

1. Спосіб генерації псевдовипадкових чисел, що включає ініціалізацію, циклічну генерацію шляхом додавання в цифровій сітці довжини  $L$ , перетворення результатів додавання в постійній та оперативній пам'яті, який **відрізняється** тим, що:

- циклічно змінюють адреси операндів і результату додавання у циклі генерації,
- залишають не використаною частину поточного операнда,
- зберігають як стартові, так і поточні початкові значення, що змінюються з перетворенням кожної порції даних,
- незалежність перетворень різних повідомлень забезпечують холостою прокруткою генератора чисел між перетворенням порцій даних,
- застосовують декілька незалежних пар початкових значень відповідно до призначення основного генератора,
- автоматично враховують використання корисної довжини періоду за збереженими значеннями її невикористаної частини і розмірами перетворених порцій даних,
- при вичерпанні корисної довжини періоду основного генератора її автоматично відновлюють при звертанні до внутрішнього генератора псевдовипадкових чисел,
- відновлення початкових значень здійснюють зміною частини не використовуваної частини поточних операндів, зберігаючи принаймні один старший біт, наступний за ключем, частиною, що використовується при перетворенні даних,
- нетривіальні початкові значення послідовності операндів основного генератора чисел визначають за допомогою внутрішнього генератора,
- визначають початкові значення внутрішнього генератора за двома парами стандартних початкових значень, отримуючи щонайменше дві пари його незалежних початкових значень припиненням ініціювання для кожної пари в довільний момент часу після початку ініціювання,
- автоматично перевіряють і коригують молодші біти початкових значень внутрішнього і основного генераторів псевдовипадкових чисел,
- автоматично запобігають появі значної кількості нульових кодів перетворення і/або нульових початкових значень основного генератора перестановкою початкових значень внутрішнього генератора і/або їх корекцією,
- автоматично створюють і використовують масив запасу початкових значень основного генератора псевдовипадкових чисел,
- забезпечують період внутрішнього генератора за рахунок значної довжини його операндів,
- кожне з пари початкових значень основного генератора формують внутрішнім генератором незалежно від інших початкових значень.

2. Цифровий пристрій, що реалізує спосіб генерації псевдовипадкових чисел за п. 1, що містить оперативну та постійну пам'ять, блок адресації, блок шифрування та інтерфейс керування пристроєм, який **відрізняється** тим, що додатково містить блок адресації запасу наявних пар початкових значень, блок відстежування залишку корисної довжини періоду, блок внутрішньої генерації цифрових початкових значень з блоком додавання з блоком прокрутки та з блоком виділення і корекції початкових значень, блок основної генерації пар двійкових поточних чисел та кодів перетворення з блоком двійкового додавання з блоком прокрутки адреси та з лічильником прокруток, і блоком виділення кодів перетворення, два блоки перетворення, блок перетворення ідентифікатора абонента, блок відновлення стану і даних, причому вихід блока інтерфейсу керування пристроєм, вихід блока адресації запасу наявних пар початкових значень і лічильник прокруток блока основної генерації з'єднують з входом блока відстежування залишку корисної довжини періоду основної генерації, вихід якого з'єднують з входом блока внутрішньої генерації, вихід якого з'єднують з блоком адресації запасу наявних пар двійкових початкових значень блока основної генерації і їх вільних адрес та з входом блока основної генерації, вихід якого з'єднують з входом блока відстежування залишку корисної довжини періоду основної генерації та з першим блоком перетворення, другий вхід якого з'єднують з входом пристрою та з блоком перетворення ідентифікатора абонента, а вихід з'єднують з входом другого блока перетворення, другий вхід якого з'єднують з блоком основної генерації, вихід другого блока перетворення є виходом пристрою і з'єднаний з входом інтерфейсу керування пристроєм та, відповідно, з постійною пам'яттю пристрою абонента та з блоком запису в облікову систему, також вихід інтерфейсу пристрою з'єднаний з лічильником холостих прокруток блока основної генерації.