвищення його стійкості за рахунок збільшення розміру ключа та кількості ітерацій криптографічних перетворень. Також у процесі дослідження стійкості способу шифрування AES Rijndael було виявлено ряд потенційних вразливостей, що наразі не мають практичного застосування, але можуть становити небезпеку з розвитком та підвищенням потужностей обчислювальних технологій.

Найближчим за суттєвими ознаками до заявленого способу шифрування є спосіб шифрування двійкових блоків даних "Калина", (патент України на винахід № 89382, МПК H04L 9/06, опубл. 25.01.2010, Бюл. № 2). Спосіб шифрування двійкових блоків даних "Калина" полягає у виконанні ітеративної багатоциклової процедури криптографічних перетворень з використанням набору підключів, сформованих з майстер-ключа. Дана процедура складається з первинного забілювання вихідного блока даних (представленого послідовністю байт) шляхом додавання першого підключа за модулем 2, циклових перетворень (кількість циклів залежить від розміру ключа), а також завершального перетворення, що здійснює додавання останнього підключа за модулем 2^{32}. Кожен цикл складається з наступних перетворень: SBox - здійснює заміну байтів блока даних використовуючи фіксовані таблиці підстановок; ShiftRows – виконує циклічний зсув рядків блока даних на різну кількість байт; MixColumn - здійснює множення байтових рядків на матрицю лінійного перетворення; XOR та Add32 - виконують додавання циклового підключа за модулями 2 та 2^{32} відповідно. Циклові підключі формуються схемою розгортання майстер-ключа, що використовує описані циклові перетворення, на вхід яких подаються фіксовані константи як вхідний блок та майстер-ключ (а також його лінійні перетворення або Інверсію) як цикловий підключ.

Описаний спосіб шифрування двійкових блоків даних забезпечує високу криптографічну стійкість та багатий вибір режимів роботи (розміри вхідного блока та майстер-ключа), проте має порівняно низьку швидкодію та надмірно високі вимоги до обсягу необхідної пам'яті при програмній та апаратній реалізації.

Технічною задачею винаходу є реалізація способу криптографічного перетворення двійкових даних, що забезпечує високий рівень стійкості, швидкодію, що не поступається аналогам, та оптимальні вимоги до обсягу необхідної пам'яті.

Такий технічний результат можливо наступним чином. У способі шифрування двійкових блоків даних "Калина-2", що містить формування сукупності циклових ключів із ключа шифрування, початкове та завершальне забілювання ключа, циклові перетворення, а саме операцію додавання ключа за модулем, заміну байтів відповідно до фіксованих таблиць підстановок, лінійне перетворення результату байтової заміни, яке представлене циклічними зсувами байтових рядків у межах блока даних та побайтовим множенням на фіксовану матрицю у скінченному полі, згідно з винаходом, процедура шифрування містить 10, 14 або 18 циклів в залежності від розміру ключа, у блоці байтової заміни SBox використовують чотири різні таблиці підстановок для різних груп байтів блока даних, а циклічні зсуви лінійного перетворення ShiftRows залежать від розмірів вхідного блока даних, додавання циклових ключів відбувається за модулями 2^{64} та за модулем 2, при цьому для додавання циклового ключа до блоку даних на сусідніх циклах використовують однакові модулі, а сама процедура розгортання реалізується

шляхом формування проміжного ключа з ключа шифрування та виконання зменшеної кількості циклів процедури криптографічного перетворення, до якої подається ключ шифрування або його циклічний зсув як вхідний блок даних і проміжний ключ або його сума з деякою константою як цикловий ключ перетворення.

На фіг. 1 представлена узагальнена схема пристрою, що реалізує запропонований спосіб шифрування, а саме виконання процедури шифрування.

На фіг. 2 представлена схема пристрою, що виконує обчислення проміжного ключа, що використовується схемою розгортання ключа шифрування.

На фіг. 3 представлена блок-схема процедури формування циклових ключів, що мають парні індекси.

У таблиці 1 представлено значення циклічних зсувів для формування циклових ключів, що мають непарні індекси.

У таблиці 2 представлено залежність кількості циклів процедури шифрування в залежності від розміру блока та ключа шифрування.

У таблиці 3 представлена порівняльна характеристика швидкодії шифрів "Калина-2", ГОСТ 28147-89 та AES за різних режимів.

Узагальнена схема пристрою, що реалізує криптографічне перетворення даних відповідно до запропонованого способу шифрування (див. фіг. 1), включає: 1 - накопичувач вхідного блока даних (IN); 7 - блок додавання за модулем 2 (XOR); 2, 12 - блоки додавання за модулем 2^{64}; 3, 8, 13 - блоки зберігання циклових ключів K_i, 4, 9 - блоки байтової заміни (Sbox); 5,10 - блоки зсувів байтових рядків (ShiftRows); 6, 11 - блоки множення байтових рядків на матрицю лінійного перетворення (MixColumn).

Вхідний блок даних спершу вводиться у накопичувач 1, після чого відбувається первинне ключове перетворення (забілювання). Для здійснення цього перетворення блок даних надходить із накопичувача до першого входу суматора 2, а до другого входу подається перший цикловий ключ K_0, що зберігається у блоці пам'яті 3. Після перетворення у суматорі 2 над блоком даних здійснюється багатоциклове перетворення, на кожному циклі якого послідовно виконується байтова заміна відповідно до фіксованих таблиць підстановок 4, циклічний зсув рядків блока даних 5, множення стовбців блока даних на матрицю лінійного перетворення 6 та додавання чергового циклового ключа (що зберігається у блоці пам'яті 8) у суматорі 7.

Завершальне циклове перетворення виконують за допомогою блоків 9, 10, 11 і суматора 12, повторюючи байтову заміну, циклічний зсув рядків та множення блока даних на матрицю лінійного перетворення. Останнім перетворенням є додавання ключа за модулем 2^{64} у суматорі 12, на вхід якого подається результат обчислення у блоці 11 та останній цикловий ключ з блока пам'яті 13. Результуючий блок даних формується у вихідному накопичувачі 14.

Нова процедура розгортання ключів формує циклові ключі, використовуючи проміжний ключ K_t та ключ шифрування. Спосіб розгортання ключа шифрування працює за схемою, що складається з двох етапів:

1) вироблення ключового проміжного ключа K_t;

2) використовуючи проміжний ключ K_t формуються циклові ключі K_i.

Проміжний ключ k, обчислюється з ключа шифрування k (див. фіг. 2) використовуючи описані криптографічні перетворення. Спочатку до блока накопичувача 1 вводиться значення, що залежить від розміру блока (N_k) та ключа шифрування (N_k). Наступним кроком у суматорі 2 здійснюється додавання ключа шифрування, що зберігається у блоці пам'яті 3, до блока даних за модулем 2^{64}. Якщо ключ шифрування є довшим за блок даних, на суматор 2 подається його перша половина. Результат обчислення подається до циклового перетворення описаного способу шифрування, що реалізоване перетвореннями 4 (байтова заміна), 5 (циклічний зсув рядків блока), 6 (множення на матрицю лінійного перетворення) та 7 (додавання за модулем 2 ключа, що зберігається у блоці пам'яті 8, до блока даних). Далі блок даних повторно оброблюється цикловим перетворенням, але додавання ключа здійснюють за модулем 2^{64} з використанням суматора 12. Якщо ключ шифрування є довшим за блок даних, на суматор 12 подається його друга половина. Отриманий блок даних востаннє подається до перетворень 14 (байтова заміна), 15 (циклічний зсув рядків блока) та 16 (множення на матрицю лінійного перетворення). Результуючий блок даних є проміжним ключем K_t.

Блок-схема пристрою, що виконує розгортання ключа та формування циклових ключів з парними індексами відповідно до запропонованого способу шифрування, представлена на фіг. 3. При формуванні циклових ключів з парними індексами ключ шифрування K (або його циклічний зсув) подається на вхід до двох циклів шифрування як вхідний блок (один або два блоки, в залежності від довжини). Як цикловий ключ використовується результат обробки проміжного ключа k, перетворенням Add64, де значення другого аргументу залежить від індекса

циклового ключа, що формується. Розмір змінної tmv (tmp_modification_value) дорівнює довжині блока. Її значення формується повторенням байт 0×01, 0×00 (в шістнадцятковому представленні). Операція ShiftLeft виконує логічний зсув аргумента на один біт ліворуч. Операція Rotate виконує циклічний зсув аргументу на 8 байт ліворуч.

Циклові ключі з непарними індексами обчислюються з вже сформованих парних циклових ключів шляхом циклічного зсуву вліво на $2 \cdot N_b+3$ байт, де N_b - розмір блока даних. Залежність константи, що визначає значення зсуву вліво циклового ключа з парним індексом, від розміру блока наведена у таблиці 1.

У запропонованому способі шифрування процедура розгортання ключів залежить від довжини ключа шифрування і розміру блока даних. При виконанні цієї процедури ключ шифрування розгортається до необхідної довжини. Загальна довжина розгорнутого ключа в бітах може бути обчислена таким чином:

$L_K=N_b \times 64 \times (r+1)$,

де N_b - розмір блока (кількість 64-бітних слів), r - кількість циклів, при цьому довжина кожного циклового ключа збігається з довжиною блока даних. Запропонований спосіб криптографічного перетворення двійкових даних "Калина-2" порівняно з прототипом має еквівалентні показники стійкості та значно кращі показники швидкодії шифрування. Такий позитивний ефект одержується за рахунок:

1 Використання операцій додавання циклових ключів за різними модулями.

1.1 Використання операцій додавання циклових ключів за модулем 2 і за модулем 2^{64} дозволяє підвищити криптографічну стійкість шифру у порівнянні з використанням лише додавання за модулем 2. Додавання за модулем 2^{64} дозволяє застосувати перетворення одразу до 8 байт блока даних, що покращує швидкодію програмної та апаратної реалізації на 64-бітних платформах.

1.2 Для випадку диференціального й лінійного криптоаналізу кожна операція додавання за модулем 2^{64} може розглядатися як додаткове нелінійне перетворення, що підвищує невизначеність криптоаналітика при спробі відновлення секретного ключа.

2 Циклічне використання чотирьох не алгебраїчно побудованих підстановок

2.1 Використання випадково сформованих та додатково відібраних за критеріями стійкості до диференційного та лінійного криптоаналізу підстановок дозволяє знизити ймовірність існування квадратичних залежностей між вхідними та вихідними бітами S-блоку, що підвищує стійкість шифру до алгебраїчних атак. Для заміни кожних восьми байт блока даних циклічно використовуються чотири різних підстановки, що зменшує об'єм необхідної пам'яті при реалізації.

3 Використання нової схеми розгортання ключа шифрування

3.1 На відміну від схеми розгортання ключа шифру "Калина" схема розгортання ключа запропонованого способу шифрування "Калина-2" використовує лише перетворення, які застосовуються при зашифруванні блока інформації.

3.2 Схема розгортання ключа шифру "Калина-2" не дозволяє відновити значення вихідного ключа шифрування, маючи значення циклових ключів.

3.3 Розгортання ключа шифру "Калина-2" виконується за час, що не перевищує час зашифрування двох блоків інформації.

3.4 Для одержання одного з циклових ключів не потрібне виконання всієї схеми розгортання ключа (генерації всіх циклових ключів).

Таблиця 1

Розмір блока, біт (байт)	Зсув вліво (байт)
128(16)	7
256 (32)	11
512(64)	19

Таблиця 2

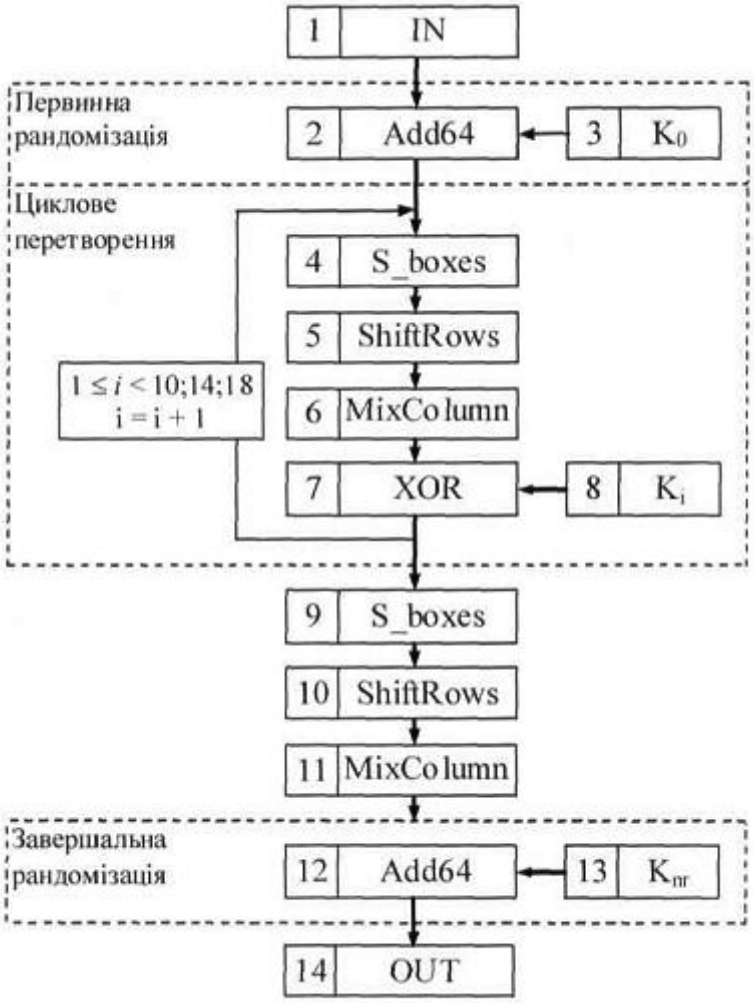
Розмір ключа Розмір блока	128 (N_k=2)	256 (Nt=4)	512 (N_k=8)
128 (N_b=2)	10	14	-
256 (N_b=4)	-	14	18
512 (N_b=8)	-	-	18

Таблиця 3

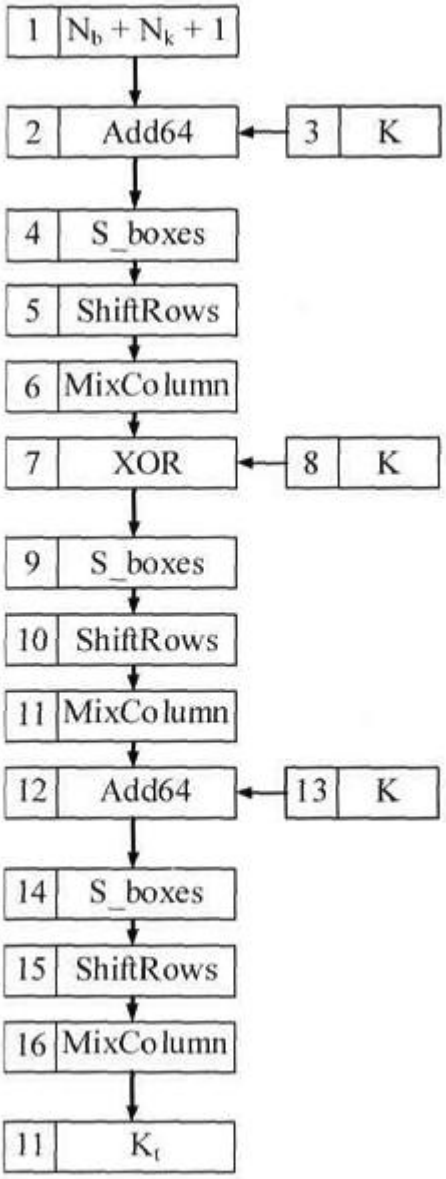
Алгоритм, режим шифрування	Швидкодія, Мб/с	
	Intel Core i5 Windows Server 2008 R2 × 64 Visual C++ 2008	Core 2 Duo B8500 Linux (64 bit) GCC
Калина 128/128	1538.3	1828.6
Калина 128/256	1098.2	1291.7
Калина 256/256	1256.2	1219.1
Калина 256/512	977.61	948.15
Калина 512/512	995.72	948.15
AES-128	1483.3	1668
AES-256	1095.2	1254
ГОСТ 28147	376.3	492.31
STB-BelT	609.18	753.5

ФОРМУЛА ВИНАХОДУ

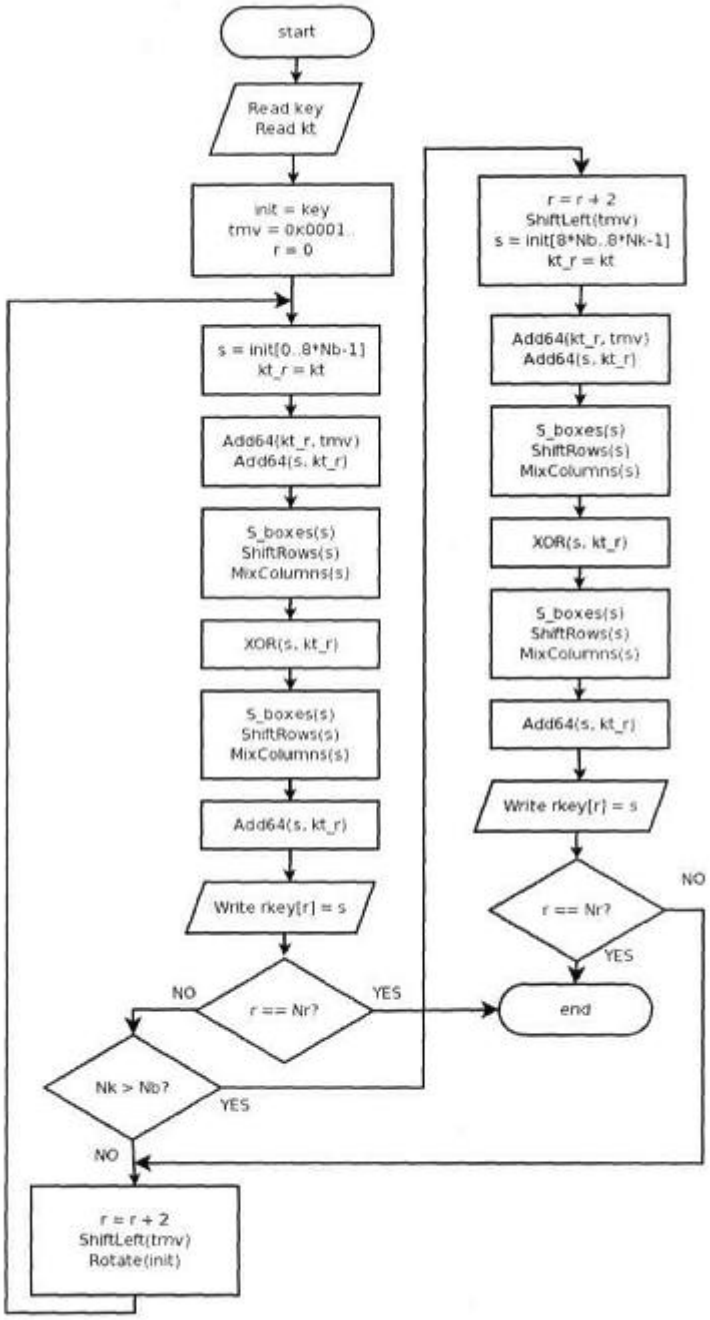
Спосіб шифрування двійкових блоків даних, що включає формування сукупності циклових ключів із ключа шифрування, початкове та завершальне забілювання ключа, циклові перетворення, а саме операцію додавання ключа за модулем, заміну байтів відповідно до фіксованих таблиць підстановок, лінійне перетворення результату байтової заміни, яке представлене циклічними зсувами байтових рядків у межах блока даних та побайтовим множенням на фіксовану матрицю у скінченному полі, який **відрізняється** тим, що спосіб включає 10, 14 або 18 циклових перетворень в залежності від розміру ключа, у блоці байтової заміни SBox використовують чотири різні таблиці підстановок для різних груп байтів блока даних, а циклічні зсуви лінійного перетворення ShiftRows залежать від розмірів вхідного блока даних, додавання циклових ключів відбувається за модулями 2^{64} та за модулем 2, при цьому для додавання циклового ключа до блока даних на сусідніх циклах використовують однакові модулі, а сама процедура розгортання реалізується шляхом формування проміжного ключа з ключа шифрування та виконання циклових перетворень, до якої подається ключ шифрування або його циклічний зсув як вхідний блок даних і проміжний ключ або його сума з деякою константою як цикловий ключ перетворення.


1
IN
Первинна рандомізація
2
Add64
3
K0
Циклове перетворення
4
S_boxes
5
ShiftRows
1 ≤ i < 10;14;18
i = i + 1
6
MixColumn
7
XOR
8
Ki
9
S_boxes
10
ShiftRows
11
MixColumn
Завершальна рандомізація
12
Add64
13
Knr
14
OUT

Фіг. 1


1
$N_b + N_k + 1$
2
Add64
3
K
4
S_boxes
5
ShiftRows
6
MixColumn
7
XOR
8
K
9
S_boxes
10
ShiftRows
11
MixColumn
12
Add64
13
K
14
S_boxes
15
ShiftRows
16
MixColumn
11
K_t

Фіг. 2



Фіг. 3

Комп'ютерна верстка Л. Литвиненко

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

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