УКРАЇНА **(19) UA** **(11) 153398** **(13) U**

(51) МПК (2023.01)
G06F 7/00
G06F 7/58 (2006.01)
G07C 15/00

НАЦІОНАЛЬНИЙ ОРГАН ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЕРЖАВНА ОРГАНІЗАЦІЯ "УКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ОФІС ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ТА ІННОВАЦІЙ"

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2022 05115**
(22) Дата подання заявки: **29.12.2022**
(24) Дата, з якої є чинними права інтелектуальної власності: **29.06.2023**
(46) Публікація відомостей про державну реєстрацію: **28.06.2023, Бюл.№ 26**

(72) Винахідник(и):
Торба Алєксандр Алєксєєвіч (UA),
Ткачов Віталій Миколайович (UA),
Дяченко Владислав Олександрович (UA),
Партика Станіслав Олександрович (UA),
Єрошенко Ольга Артурівна (UA)

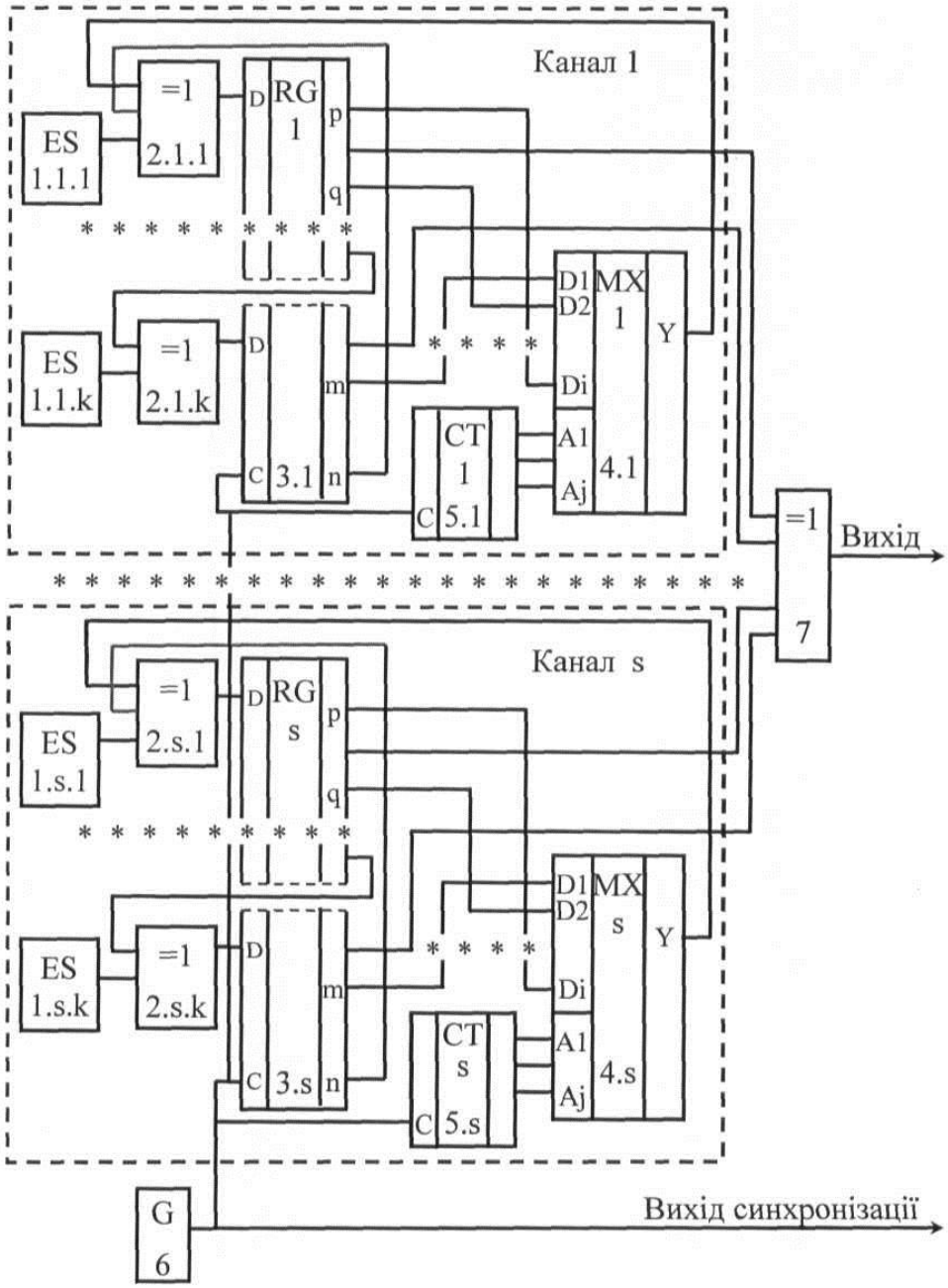
(73) Володілець (володільці):
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ,
пр. Науки, 14, м. Харків, 61166 (UA)

(54) НЕДЕТЕРМІНОВАНИЙ ГЕНЕРАТОР ВИПАДКОВИХ БІТІВ

(57) Реферат:

Недетермінований генератор випадкових бітів має канал перетворення сигналів з виходів джерел ентропії у випадкові біти, який складається з k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО". Другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву. Третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і лічильника імпульсів. Додатково введені ще декілька каналів перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти з аналогічними компонентами, а також введено ще один елемент "ВИКЛЮЧНЕ АБО", на входи якого подаються сигнали з декількох проміжних виходів регістрів зсуву у кожному каналі, а вихід цього елементу "ВИКЛЮЧНЕ АБО" є виходом всього пристрою. При цьому тактовий генератор є спільним для усіх каналів перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти. Вихід тактового генератора підключений до синхровходів регістрів зсуву та лічильників імпульсів в усіх каналах перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти і вихід тактового генератора є виходом синхронізації всього пристрою.

UA 153398 U


Канал 1
ES 1.1.1
=1 2.1.1
D RG 1 p q
ES 1.1.k
=1 2.1.k
D m C 3.1 n
D1 D2 MX 1 Y Di
A1 CT 1 Aj 4.1
C 5.1
=1 7
Вихід
Канал s
ES 1.s.1
=1 2.s.1
D RG s p q
ES 1.s.k
=1 2.s.k
D m C 3.s n
D1 D2 MX s Y Di
A1 CT s Aj 4.s
C 5.s
G 6
Вихід синхронізації

Корисна модель належить до області обчислювальної техніки і може бути використана в системах захисту інформації обчислювальних систем, наприклад при генерації параметрів алгоритмів криптографічного перетворення, в протоколах аутентифікації, в засобах імовірнісного кодування та ін.

Відомий генератор рівномірно розподілених випадкових послідовностей (див. патент на корисну модель України № 50386 А, МПК6 G06F 7/58, G07C 15/00, опублікований 15.10.2002, Бюл. № 10), що містить n джерел ентропії, які складаються з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, виходи джерел ентропії підключені до перших входів n елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з входами регістра зсуву, поділеного на n частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", входи першого елемента "ВИКЛЮЧНЕ АБО" з'єднані з останнім виходом регістра зсуву та проміжним виходом цього регістра, виходи регістра зсуву підключені до входів вихідного паралельного регістра, а його виходи підключені до шини даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і входом лічильника імпульсів, вихід якого під'єднай до синхровходу вихідного паралельного регістра та входу тригера "прапора", а його вихід з'єднаний з входом запиту переривання ПЕОМ і через буферний елемент "І" з шиною даних ПЕОМ, та дешифратор адреси, включений входами до шини адреси ПЕОМ, а першим виходом до входу дозволу вихідного регістра і входу скидання тригера "прапора", і другим виходом до буферного елемента "І".

Недоліком цього генератора є його низька надійність роботи з-за недостатньої крипостійкості у випадку повного збою усіх джерел ентропії.

Найближчим аналогом по сукупності ознак є генератор випадкових бітових послідовностей на основі ЛРР зі змінами параметрів рекуренти (див. рисунок 6.4 в монографії: Торба А.А. Методы и средства генерации случайных битовых последовательностей: Под ред. д.т.н., проф. Горбенко И.Д. / А.А.Торба, А.А. Бобкова, Ю.И. Горбенко, В.А. Бобух. - Харьков: Изд-во "Форт", 2012. - 232 с.), що містить k джерел ентропії, підключених до перших входів елементів "ВИКЛЮЧНЕ АБО", виходи яких з'єднані з проміжними входами регістра зсуву, поділеного на k частин, а останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора.

Цей генератор рівномірно розподілених випадкових бітових послідовностей має достатню надійність роботи за рахунок гарячого резервування джерел ентропії, а також достатню крипостійкість у випадку повного збою усіх джерел ентропії згідно з Міжнародним стандартом ISO/IEC 18031:2005, але цей генератор буде нероботоспроможним при несправності одного з цифрових блоків.

В основу корисної моделі поставлена задача створення такого недетермінованого генератора випадкових бітів, в якому додавання нових схемних елементів і зв'язків дозволило б підвищити надійність роботи за рахунок гарячого резервування цифрових каналів перетворення сигналів джерел ентропії в вихідні випадкові біти.

Поставлена задача вирішується тим, що у недетермінований генератор випадкових бітів, що містить канал перетворення сигналів з виходів джерел ентропії у випадкові біти, який складається з k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і лічильника імпульсів, згідно з корисною моделлю, додатково введені ще декілька каналів перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти з аналогічними компонентами, а також введено ще один елемент "ВИКЛЮЧНЕ АБО", на входи якого подаються сигнали з декількох проміжних виходів регістрів зсуву у кожному каналі, а вихід цього елементу "ВИКЛЮЧНЕ АБО" є виходом всього пристрою, а також тактовий генератор є спільним для усіх каналів перетворення сигналів з виходів додаткових джерел ентропії у

випадкові біти, вихід тактового генератора підключений до синхровходів регістрів зсуву та лічильників імпульсів в усіх каналах перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти і вихід тактового генератора є виходом синхронізації всього пристрою.

На кресленні зображена структурна схема недетермінованого генератора випадкових бітів. На кресленні використані наступні міжнародні позначення: ES - джерело ентропії, RG - регістр, MS - мультиплексор, G - генератор, CT - лічильник.

Недетермінований генератор випадкових бітів містить s каналів, кожен з яких складається з джерел 1.1.1-1.1.k…1.s.1-1.s.k ентропії, виходи яких підключені до перших входів елементів 2.1.1-2.1.k…2.s.1-2.s.k "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістрів 3.1…3.s зсуву, поділених на k частин (необов'язково рівних), останні виходи кожної частини регістрів 3.1…3.S зсуву підключені до других входів наступних елементів 2.1.1-2.1.k…2.s.1-2.s.k "ВИКЛЮЧНЕ АБО", другий вхід перших елементів 2.1.1…2.S.1 "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістрів 3.1…3.S зсуву, а третій вхід перших елементів 2.1.1…2.S.1 "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексорів 4.1…4.S, інформаційні входи яких підключені до проміжних виходів регістрів 3.1…3.S зсуву у довільному порядку, і лічильники 5.1…5.S імпульсів, останні виходи яких підключені до адресних входів мультиплексорів 4.1…4.S, а також тактовий генератор 6, вихід якого з'єднаний з синхровходами регістрів 3.1…3.s зсуву і лічильників 5.1…5.S імпульсів. Цей тактовий генератор 6 є єдиним для усіх каналів, а вихід цього тактового генератора 6 є виходом синхронізації всього пристрою. Входи вихідного елемента 7 "ВИКЛЮЧНЕ АБО" підключені у довільному порядку до декількох проміжних виходів регістрів 3.1…3.s усіх каналів, а вихід цього вихідного елемента 7 "ВИКЛЮЧНЕ АБО" є виходом всього пристрою.

Недетермінований генератора випадкових бітів працює наступним чином.

На виходах джерел 1.1.1-1.1.k…1.S.1-1.s.k ентропії формуються логічні рівні, які з рівною імовірністю приймають значення нуля або одиниці в випадкові моменти часу. Ці випадкові логічні рівні перемикають на протилежні значення логічні рівні, що подаються з останніх виходів частин регістрів 3.1…3.s зсуву в кожному каналі до входів наступних частин цих регістрів, в випадкові моменти часу за допомогою елементів 2.1.1-2.1.k…2.s.1-2.s.k "ВИКЛЮЧНЕ АБО". Тактовий генератор 6 визначає частоту зсуву випадкових бітів в регістрах 3.1…3.S зсуву і таким чином визначає швидкість формування випадкових бітів, які за рахунок дії джерел I.1.1-1.1.k…1.s.1-1.s.k ентропії стають непередбачуваними, недетермінованими.

Для зміни параметрів рекуренти регістрів 3.1…3.S зсуву їх логічні рівні з проміжних виходів подаються на інформаційні входи мультиплексорів 4.1…4.S, виходи яких підключені до третіх входів елементів 2.1.1…2.S.1 "ВИКЛЮЧНЕ АБО". Адресні входи мультиплексорів 4.1…4.S підключені до останніх виходів лічильників 5.1….5.s імпульсів.

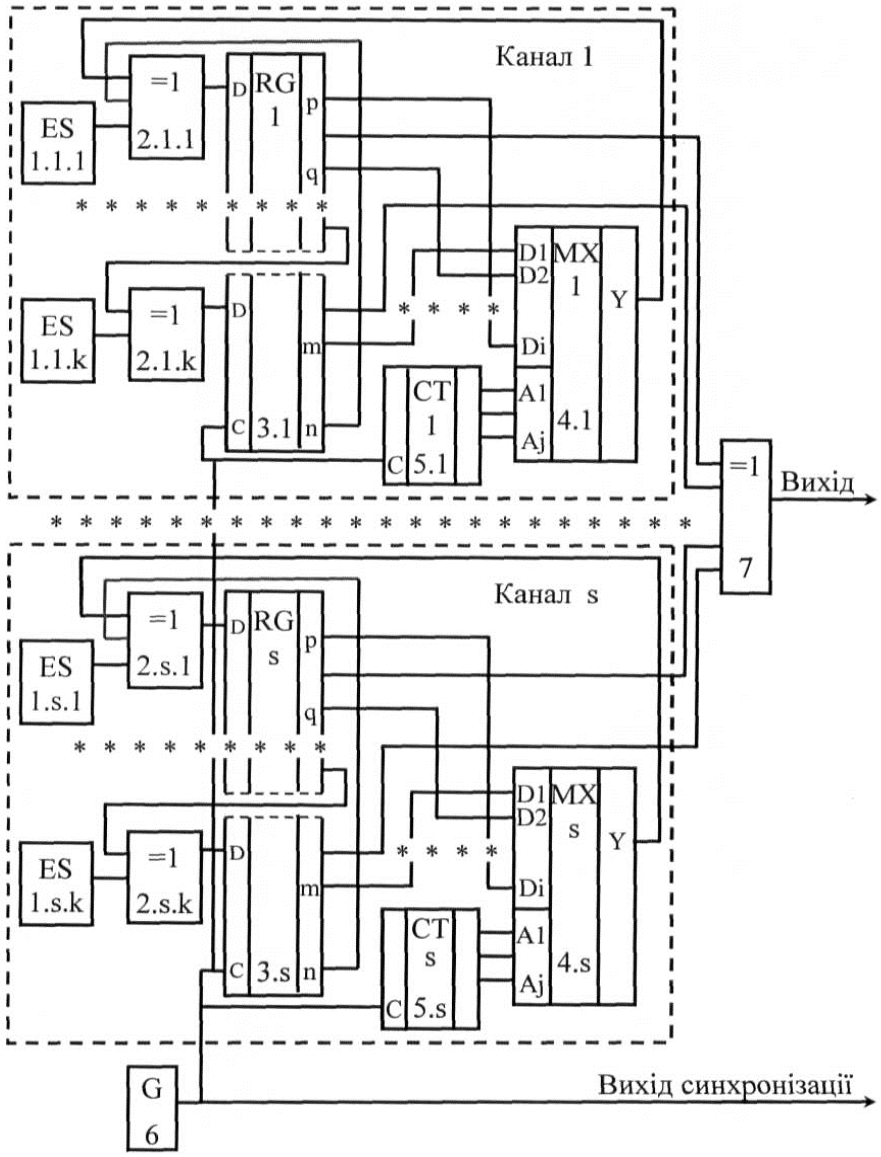
Декілька проміжних виходів регістрів 3.1…3.S зсуву кожного каналу об'єднуються вихідним елементом 7 "ВИКЛЮЧНЕ АБО". Це забезпечує гаряче резервування каналів перетворення сигналів з виходів джерел ентропії у випадкові біти, тобто при роботоспроможності хоча б одного каналу - на виході пристрою будуть формуватися недетерміновані випадкові біти, які проходять усі тести випадковості та рівноймовірності.

Таким чином, вирішена поставлена задача створення такого недетермінованого генератора випадкових бітів, в якому додавання нових схемних елементів і зв'язків дозволило підвищити надійність роботи за рахунок гарячого резервування цифрових каналів перетворення сигналів джерел ентропії в вихідні випадкові біти.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Недетермінований генератор випадкових бітів, що містить канал перетворення сигналів з виходів джерел ентропії у випадкові біти, який складається з k джерел ентропії, виходи яких підключені до перших входів k елементів "ВИКЛЮЧНЕ АБО", а їх виходи з'єднані з проміжними входами регістра зсуву, поділеного на k частин, останні виходи кожної частини регістра зсуву підключені до других входів наступних елементів "ВИКЛЮЧНЕ АБО", другий вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з останнім виходом регістра зсуву, а третій вхід першого елемента "ВИКЛЮЧНЕ АБО" з'єднаний з виходом мультиплексора, інформаційні входи якого підключені до проміжних виходів регістра зсуву у довільному порядку, і лічильника імпульсів, останні виходи якого підключені до адресних входів мультиплексора, а також тактовий генератор, вихід якого з'єднаний з синхровходами регістра зсуву і лічильника імпульсів, який **відрізняється** тим, що додатково введені ще декілька каналів перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти з аналогічними компонентами, а також введено ще один елемент "ВИКЛЮЧНЕ АБО", на входи якого подаються сигнали з декількох проміжних

виходів регістрів зсуву у кожному каналі, а вихід цього елемента "ВИКЛЮЧНЕ АБО" є виходом всього пристрою, а також тактовий генератор є спільним для усіх каналів перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти, вихід тактового генератора підключений до синхровходів регістрів зсуву та лічильників імпульсів в усіх каналах перетворення сигналів з виходів додаткових джерел ентропії у випадкові біти і вихід тактового генератора є виходом синхронізації всього пристрою.



Комп'ютерна верстка С. Чулій

ДО "Український національний офіс інтелектуальної власності та інновацій", вул. Глазунова, 1, м. Київ – 42, 01601