

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

Відомий генератор випадкових чисел (Деклараційний патент України № 68912 А, опубл. Бюл. №8, 16.08.2004), що містить багатоканальний вузол генерації випадкових бітів, кожен канал якого складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача та лічильного тригера, перший паралельний регістр, входи якого під'єднані до виходів лічильних тригерів, а виходи - до входів елемента «ВИКЛЮЧНЕ АБО», і вузол спраження з ПЕОМ, який включає в себе регістр зсуву, вхід даних якого з'єднаний з виходом елемента «ВИКЛЮЧНЕ АБО», виходи регістра зсуву увімкнуті до входів вихідного паралельного регістру, з'єданого виходами з шиною даних ПЕОМ, тактовий генератор, вихід якого з'єднаний з синхровходами першого паралельного регістру і регістру зсуву а також з входом лічильника імпульсів, вихід якого під'єднаний до синхровходу вихідного паралельного регістру та входу тригера «прапора», вихід якого з'єднаний з виходом запиту переривання ПЕОМ та через буферний елемент І з шиною даних ПЕОМ, і дешифратор адреси, включений входами до шини адреси ПЕОМ, першим виходом до входу дозволу вихідного регістру і входу скидання тригера «прапора», а другим виходом до буферного елементу І.

Недоліком цього генератора є можливість виникнення „метастабільних станів" в тригерах першого паралельного регістру при зміні логічних рівнів на виходах лічильних тригерів під час запису станів цих логічних рівнів в перший паралельний регістр. „Метастабільні стани" закінчуються, зазвичай, встановленням нульового стану на виходах тригерів першого паралельного регістру. Тому імовірність нульових бітів на виходах першого паралельного регістру більше імовірності одиничних бітів за умови рівних імовірностей станів на виходах лічильних тригерів.

Найбільш близьким по сукупності ознак є генератор послідовності випадкових чисел (Патент Російської Федерації № 2191421, МПК G06F 7/58, H03K 3/84 від 20.10.2002), що містить двоканальний вузол генерації випадкових бітів, кожен канал якого включає в себе послідовно з'єднані генератор шуму, підсилювач-обмежувач, елемент І, лічильний тригер і D-тригер, виходи двох каналів з'єднані з входами елемента "ВИКЛЮЧНЕ АБО", вихід якого є інформаційним виходом пристрою, а також генератор тактових імпульсів, перший вихід якого з'єднано з другими входами елементів І, а другий вихід генератора тактових імпульсів увімкнутий до схем формування імпульсів скидання лічильних тригерів та формування сигналу готовності.

Усунення метастабільних станів у вихідних D-тригерах досягається зупинкою роботи лічильних тригерів (за рахунок блокування вхідних випадкових імпульсів на їхніх входах) перед записом логічних станів цих тригерів у вихідні D-тригери. Але таке схемне рішення призводить до зменшення швидкодії усього генератора випадкових чисел у кількість разів, що є зворотна до шпаруватості імпульсів на першому виході генератора тактових імпульсів.

В основу винаходу поставлена задача створення такого генератора рівномірно розподілених випадкових бітів, у якого нове схемне рішення дозволило б усунути метастабільні стани у вихідних D-тригерах без зменшення швидкодії усього пристрою.

Такий технічний результат може бути досягнутий, якщо в генератор рівномірно розподілених випадкових бітів, що містить двоканальний вузол формування випадкових бітів, кожен канал якого складається з послідовно з'єднаних генератора шуму, підсилювача-обмежувача лічильного тригера та вихідного D-тригера, виходи D-тригерів підключені до входів елемента "ВИКЛЮЧНЕ АБО", вихід якого з'єднаний з виходом пристрою, а також генератор тактових імпульсів, вихід якого підключено до входів синхронізації D-тригерів, згідно винаходу, кількість каналів формування випадкових бітів може бути " $n \geq 2$ " і в кожен канал додатково введені тригери-засувки, входи яких з'єднані з виходами лічильних тригерів, а виходи - з входами D-тригерів, входи синхронізації тригерів-засувок підключені до виходу генератора тактових імпульсів.

Таким чином, введення в кожен канал тригерів-засувок, які при одиничному стані на своєму синхровході працюють як повторювачі вхідних логічних рівнів, а при нульовому стані на своєму синхровході вони "заморожують" свій вихідний логічний стан, дозволяє уникнути "метастабільних станів" в D-тригерах під час запису в них логічних рівнів з виходів тригерів-засувок. Робота лічильних тригерів в кожному каналі не блокується під час запису їх станів, тому швидкодія усіх каналів не зменшується. Збільшення кількості каналів до $n \geq 2$ дозволяє збільшити надійність роботи всього пристрою за рахунок гарячого резервування формувачів випадкових бітів в кожному каналі, а також поліпшити статистичні властивості випадкових бітів, що генеруються.

На рисунку зображена структурна схема генератора рівномірно розподілених випадкових бітів.

Генератор рівномірно розподілених випадкових бітів містить n каналів формування випадкових бітів, в кожному каналі послідовно з'єднані генератор 1.1...1. n шуму, підсилювач-обмежувач 2.1...2. n , лічильний тригер 3.1. ...3. n , тригер-засувка 4.1...4. n і вихідний D-тригер 5.1...5. n , де $n \geq 2$ - кількість каналів. Виходи D-тригерів кожного каналу під'єднані до входів елемента "ВИКЛЮЧНЕ АБО" 6, а його вихід є виходом пристрою. Вихід генератора 7 тактових імпульсів з'єднано з синхровходами усіх тригерів-засувок 4.1 ...4. n і D-тригерів 5.1 ...5. n .

Генератор рівномірно розподілених випадкових бітів працює слідуючим чином. На виходах генераторів шуму 1.1...1. n формуються імпульси випадкової амплітуди, наступні через випадкові часові інтервали. Амплітуди цих імпульсів підсилювачами-обмежувачами 2.1...2. n перетворюються в логічні рівні КМОН мікросхем. Для вирівнювання ймовірностей в кожний канал введені лічильні тригери 3.1...3. n , вихідні сигнали яких з рівною ймовірністю знаходяться в стані логічного нуля і логічної одиниці.

Вихідні рівні лічильних тригерів 3.1...3. n подаються через тригери-засувки 4.1...4. n до інформаційних входів D-тригерів 5.1...5. n і запам'ятовуються у цих D-тригерах 5.1...5. n під час наростаючого фронту вихідного імпульсу генератора 7 тактових імпульсів. Вихідні логічні рівні усіх каналів об'єднуються елементом "ВИКЛЮЧНЕ АБО" 6.

Для запобігання "метастабільних станів" у D-тригерах 5.1...5. n вихідний імпульс генератора 7 тактових імпульсів подається також і на синхровходи тригерів-засувок 4.1...4. n , заморожуючи своїм нульовим рівнем їх стан перед записом у вихідні D-тригери 5.1...5. n .

