



УКРАЇНА

(19) **UA** (11) **109675** (13) **U**
(51) МПК (2016.01)
G09C 5/00
G06F 7/58 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

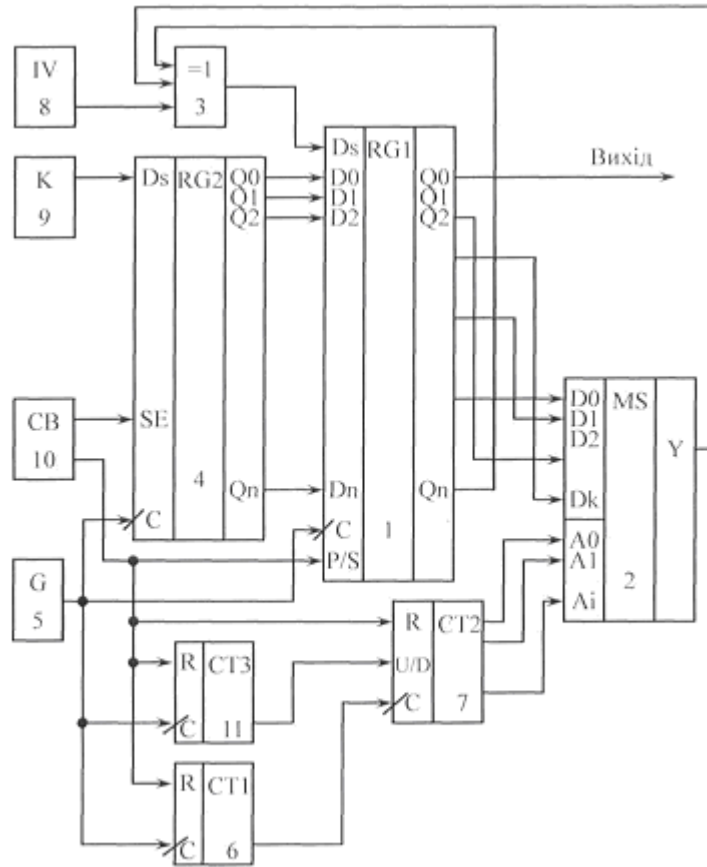
(21) Номер заявки: u 2016 03214	(72) Винахідник(и): Торба Александр Алексєєвич (UA), Бобух Всеволод Анатолійович (UA), Торба Максим Олегович (UA), Торба Олександр Олегович (UA), Торба Дмитро Дмитрович (UA)
(22) Дата подання заявки: 28.03.2016	
(24) Дата, з якої є чинними права на корисну модель: 25.08.2016	
(46) Публікація відомостей про видачу патенту: 25.08.2016, Бюл.№ 16	(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, 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 входу скидання першого лічильника та до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву. Додатково введені другий реверсний лічильник та третій лічильник, у яких входи скидання підключені до другого виходу блока керування. Синхровхід другого реверсивного лічильника з'єднаний з виходом першого лічильника, а його виходи підключені до адресних входів мультиплексора. Синхровхід третього лічильника з'єднано з виходом тактового генератора. Вихід третього лічильника підключено до входу перемикачів режимів другого реверсивного лічильника.

UA 109675 U



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 (PP333) довжиною 19, 22 і 23. Виходом є логічна функція "ВИКЛЮЧНЕ АБО" - XOR трьох PP333. 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 PP333.

Недоліком цього апаратного алгоритму є недостатня криптостійкість тому, що існує тривіальна атака на відкритому тексті (алгоритм Берлекемпа-Мессі), заснована на припущенні про зміст перших двох PP333 і спробі визначення третього PP333 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) 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 криптостійкість псевдовипадкових послідовностей, що генеруються, тому, що довгострокові таємні параметри змінюються в постійному порядку.

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 криптостійкість 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 регістру зсуву, тактовий генератор, вихід якого з'єднаний з синхровходами першого й другого регістрів зсуву та першого лічильника, 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 входу скидання першого лічильника та до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву згідно з корисною моделлю, додатково введені другий реверсний лічильник та третій лічильник, у яких входи скидання підключені до другого виходу блока керування, синхровхід другого реверсивного лічильника з'єднаний з виходом першого лічильника, а його виходи підключені до адресних входів мультиплексора, синхровхід третього лічильника з'єднано з виходом тактового генератора, а вихід третього лічильника підключено до входу перемикачів режимів другого реверсивного лічильника.

Таким чином, введення у детермінований генератор псевдовипадкових послідовностей для потокового шифрування додаткових другого реверсивного та третього лічильників, 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 порядку збільшення або зменшення.

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

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування містить перший реєстр 1 зсуву, мультиплексор 2, інформаційні входи якого у довільному порядку підключені до виходів першого реєстра 1 зсуву, а вихід мультиплексора 2 з'єднаний з першим входом елемента 3 "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого реєстра 1 зсуву, а вихід елемента 3 "ВИКЛЮЧНЕ АБО" з'єднано з послідовним входом першого реєстра 1 зсуву, другий реєстр 4 зсуву, виходи якого підключені до входів паралельного завантаження першого реєстра 1 зсуву, тактовий генератор 5, вихід якого з'єднаний з синхреходами першого та другого реєстрів 1, 4 зсуву і синхреходами першого та третього лічильників 6, 11, вихід першого лічильника 6 підключено до синхреходу другого 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 реєстра 4 зсуву, та блок 10 керування, перший вихід якого з'єднано з входом керування другого реєстра 4 зсуву, а другий вихід блока 10 керування підключено до входів скидання першого, другого реверсивного та третього лічильників 6, 7, 11 та до входу керування першого реєстра 1 зсуву, вихід третього лічильника 11 підключено до входу перемикачів режимів другого реверсивного лічильника 7, виходом пристрою є один із виходів першого реєстра зсуву.

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування працює наступним чином.

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

Шифрування починається з передавання випадкового значення ініціалізації IV, яке одночасно в послідовному форматі вводиться в перший реєстр 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 реєстра 1 зсуву та виходу мультиплексора 2 для формування рекурентної псевдовипадкової послідовності.

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

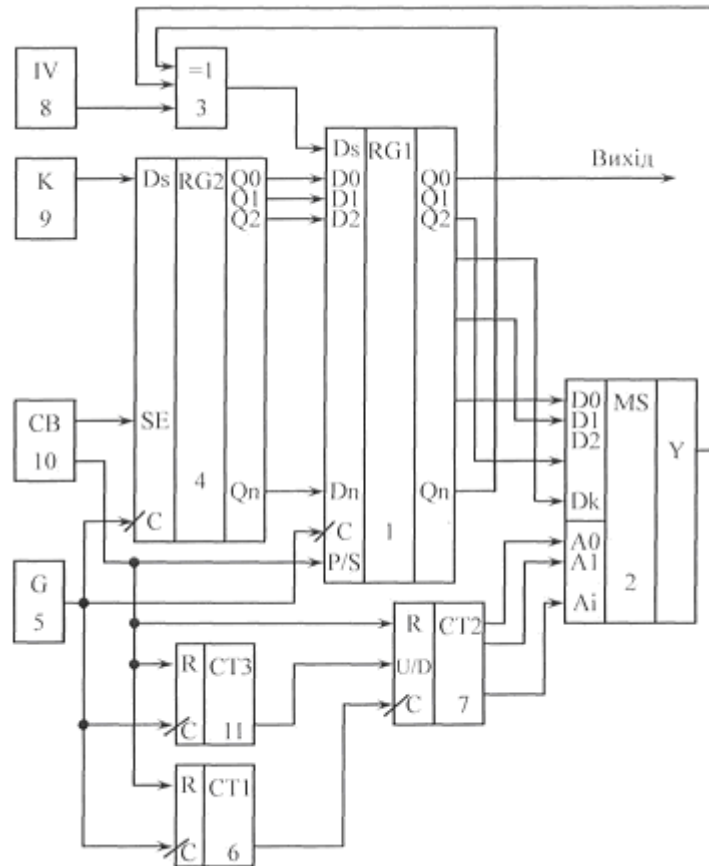
Для зміни параметрів рекуренти першого реєстра 1 зсуву логічні рівні з його проміжних виходів подаються па інформаційні входи мультиплексора 2, вихід якого підключено до другого входу першого елемента 3 "ВИКЛЮЧНЕ АБО". Адресні входи мультиплексора 2 підключені до виходів другого реверсивного лічильника 7, синхрехід якого з'єднаний з виходом першого лічильника 6. Третій лічильник 11 формує часові інтервали, через які другий реверсивний лічильник 7 перемикається у режим збільшення або зменшення.

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

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Детермінований генератор псевдовипадкових послідовностей для потокового шифрування, що містить перший реєстр зсуву, мультиплексор, інформаційні входи якого у довільному порядку підключені до виходів першого реєстра зсуву, а вихід мультиплексора з'єднаний з першим входом елемента "ВИКЛЮЧНЕ АБО", другий вхід якого підключено до останнього виходу першого реєстра зсуву, а вихід елемента "ВИКЛЮЧНЕ АБО" з'єднано з послідовним входом першого реєстра зсуву, другий реєстр зсуву, виходи якого підключені до входів паралельного завантаження першого реєстра зсуву, тактовий генератор, вихід якого з'єднаний з

синхривходами першого й другого регістрів зсуву та першого лічильника, 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 входу скидання першого лічильника та до входу керування першого регістра зсуву, а виходом пристрою є один із виходів першого регістра зсуву, який **відрізняється** тим, що додатково введені другий реверсний лічильник та третій лічильник, у яких входи скидання підключені до другого виходу блока керування, синхривхід другого реверсивного лічильника з'єднаний з виходом першого лічильника, а його входи підключені до адресних входів мультиплексора, синхривхід третього лічильника з'єднано з виходом тактового генератора, а вихід третього лічильника підключено до входу перемикавання режимів другого реверсивного лічильника.



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