УКРАЇНА **(19) UA** **(11) 92794** **(13) U**

(51) МПК (2014.01)
G09C 5/00
G06F 7/58 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2014 00928**
(22) Дата подання заявки: **31.01.2014**
(24) Дата, з якої є чинними права на корисну модель: **10.09.2014**
(46) Публікація відомостей про видачу патенту: **10.09.2014, Бюл.№ 17**

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

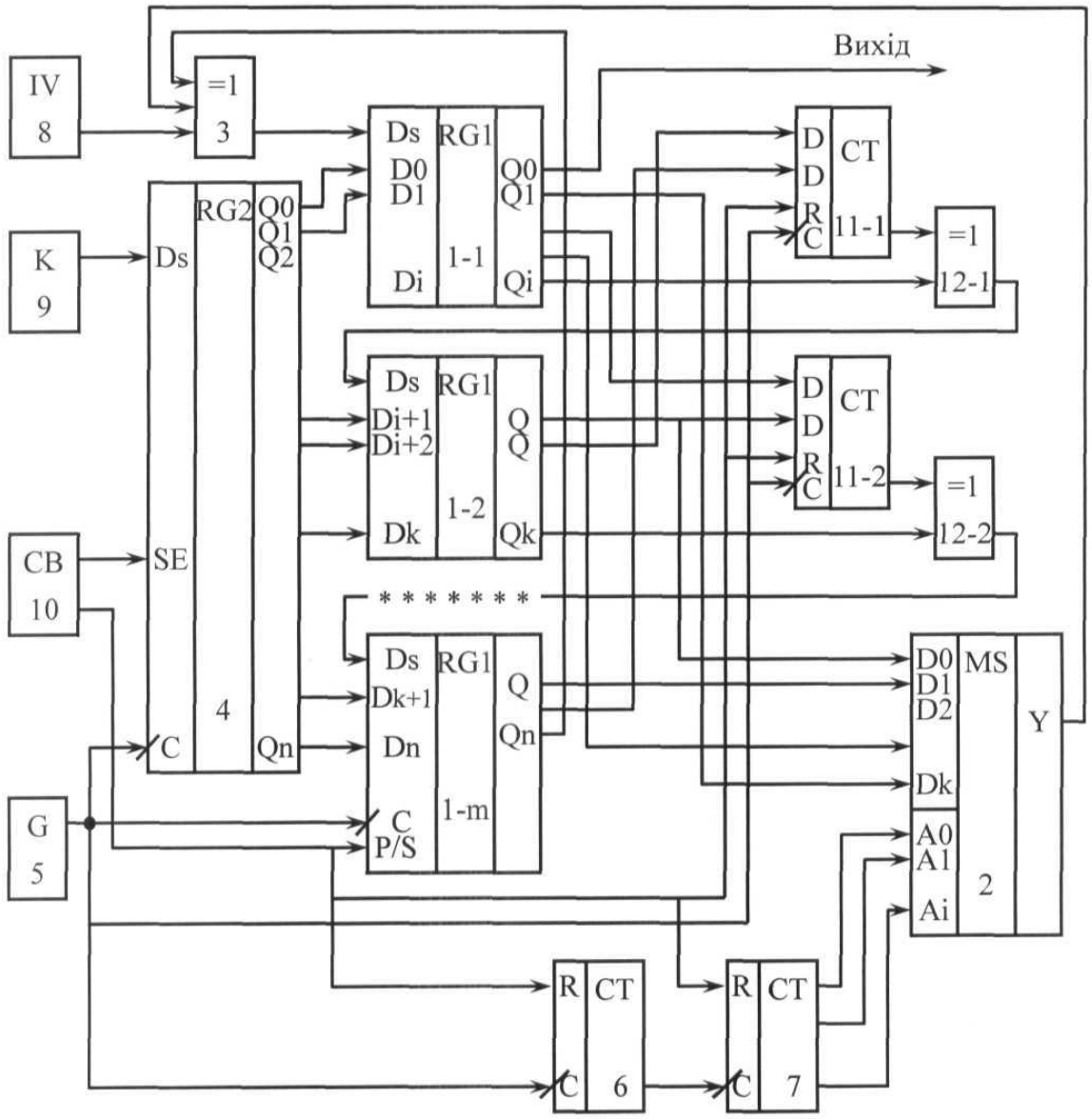
(73) Власник(и):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Леніна, 14, м. Харків, 61166 (UA)

(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. 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. Перший регістр зсуву розділено на m частин, останні виходи m - 1 частин першого регістра зсуву підключені до перших входів додатково введених m - 1 елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з послідовними входами наступних частин першого регістра зсуву, містить m - 1 лічильників з програмованим коефіцієнтом ділення, виходи яких підключені до других входів додаткових елементів "ВИКЛЮЧНЕ АБО", синхровходи лічильників з програмованим коефіцієнтом ділення з'єднані з виходом тактового генератора, входи скидання лічильників з програмованим коефіцієнтом ділення підключені до другого виходу блока керування. Інформаційні входи лічильників з програмованим коефіцієнтом ділення підключені у довільному порядку до виходів першого регістра зсуву.

UA 92794 U


Вихід
IV
8
=1
3
K
9
CB
10
G
5
Ds
RG2
Q0
Q1
Q2
SE
C
4
Qn
Ds
RG1
D0
D1
Di
1-1
Q0
Q1
Qi
Ds
RG1
Di+1
Di+2
Dk
1-2
Q
Q
Qk
* * * * * * *
Ds
RG1
Dk+1
Dn
C
P/S
1-m
Q
Qn
D
D
R
C
CT
11-1
=1
12-1
D
D
R
C
CT
11-2
=1
12-2
D0
D1
D2
Dk
MS
Y
A0
A1
Ai
2
R
CT
C
6
R
CT
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 зворотнім зв'язком (РРЗЗЗ) довжиною 19, 22 і 23. Виходом є логічна функція "ВИКЛЮЧНЕ АБО" - XOR трьох РРЗЗЗ. В 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, заснована 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 № 85039, МПК (2013.01) G09C 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 через постійні проміжки 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 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, згідно з корисною моделлю, перший регістр зсуву розділено на m частин, останні виходи m-1 частин першого регістра зсуву підключені до перших входів додатково введених m-1 елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з послідовними входами наступних частин першого регістра зсуву, додатково введені m-1 лічильників з програмованим коефіцієнтом ділення, виходи яких підключені до других входів додаткових елементів "ВИКЛЮЧНЕ АБО", синхровходи лічильників з програмованим коефіцієнтом ділення з'єднані з виходом тактового генератора, входи скидання лічильників з програмованим коефіцієнтом ділення підключені до другого

виходу блока керування, а інформаційні входи лічильників з програмованим коефіцієнтом ділення підключені у довільному порядку до виходів першого регістра зсуву.

Таким чином, введення у детермінований генератор псевдовипадкових послідовностей для потокового шифрування додаткових m-1 лічильників з програмованим коефіцієнтом ділення, додаткових m-1 елементів "ВИКЛЮЧНЕ АБО" та розділення першого регістра зсуву на m частин 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 через псевдовипадкові проміжки часу.

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 розділений на m частин перший регістр 1-1…1-m зсуву, мультиплексор 2, інформаційні входи якого у довільному порядку підключені до виходів першого регістра 1-1…1-m зсуву, а вихід мультиплексора 2 з'єднаний з першим входом елемента 3 "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого регістра 1-1…1-m зсуву, а вихід елемента 3 "ВИКЛЮЧНЕ АБО" з'єднано з послідовним входом першого регістра 1-1…1-m зсуву, другий регістр 4 зсуву, виходи якого підключені до входів паралельного завантаження першого регістра 1-1…1-m зсуву, тактовий генератор 5, вихід якого з'єднаний з синхровходами першого та другого регістрів 1-1…1-m, 4 зсуву і синхровходом першого лічильника 6, а його вихід підключено до входу другого 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 другого лічильників 6, 7 та до входу керування першого регістра 1-1…1-m зсуву, останні виходи m-1 частин першого регістра 1-1…1-m зсуву підключені до перших входів додаткових m-1 елементів 12-1…12-m-1 "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з послідовними входами наступних частин першого регістра 1-1…1-m зсуву, а другі входи додаткових m-1 елементів 12-1…12-m-1 "ВИКЛЮЧНЕ АБО" підключені до виходів m-1 лічильників 11-1…11-m-1 з програмованим коефіцієнтом ділення, синхровходи яких з'єднані з виходом тактового генератора 5, входи скидання лічильників 11-1…11-m-1 з програмованим коефіцієнтом ділення підключені до другого виходу блока 10 керування, інформаційні входи цих лічильників 11-1…11-m-1 підключені у довільному порядку до виходів першого регістра 1-1…1-m зсуву, а виходом пристрою є один із виходів першого регістра 1-1…1-m зсуву.

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 1-1…1-m зсуву. Для цього блок 10 керування формує логічний сигнал, який переводить перший регістр 1-1…1-m зсуву в режим паралельного завантаження, перший та другий лічильники 6,7 а також лічильники 11-1…11-m-1 з програмованим коефіцієнтом ділення утримується нульовому стані. Перед початком шифрування блок 10 керування переводить перший регістр 1-1…1-m зсуву в послідовний режим зсуву.

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

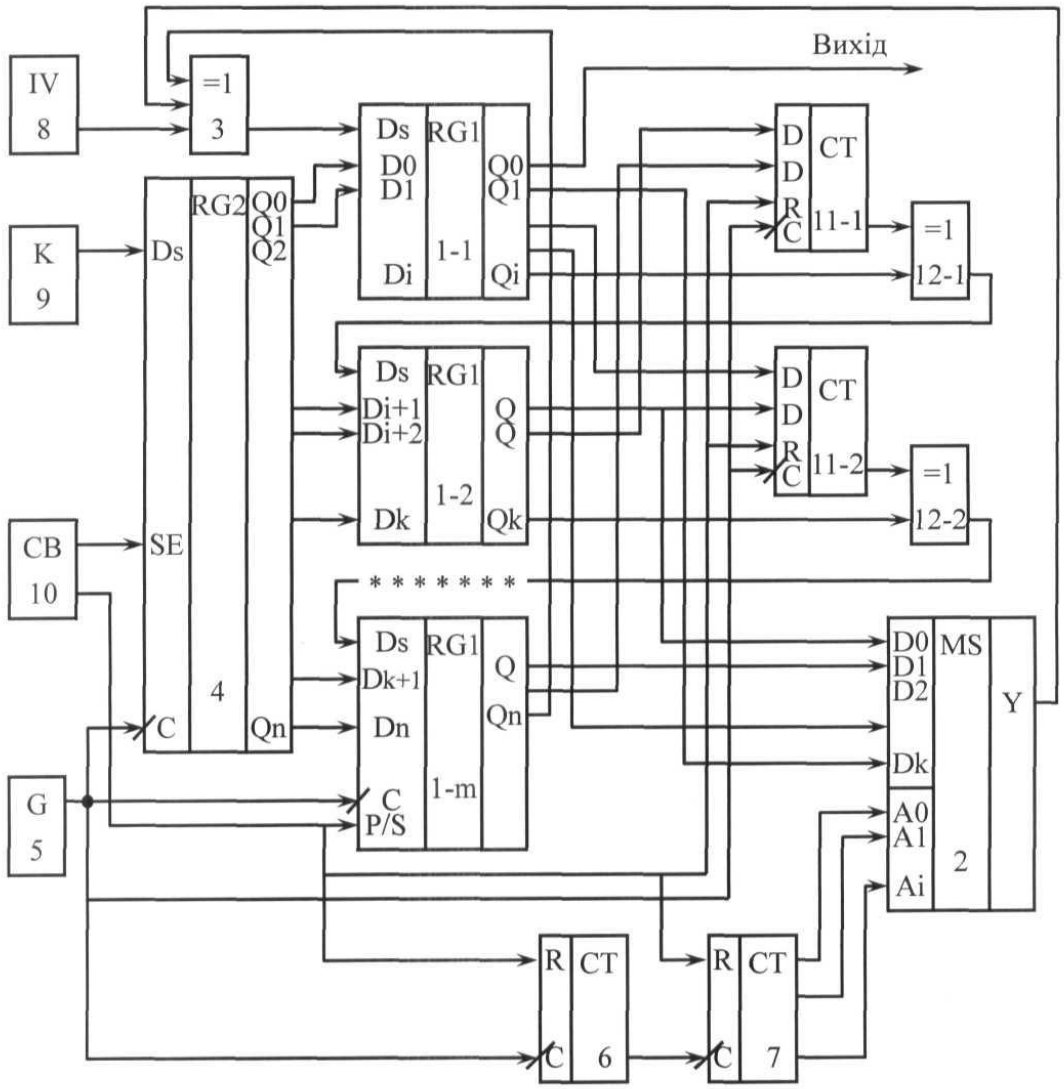
Тактовий генератор 5 визначає частоту зсуву першого та другого регістрів 1-1…1-m, 4 зсуву і таким чином визначає швидкість формування детермінованої псевдовипадкової послідовності.

Для зміни параметрів першого регістра 1-1…1-m зсуву логічні рівні з його проміжних виходів подаються у довільному порядку на інформаційні входи лічильників 11-1…11-m-1 для зміни їх коефіцієнтів ділення. Логічні рівні з виходів цих лічильників 11-1…11-m-1 подаються на другі

входи додаткових елементів 12-1…12-m-1 "ВИКЛЮЧНЕ АБО", які пропускають сигнали, що розповсюджуються в першому регістрі 1-1…1-m-1 зсуву, - з інверсією або без інверсії - в залежності від логічних рівнів вихідних сигналів лічильників 11-1…11-m-1 з програмованим коефіцієнтом ділення.

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 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, який **відрізняється** тим, що перший регістр зсуву розділено на m частин, останні виходи m - 1 частин першого регістра зсуву підключені до перших входів додатково введених m - 1 елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з послідовними входами наступних частин першого регістра зсуву, додатково введені m - 1 лічильників з програмованим коефіцієнтом ділення, виходи яких підключені до других входів додаткових елементів "ВИКЛЮЧНЕ АБО", синхровходи лічильників з програмованим коефіцієнтом ділення з'єднані з виходом тактового генератора, входи скидання лічильників з програмованим коефіцієнтом ділення підключені до другого виходу блока керування, а інформаційні входи лічильників з програмованим коефіцієнтом ділення підключені у довільному порядку до виходів першого регістра зсуву.



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