УКРАЇНА

(19) UA (11) 97734 (13) U

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

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **a 2014 00478**

(22) Дата подання заявки: **20.01.2014**

(24) Дата, з якої є чинними права на корисну модель: **10.04.2015**

(46) Публікація відомостей про видачу патенту: **10.04.2015, Бюл.№ 7**

(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, другий регістр зсуву, тактовий генератор, синхровхід лічильника, блок формування випадкового значення ініціалізації, блок формування сеансових ключів, блок керування. Додатково введені n-1 перших лічильників, синхровходи яких з'єднані з виходом тактового генератора. Виходи n-1 перших лічильників з'єднані з синхровходами додатково введених n-1 других лічильників. Виходи других лічильників підключені до адресних входів додатково введених n-1 мультиплексорів, у яких інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву. Виходи n-1 мультиплексорів з'єднані з додатковими n-1 входами елемента "ВИКЛЮЧНЕ АБО".

UA 97734 U

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

Відомий аналог є 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 (РР333) довжиною 19, 22 і 23. Виходом є логічна функція "ВИКЛЮЧНЕ АБО" - XOR трьох РР333. 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 РР333.

Недоліком аналога є недостатня криптостійкість тому, що існує тривіальна атака на відкритому тексті, заснована на припущенні про зміст перших двох РР333 і спробі визначення третього РР333 по ключовій послідовності.

Найбільш близьким аналогом до корисної моделі 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 найближчого аналога є недостатня крипостійкість псевдовипадкових послідовностей, що генеруються, тому, що у довільному порядку змінюється тільки один довгостроковий таємний параметр.

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, вихід мультиплексора з'єднаний з першим входом елемента "ВИКЛЮЧНЕ АБО", а вихід цього елемента 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, а також з синхровходом першого лічильника, вихід якого з'єднаний з синхровходом другого лічильника, а його виходи підключені до адресних входів мультиплексора, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з останнім 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, згідно з корисною моделлю, додатково введені n-1 перших лічильників, синхровходи яких з'єднані з виходом тактового генератора, а виходи n-1 перших лічильників з'єднані з синхровходами додатково введених n-1 других лічильників, виходи других лічильників підключені до адресних входів додатково введених n-1 мультиплексорів, у яких інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а виходи n-1 мультиплексорів з'єднані з додатковими n-1 входами елемента "ВИКЛЮЧНЕ АБО".

Таким чином, введення у детермінований генератор псевдовипадкових послідовностей для потокового шифрування додаткових n-1 перших та других лічильників, та додаткових n-1 мультиплексорів, 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 змін довгострокових таємних параметрів.

Корисна модель пояснюється кресленням, де зображена структурна схема детермінованого генератора псевдовипадкових послідовностей для потокового шифрування. На креслені 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, n мультиплексор 2-1…2-n, інформаційні входи яких у довільному порядку підключені до виходів першого регістра 1 зсуву, а виходи мультиплексорів 2-1…2-n з'єднані з n входами елемента 3 "ВИКЛЮЧНЕ АБО", вихід якого підключено до послідовного входу 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 й синхровходами перших лічильників 6-1…6-n, а їх виходи підключено до синхровходів других лічильників 7-1…7-n, виходи яких з'єднані з адресними входами мультиплексорів 2-1…2-n, блок 8 формування випадкового значення ініціалізації, вихід якого підключено до n+1 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 входу керування першого регістра 1 зсуву, та до входів скидання перших лічильників 6-1…6-n та других лічильників 7-1…7-n, а виходом пристрою є будь-який вихід першого регістра 1 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, перші лічильники 6-1…6-n та другі лічильники 7-1…7-n утримуються 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 n+1 вхід першого елемента 3 "ВИКЛЮЧНЕ АБО". На перші n входи елемента 3 "ВИКЛЮЧНЕ АБО" подаються сигнали з виходів мультиплексорів 2-1…2-n 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.

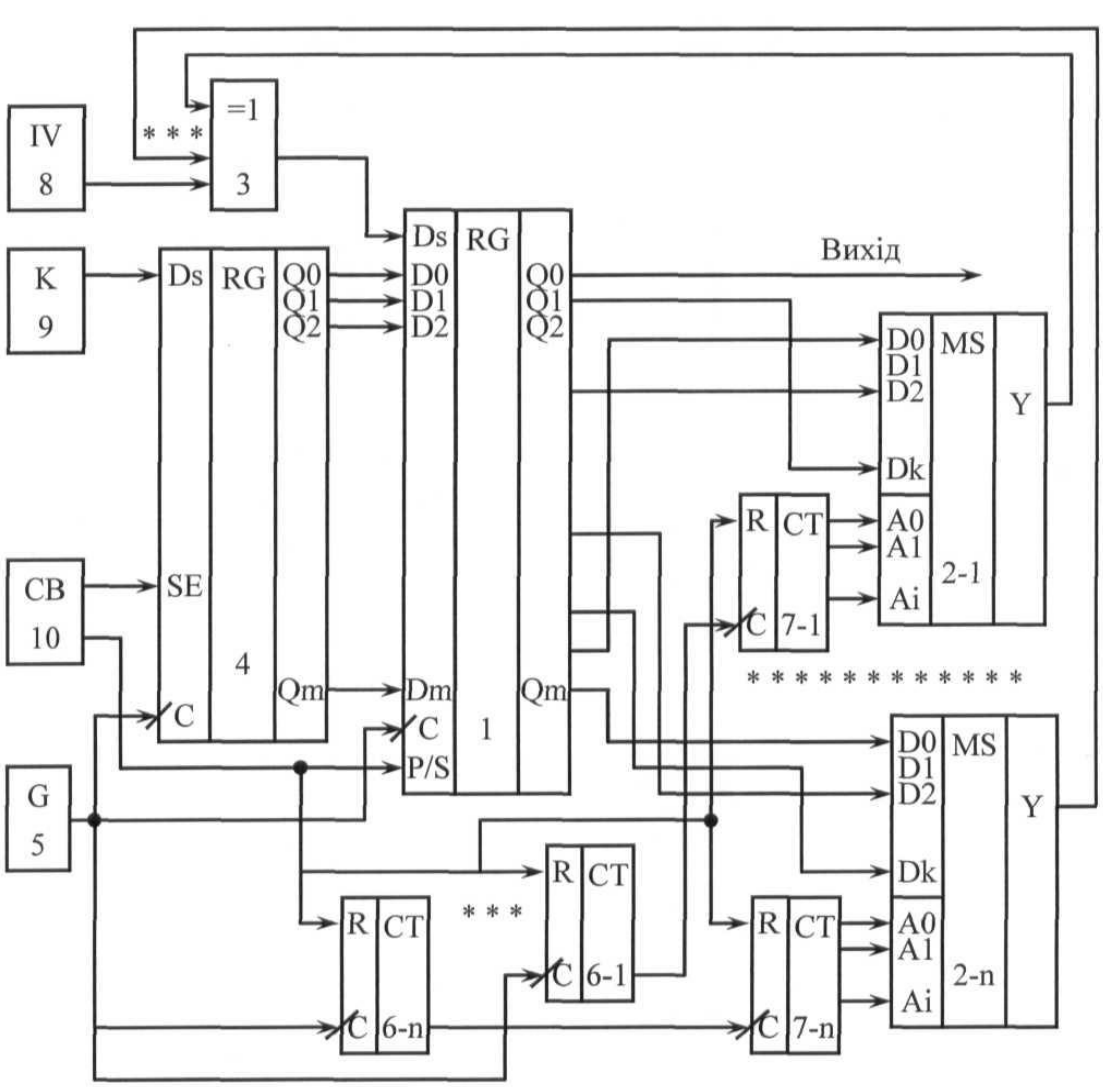
Для зміни параметрів рекуренти першого регістра 1 зсуву логічні рівні з його проміжних виходів подаються на інформаційні входи мультиплексорів 2-1…2-n, виходи яких підключені до n входів елемента 3 "ВИКЛЮЧНЕ АБО". Таким чином постійно змінюються у псевдовипадковому порядку усі параметри рекуренти - довжина регістра 1 зсуву та номери його відводів.

Коефіцієнти ділення перших лічильників 6-1…6-n треба обирати різними, та ці коефіцієнти повинні бути простими числами.

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, вихід мультиплексора з'єднаний з першим входом елемента "ВИКЛЮЧНЕ АБО", а вихід цього елемента 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, а також з синхровходом першого лічильника, вихід якого з'єднаний з синхровходом другого лічильника, а його виходи підключені до адресних входів мультиплексора, блок формування випадкового значення ініціалізації, вихід якого з'єднаний з останнім 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, який **відрізняється** тим, що додатково введені n-1 перших лічильників, синхровходи яких з'єднані з виходом тактового генератора, а виходи n-1 перших лічильників з'єднані з синхровходами додатково введених n-1 других лічильників, виходи других лічильників підключені до адресних входів додатково введених n-1 мультиплексорів, у яких інформаційні входи підключені у довільному порядку до виходів першого регістра зсуву, а виходи n-1 мультиплексорів з'єднані з додатковими n-1 входами елемента "ВИКЛЮЧНЕ АБО".



Комп'ютерна верстка Д. Шеверун

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

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