УКРАЇНА

(19) UA (11) 99194 (13) U

(51) МПК (2015.01)
G06F 7/58 (2006.01)
G09C 5/00

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 12599**

(22) Дата подання заявки: **24.11.2014**

(24) Дата, з якої є чинними права на корисну модель: **25.05.2015**

(46) Публікація відомостей про видачу патенту: **25.05.2015, Бюл.№ 10**

(72) Винахідник(и):
Торба Алєксандр Алєксєєвіч (UA),
Бобкова Анна Алєксандровна (UA),
Торба Олег Олександрович (UA),
Торба Дмитро Олександрович (UA)

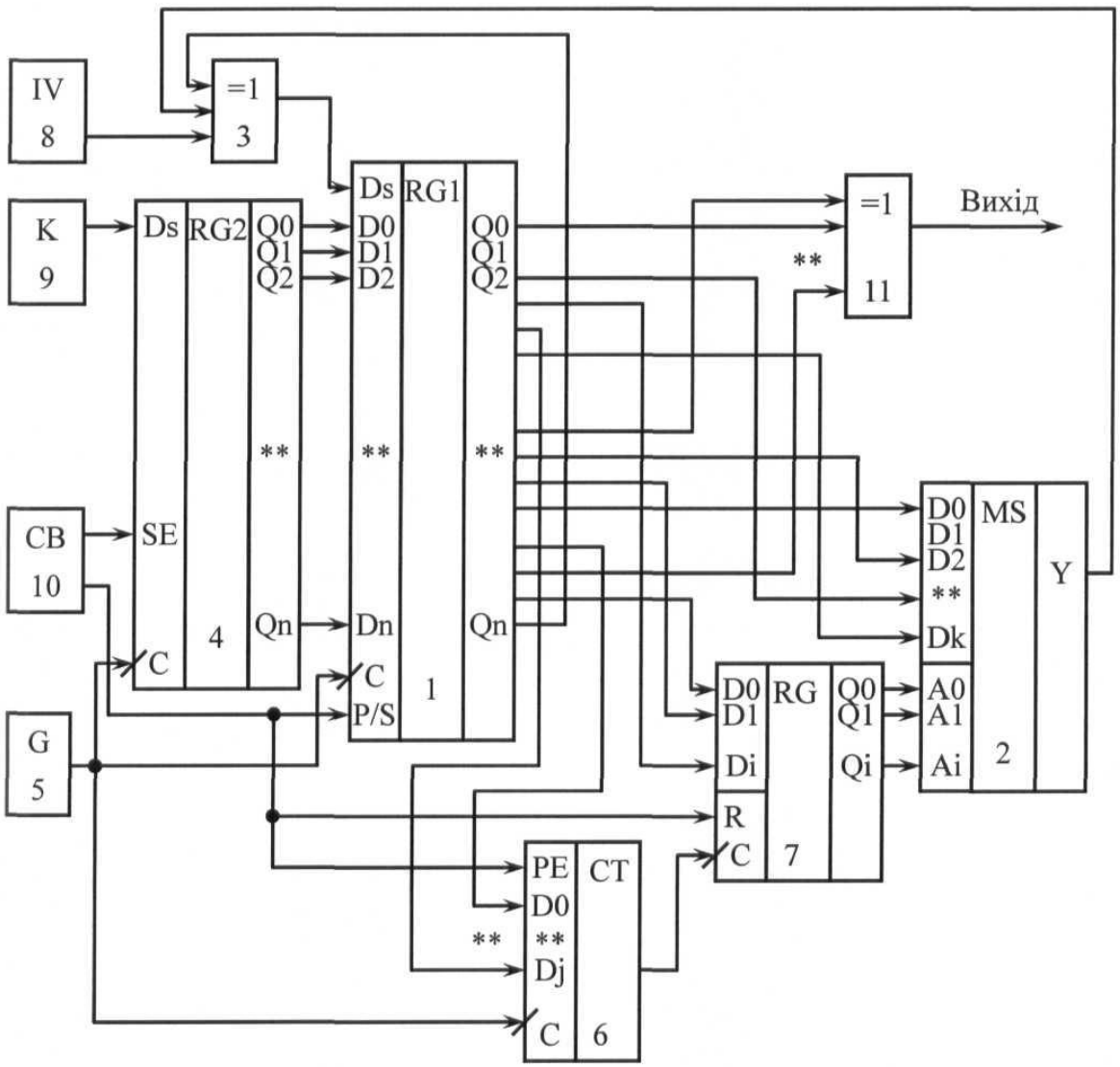
(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Леніна, 14, м. Харків, 61166 (UA)

(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 першого елемента "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід першого 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, паралельний регістр, виходи якого з'єднані з адресними входами мультиплексора, а інформаційні входи паралельного регістра підключені у довільному порядку до виходів першого регістра зсуву, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з третім входом першого 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 входу скидання паралельного регістра, а також до входу керування першого регістра зсуву, другий елемент "ВИКЛЮЧНЕ АБО", входи якого у довільному порядку з'єднані з виходами першого регістра зсуву, а вихід цього елемента є виходом пристрою. Додатково введений лічильник з програмованим коефіцієнтом ділення, у якого синхровхід з'єднано з виходом тактового генератора, вхід дозволу паралельного завантаження підключено до другого виходу блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід з'єднано з синхровходом паралельного регістра.

UA 99194 U


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

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

Відомий детермінований генератор псевдовипадкових послідовностей для потокового шифрування [див. патент України на корисну модель № 85039, МПК (2013.01) G09 C 5/00, G06F 7/58 (2006.01), опублікований 11.11.2013, Бюл. № 21], 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 входом першого лічильника, а його вихід підключено до входу другого лічильника, виходи якого з'єднані з адресними входами 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 та другого лічильників та до входу керування першого регістра зсуву, а 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 у постійному порядку.

Найбільш близьким по сукупності ознак є детермінований генератор псевдовипадкових послідовностей для потокового шифрування [див. патент України на корисну модель № 93117, МПК (2014.01) G09 C 5/00, G06F 7/58 (2006.01), опублікований 25.09.2014, Бюл. № 18], 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 першого елемента "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід першого 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 входом лічильника, а його вихід підключено до синхровходу паралельного регістра, виходи якого з'єднані з адресними входами мультиплексора, а інформаційні входи паралельного регістра підключені у довільному порядку до виходів першого регістра зсуву, 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 лічильника та паралельного регістра, а також до входу керування першого регістра зсуву, другий елемент "ВИКЛЮЧНЕ АБО", входи якого у довільному порядку з'єднані з виходами першого регістра зсуву, а вихід цього елемента є виходом пристрою.

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

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 в 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 першого елемента "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід першого 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, паралельний регістр, виходи якого з'єднані з адресними входами мультиплексора, а інформаційні входи паралельного регістра підключені у довільному порядку до виходів першого регістра зсуву, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з

третім входом першого 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 входу скидання паралельного регістра, а також до входу керування першого регістра зсуву, другий елемент "ВИКЛЮЧНЕ АБО", входи якого у довільному порядку з'єднані з виходами першого регістра зсуву, а вихід цього елемента є виходом пристрою, згідно з корисною моделлю додатково введений лічильник з програмованим коефіцієнтом ділення, у якого синхровхід з'єднано з виходом тактового генератора, вхід дозволу паралельного завантаження підключено до другого виходу блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід з'єднано з синхровходом паралельного регістра.

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, яка залежить від таємного сеансового ключа та початкового значення ініціалізації, а також від зміни довгострокових таємних параметрів у псевдовипадковому порядку через псевдовипадкові часові інтервали.

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 першого елемента 3 "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра 1 зсуву, а вихід першого 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 синхровходом лічильника 6 з програмованим коефіцієнтом ділення, а його вихід підключено до синхровходу паралельного регістра 7, інформаційні входи якого підключені у довільному порядку до виходів першого регістра 1 зсуву, а виходи паралельного регістра 7 з'єднані з адресними входами мультиплексора 2, блок 8 формування випадкового значення ініціалізації, вихід якого підключено до третього входу першого 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 входу керування першого регістра 1 зсуву, а також до входу дозволу паралельного завантаження лічильника 6 з програмованим коефіцієнтом ділення та до входу скидання паралельного регістра 7, другий елемент 11 "ВИКЛЮЧНЕ АБО", входи якого у довільному порядку підключені до виходів першого регістра 1 зсуву, а вихід другого елемента 11 "ВИКЛЮЧНЕ АБО" є виходом пристрою.

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування працює наступним чином.

До початку шифрування з виходу блоку 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 а також лічильник 6 з програмованим коефіцієнтом ділення в режим паралельного завантаження та утримує паралельний регістр 7 в нульовому стані. 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.

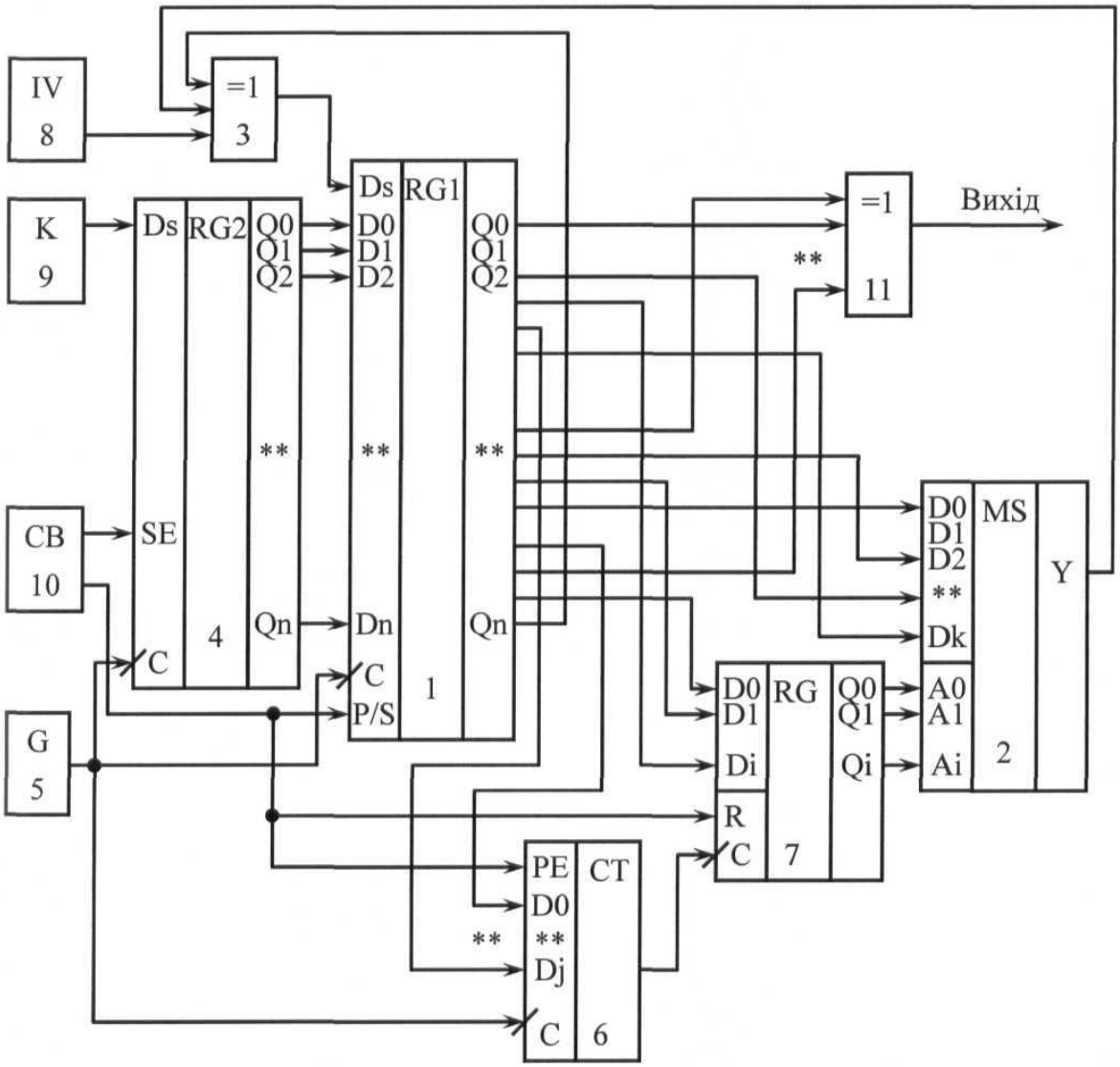
Для зміни параметрів рекуренти першого регістра 1 зсуву логічні рівні з його проміжних виходів подаються на інформаційні входи мультиплексора 2, вихід якого підключено до другого входу першого елемента 3 "ВИКЛЮЧНЕ АБО". Адресні входи мультиплексора 2 підключені до виходів паралельного регістра 7, входи якого у довільному порядку з'єднані з виходами першого регістра 1 зсуву. Лічильник 6 з програмованим коефіцієнтом ділення визначає псевдовипадкові проміжки часу між змінами параметрів рекуренти першого регістра 1 зсуву. Псевдовипадкові коди на адресних входах мультиплексора 2 визначають випадкову послідовність зміни параметрів рекуренти.

Вихідна псевдовипадкова послідовність знімається з виходу другого елемента 11 "ВИКЛЮЧНЕ АБО", входи якого підключені до виходів першого регістра 1 зсуву у довільному порядку. Це дозволяє зменшити різницю ймовірностей вихідних псевдовипадкових бітів.

Таким чином досягнуто підвищення криптостійкості псевдовипадкових послідовностей, що генеруються.

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 першого елемента "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра зсуву, а вихід першого 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, паралельний регістр, виходи якого з'єднані з адресними входами мультиплексора, а інформаційні входи паралельного регістра підключені у довільному порядку до виходів першого регістра зсуву, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з третім входом першого 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 входу скидання паралельного регістра, а також до входу керування першого регістра зсуву, другий елемент "ВИКЛЮЧНЕ АБО", входи якого у довільному порядку з'єднані з виходами першого регістра зсуву, а вихід цього елемента є виходом пристрою, який **відрізняється** тим, що додатково введений лічильник з програмованим коефіцієнтом ділення, у якого синхровхід з'єднано з виходом тактового генератора, вхід дозволу паралельного завантаження підключено до другого виходу блока керування, інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а вихід з'єднано з синхровходом паралельного регістра.



Комп'ютерна верстка Г. Паяльніков

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