УКРАЇНА **(19) UA (11) 115703 (13) U**

(51) МПК (2017.01)
G09C 5/00
G06F 7/58 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2016 11164**
(22) Дата подання заявки: **07.11.2016**
(24) Дата, з якої є чинними права на корисну модель: **25.04.2017**
(46) Публікація відомостей про видачу патенту: **25.04.2017, Бюл.№ 8**

(72) Винахідник(и):
Торба Алєксандр Алєксєєвіч (UA),
Бобух Всеволод Анатолійович (UA),
Шинкаренко Юрій Курбанович (UA),
Торба Максим Олегович (UA),
Торба Олександр Олегович (UA),
Торба Дмитро Дмитрович (UA)

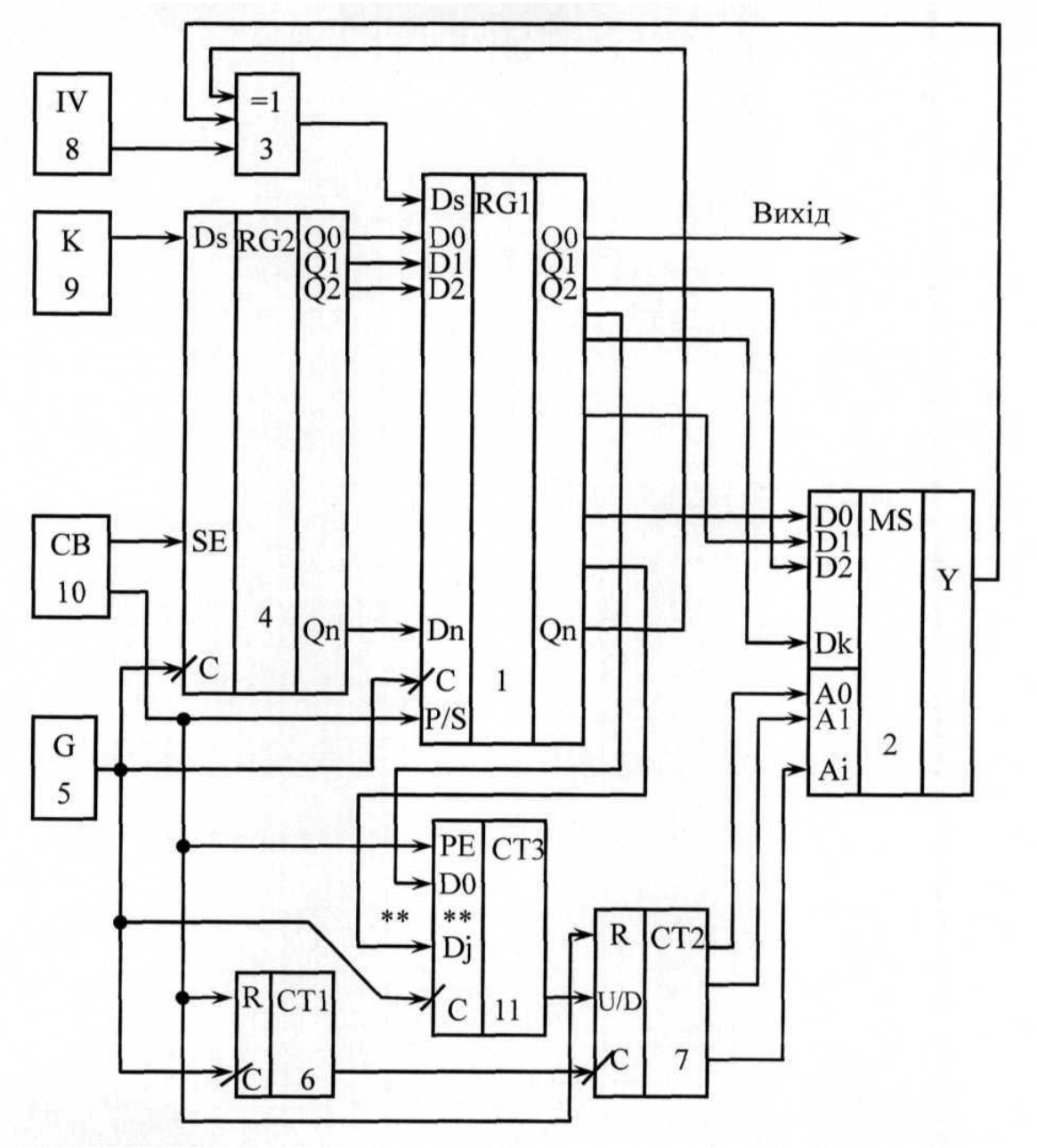
(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Науки, 14, м. Харків, 61166 (UA)

(54) ДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ ДЛЯ ПОТОКОВОГО ШИФРУВАННЯ

(57) Реферат:

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування містить перший регістр зсуву, мультиплексор, інформаційні входи якого у довільному порядку підключені до виходів першого регістра зсуву, а вихід мультиплексора з'єднаний з першим входом елемента ВИКЛЮЧНЕ АБО, другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід елемента ВИКЛЮЧНЕ АБО з'єднано з послідовним входом першого регістра зсуву, другий регістр зсуву, виходи якого підключені до входів паралельного завантаження першого регістра зсуву, тактовий генератор, вихід якого з'єднаний з синхровходами першого й другого регістрів зсуву та першого лічильника, вихід якого підключено до синхровходу реверсивного лічильника, а його виходи підключені до адресних входів мультиплексора, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з третім входом елемента ВИКЛЮЧНЕ АБО, блок формування сеансових ключів, вихід якого підключено до послідовного входу другого регістра зсуву, та блок керування, перший вихід якого з'єднано з входом керування другого регістра зсуву, а другий вихід блока керування підключено до входів скидання першого лічильника та реверсивного лічильника, а також до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву, який відрізняється тим, що додатково введено лічильник з програмованим коефіцієнтом ділення, синхровхід якого підключено до виходу тактового генератора, вхід дозволу паралельного завантаження з'єднано з другим виходом блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід лічильника з програмованим коефіцієнтом ділення підключено до входу перемикання режимів реверсивного лічильника.

UA 115703 U


IV
8
=1
3
K
9
Ds
RG2
Q0
Q1
Q2
Ds
RG1
D0
D1
D2
Q0
Q1
Q2
Вихід
CB
10
SE
4
Qn
Dn
Qn
C
C
P/S
1
G
5
D0
D1
D2
Dk
MS
Y
A0
A1
Ai
2
PE
D0
**
**
Dj
C
CT3
11
R
CT1
C
6
R
CT2
U/D
C
7

Корисна модель належить до області криптографічного захисту інформації та може бути використана для збільшення криптостійкості та збільшення швидкодії криптографічних перетворень.

Відомий апаратний алгоритм потокового шифрування A5, який використовується для шифрування повідомлень в мережах GSM (див. http://ru.wikipedia.org/wiki/A5). Цей апаратний алгоритм складається із трьох рекурентних регістрів зсуву зі зворотним зв'язком (РРЗЗЗ) довжиною 19, 22 і 23. Виходом є логічна функція ВИКЛЮЧНЕ АБО - XOR трьох РРЗЗЗ. В алгоритмі A5 використовується керування тактуванням, що змінюється. Кожен регістр тактується залежно від свого середнього біта, потім виконується XOR зі зворотною граничною функцією середніх бітів усіх трьох регістрів. Зазвичай на кожному етапі тактується два РРЗЗЗ.

Недоліком цього апаратного алгоритму є недостатня криптостійкість тому, що існує тривіальна атака на відкритому тексті (алгоритм Берлекемпа-Мессі), основана на припущенні про зміст перших двох РРЗЗЗ і спробі визначення третього РРЗЗЗ по ключовій послідовності.

Найбільш близьким по сукупності ознак є детермінований генератор псевдовипадкових послідовностей для потокового шифрування (див. патент України на корисну модель № 109675, МПК (2016.01) G09 C 5/00, G06F 7/58, опублікований 25.06.2016, Бюл. № 16), що містить перший регістр зсуву, мультиплексор, інформаційні входи якого у довільному порядку підключені до виходів першого регістра зсуву, а вихід мультиплексора з'єднаний з першим входом елемента ВИКЛЮЧНЕ АБО, другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід елемента ВИКЛЮЧНЕ АБО з'єднано з послідовним входом першого регістра зсуву, другий регістр зсуву, виходи якого підключені до входів паралельного завантаження першого регістра зсуву, тактовий генератор, вихід якого з'єднаний з синхровходами першого та другого регістрів зсуву і синхровходами першого та третього лічильників, вихід першого лічильника підключено до синхровходу другого реверсивного лічильника, виходи якого з'єднані з адресними входами мультиплексора, блок формування випадкового значення ініціалізації, вихід якого підключено до третього входу елемента ВИКЛЮЧНЕ АБО, блок формування сеансових ключів, вихід якого підключено до послідовного входу другого регістра зсуву, та блок керування, перший вихід якого з'єднано з входом керування другого регістра зсуву, а другий вихід блока керування підключено до входів скидання першого, другого реверсивного та третього лічильників та до входу керування першого регістра зсуву, вихід третього лічильника підключено до входу перемикання режимів другого реверсивного лічильника, виходом пристрою є один із виходів першого регістра зсуву.

Недоліком цього генератора є недостатня крипостійкість псевдовипадкових послідовностей, що генеруються, тому, що довгострокові таємні параметри змінюються в детермінованому порядку через постійні часові інтервали.

В основу корисної моделі поставлена задача створення такого детермінованого генератора псевдовипадкових послідовностей для потокового шифрування, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити крипостійкість псевдовипадкових послідовностей, що генеруються.

Поставлена задача вирішується тим, що у детермінований генератор псевдовипадкових послідовностей для потокового шифрування, що містить перший регістр зсуву, мультиплексор, інформаційні входи якого у довільному порядку підключені до виходів першого регістра зсуву, а вихід мультиплексора з'єднаний з першим входом елемента ВИКЛЮЧНЕ АБО, другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід елемента ВИКЛЮЧНЕ АБО з'єднано з послідовним входом першого регістра зсуву, другий регістр зсуву, виходи якого підключені до входів паралельного завантаження першого регістра зсуву, тактовий генератор, вихід якого з'єднаний з синхровходами першого й другого регістрів зсуву та першого лічильника, вихід якого підключено до синхровходу реверсивного лічильника, а його виходи підключені до адресних входів мультиплексора, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з третім входом елемента ВИКЛЮЧНЕ АБО, блок формування сеансових ключів, вихід якого підключено до послідовного входу другого регістра зсуву, та блок керування, перший вихід якого з'єднано з входом керування другого регістра зсуву, а другий вихід блока керування підключено до входів скидання першого лічильника та реверсивного лічильника, а також до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву, згідно з корисною моделлю, додатково введено лічильник з програмованим коефіцієнтом ділення, синхровхід якого підключено до виходу тактового генератора, вхід дозволу паралельного завантаження з'єднано з другим виходом блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід лічильника з програмованим коефіцієнтом ділення підключено до входу перемикання режимів реверсивного лічильника.

На кресленні зображена структурна схема детермінованого генератора псевдовипадкових послідовностей для потокового шифрування. На кресленні використані наступні міжнародні позначення: RG - регістр, MS - мультиплексор, G - генератор, CT - лічильник, IV - значення ініціалізації, CB - блок керування.

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування містить перший регістр 1 зсуву, мультиплексор 2, інформаційні входи якого у довільному порядку підключені до виходів першого регістра 1 зсуву, а вихід мультиплексора 2 з'єднаний з першим входом елемента 3 ВИКЛЮЧНЕ АБО, другий вхід якого підключено до останнього виходу першого регістра 1 зсуву, а вихід елемента 3 ВИКЛЮЧНЕ АБО з'єднано з послідовним входом першого регістра 1 зсуву, другий регістр 4 зсуву, виходи якого підключені до входів паралельного завантаження першого регістра 1 зсуву, тактовий генератор 5, вихід якого з'єднаний з синхровходами першого та другого регістрів 1, 4 зсуву і синхровходами першого лічильника 6 та лічильника 11 з програмованим коефіцієнтом ділення, вихід першого лічильника 6 підключено до синхровходу реверсивного лічильника 7, виходи якого з'єднані з адресними входами мультиплексора 2, блок 8 формування випадкового значення ініціалізації, вихід якого підключено до третього входу елемента 3 ВИКЛЮЧНЕ АБО, блок 9 формування сеансових ключів, вихід якого підключено до послідовного входу другого регістра 4 зсуву, та блок 10 керування, перший вихід якого з'єднано з входом керування другого регістра 4 зсуву, а другий вихід блока 10 керування підключено до входів скидання першого та реверсивного лічильників 6, 7, а також до входу дозволу паралельного завантаження лічильника 11 з програмованим коефіцієнтом ділення, та до входу керування першого регістра 1 зсуву, вихід лічильника 11 з програмованим коефіцієнтом ділення підключено до входу перемикання режимів реверсивного лічильника 7, виходом пристрою є один із виходів першого регістра зсуву.

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування працює наступним чином.

До початку шифрування з виходу блока 9 формування сеансових ключів в другий регістр 4 зсуву в послідовному форматі записується таємний сеансовий ключ. Для цього блок 10 керування виробляє сигнал дозволу, який надходить на вхід керування SE другого регістра 4 зсуву. Після вводу сеансового ключа з виходів другого регістра 4 зсуву цей ключ в паралельному форматі записується в перший регістр 1 зсуву. Для цього блок 10 керування формує логічний сигнал, який переводить перший регістр 1 зсуву в режим паралельного завантаження, перший лічильник 6 та реверсивний лічильники 7 утримуються в нульовому стані, а лічильник 11 з програмованим коефіцієнтом ділення переводиться у режим паралельного завантаження. Перед початком шифрування блок 10 керування переводить перший регістр 1 зсуву в послідовний режим зсуву.

Шифрування починається з передавання випадкового значення ініціалізації IV, яке одночасно в послідовному форматі вводиться в перший регістр 1 зсуву через третій вхід першого елемента 3 ВИКЛЮЧНЕ АБО. На перший та другий входи першого елемента 3 ВИКЛЮЧНЕ АБО подаються сигнали з останнього виходу першого регістра 1 зсуву та виходу мультиплексора 2 для формування рекурентної псевдовипадкової послідовності.

Тактовий генератор 5 визначає частоту зсуву першого та другого регістрів 1, 4 зсуву і таким чином визначає швидкість формування детермінованої псевдовипадкової послідовності.

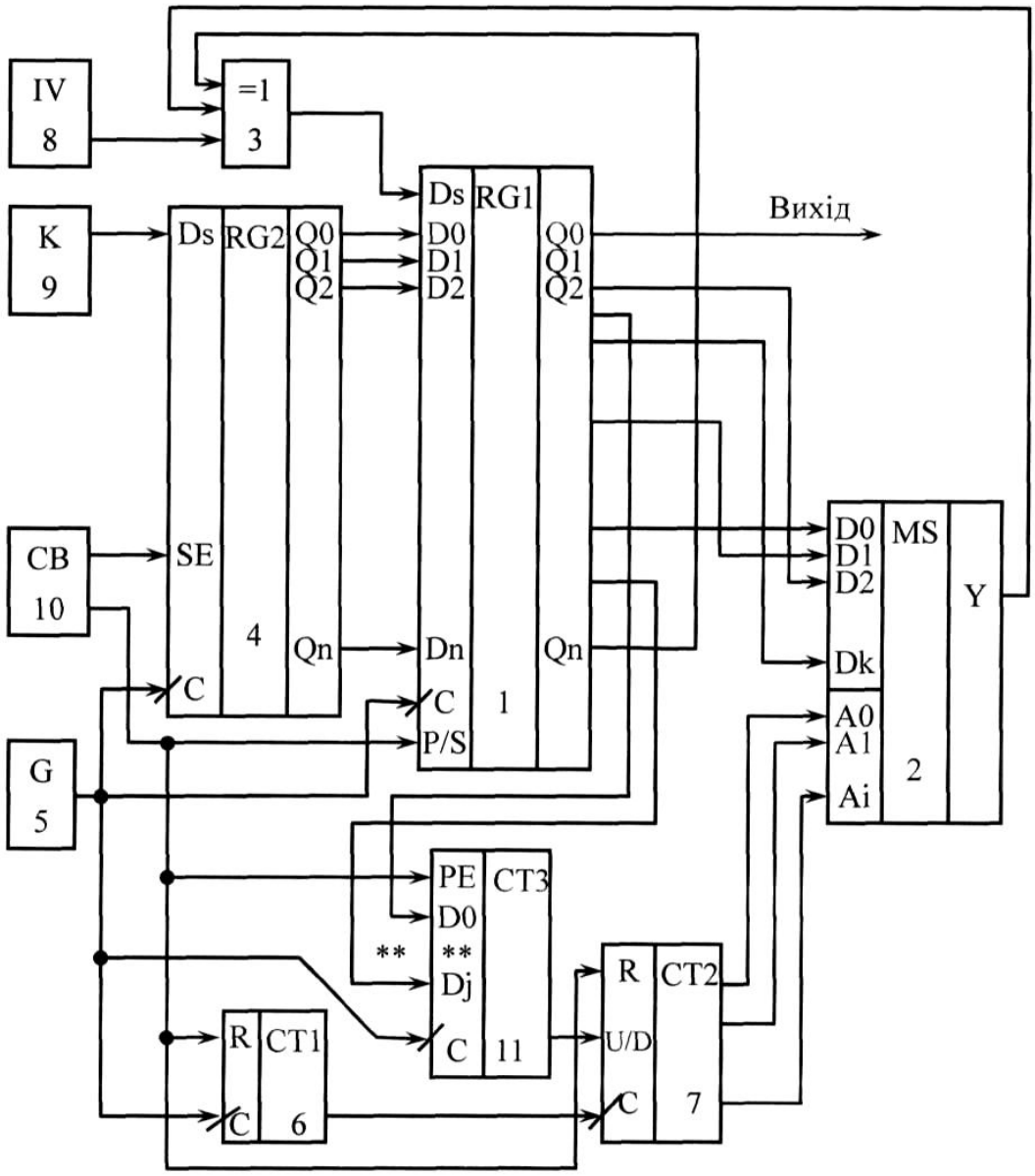
Для зміни параметрів рекуренти першого регістра 1 зсуву логічні рівні з його проміжних виходів подаються на інформаційні входи мультиплексора 2, вихід якого підключено до другого входу першого елемента 3 ВИКЛЮЧНЕ АБО. Адресні входи мультиплексора 2 підключені до виходів реверсивного лічильника 7, синхровхід якого з'єднаний з виходом першого лічильника 6. Лічильник 11 з програмованим коефіцієнтом ділення формує псевдовипадкові часові інтервали, через які реверсивний лічильник 7 перемикається у режим збільшення або зменшення.

Вихідна псевдовипадкова послідовність знімається з одного з виходів першого регістра 1 зсуву.

Таким чином, введення у детермінований генератор псевдовипадкових послідовностей для потокового шифрування додаткового лічильника з програмованим коефіцієнтом ділення, а також додавання нових зв'язків дозволяє формувати повністю детерміновану псевдовипадкову послідовність, довгострокові таємні параметри якої змінюються через псевдовипадкові часові інтервали.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування, що містить перший регістр зсуву, мультиплексор, інформаційні входи якого у довільному порядку підключені до виходів першого регістра зсуву, а вихід мультиплексора з'єднаний з першим входом елемента ВИКЛЮЧНЕ АБО, другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід елемента ВИКЛЮЧНЕ АБО з'єднано з послідовним входом першого регістра зсуву, другий регістр зсуву, виходи якого підключені до входів паралельного завантаження першого регістра зсуву, тактовий генератор, вихід якого з'єднаний з синхровходами першого й другого регістрів зсуву та першого лічильника, вихід якого підключено до синхровходу реверсивного лічильника, а його виходи підключені до адресних входів мультиплексора, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з третім входом елемента ВИКЛЮЧНЕ АБО, блок формування сеансових ключів, вихід якого підключено до послідовного входу другого регістра зсуву, та блок керування, перший вихід якого з'єднано з входом керування другого регістра зсуву, а другий вихід блока керування підключено до входів скидання першого лічильника та реверсивного лічильника, а також до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву, який **відрізняється** тим, що додатково введено лічильник з програмованим коефіцієнтом ділення, синхровхід якого підключено до виходу тактового генератора, вхід дозволу паралельного завантаження з'єднано з другим виходом блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід лічильника з програмованим коефіцієнтом ділення підключено до входу перемикання режимів реверсивного лічильника.



Комп'ютерна верстка Л. Литвиненко

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