

Передача дискретних даних з забезпеченням захисту даних; пристрої для генерації кодів доступу (паролів), записуваних на ідентифіковані пластикові картки (або вмонтовані в них мікросхеми), пристрої для медицини (генератор терапевтичного шуму); індустрія розваг (гральні автомати).

Відомі фізичні пристрої отримання випадкових чисел, побудовані на квантових ефектах. Такі пристрої дають послідовності випадкових чисел, але їх застосування пов'язано з певною небезпекою, що обмежує їх використання спеціальними умовами. Послідовності псевдовипадкових чисел можуть бути отримані за допомогою технічних засобів, що не дозволяють синхронну генерацію парою пристроїв, або комп'ютерних програм, хоча комп'ютер не є компактним приладом з довільними умовами застосування.

Послідовності псевдовипадкових чисел високої якості можуть бути згенеровані за допомогою простого цифрового пристрою, що поєднує безпечність, компактність і якість. Існує багато способів генерації псевдовипадкових чисел. Деякі з цих способів реалізовані як пристрої в галузі захисту інформації. В цій галузі зокрема можуть бути використані пристрої, що використовують просте додавання чисел. Застосування простого додавання чисел робить процес генерації максимально швидким. Прототип способу описаний в «know how» (© В.В. Мясоедов, Абсолютная защита данных. Know how. - Киев. - 2000г. - ПА №3421), де сформульовані головні риси можливого способу захисту даних. Проте у прототипі властивості вихідних послідовностей не вивчені, і їх практична придатність не доведена, не деталізовані також структура пристрою і необхідні обмеження (умови).

Вивчення методу (способу) генерації псевдовипадкових чисел з прототипу свідчить, що цей метод має переваги порівняно з ГОСТ 28147-89 (СРСР) - швидкодія, і з методом Лемера (DES, США), що має певні обмеження на початкові значення генератора, і, крім того, останній не є абсолютно надійним з огляду на методи диференціального криптоаналізу.

З іншого боку, є відомими послідовності Фібоначчі, що взагалі не допускають довільних початкових значень. Це робить неможливим їх практичне застосування при генерації псевдовипадкових чисел - відомі модифікації відповідної схеми генерації не придатні з огляду на їх лінійність та залежність статистичних характеристик результатів від початкових значень і, крім того, не забезпечують надійного шифрування даних, оскільки не визначена межа довжини послідовностей даних, що підлягають шифруванню. Винахід базується на способі генерації псевдовипадкових чисел, що походить від узагальнених послідовностей Фібоначчі. Відомі функціональні аналоги способу генерації, генератори псевдовипадкових чисел типу Фібоначчі із „запізненнями” (дивись, наприклад, патент США №5,850,444) мають тіж недоліки, що й згаданий власний прототип, і, крім того, є ускладненими, а отже не дуже ефективними. Властивості вихідних послідовностей схем генерації у всіх функціональних аналогах авторами не були вивчені теоретично, що не дозволило специфікувати суттєві риси процесу ефективної генерації псевдовипадкових чисел, а саме визначити довжину корисного періоду генератора, використати автоматичну гладку зміну початкових значень генератора за допомогою такого ж генератора з практично нескінченною довжиною періоду, забезпечити абсолютний захист інформації у лініях зв'язку наявністю прихованої частини поточних ключів перетворення даних. Близькі аналоги таких пристроїв не відомі.

Пристрій генерації псевдовипадкових чисел є цифровим пристроєм, що складається з двох триадресних суматорів з циклічною зміною адреси результату, які безпосередньо реалізують принцип генерації псевдовипадкових чисел, оперативної та постійної пам'яті, засобів автоматичного урахування потенціалу початкових значень, а також засобів запуску генератора, вибору параметрів функціонування, засобів функціональної інтеграції в системи обробки і передачі даних. Пристрій реалізується на базі елементів і компонентів цифрової техніки, зокрема з можливим використанням мікропроцесорів.

Відповідно до суттєвих рис методу визначаються і суттєві риси цифрового пристрою генерації псевдовипадкових чисел. В якості компоненти електронної схеми безпосереднього обчислення, такої, як linear feedback shift register (LFSR, дивись, наприклад посилання у патенті США №6,510,228), використовується триадресний (трибуферний, трирегістровий) суматор з блоком циклічної прокрутки адреси (що має бути віднесений до класу МПК H03, отже не заявляється), або звичайна компонента регістрового довгого додавання, що використовує ячейки пам'яті. В якості компоненти електронної схеми безпосереднього перетворення даних (шифрування) можливе застосування потрібних паралельних стеків, що забезпечують паралельне перетворення певної кількості елементів даних (на відміну від перетворення елемент за елементом). Відомостей про аналоги такої компоненти (що має бути віднесена до класу МПК H03, отже не заявляється) стекових машин немає.

У заявці №2003109374 не була наведена риса, що дозволяє уникнути довгої послідовності нульових кодів перетворення даних або нульових початкових значень, яка відрізняється від тривіальності пари початкових значень.

Для ефективного (абсолютного) захисту даних у мережах зв'язку потрібна проста ефективна нелінійна схема (спосіб) генерації псевдовипадкових чисел, що забезпечує ідентичність (синхронність) послідовностей псевдовипадкових чисел або кодів перетворення даних парою екземплярів генератора (при однакових початкових значеннях), реалізованих в залежності від умов використання як програма, або пристрій.

Спосіб оснований на використанні алгоритму Фібоначчі $u_{n+2}=u_{n+1}+u_n$, що в циклі генерує ключі t

$$u_1 = v_1, (\text{mod } d^L), u_2 = v_2, (\text{mod } d^L); t = u_1 + u_2, (\text{mod } d^L), u_1 = u_2, u_2 = t,$$

де v_1, v_2 - довільні нетривіальні початкові значення, d - кількість цифр в відповідних обраних системах зачислення, L - довжина операндів (ключів), з яких утворюються шифруючі слова (коди перетворення)

$$S_n = \frac{x_n \text{ mod } (x_n \cdot 2^{L-L_1})}{2^{L-L_1}},$$

де X_n - поточний ключ t , L_1 - довжина прихованої частини ключів. Винятком з довільності нетривіальних початкових значень є пари чисел, що належать до послідовності Фібоначчі з початковими значеннями $\{1,1\}$.

Потужність способу генерації псевдовипадкових чисел визначена корисною довжиною періоду алгоритму

Фібоначчі, $A_d \cdot d^{L-1}$, де A_d - стала, що залежить від d ($A_d = \frac{3}{2} d$, якщо d - ступінь 2; $A_{10}=60$) і значно збільшується (у

межах конструктивних рішень пристроїв, що реалізують спосіб генерації) за рахунок псевдовипадкової заміни пар початкових значень, які генеруються таким же способом, але мають потрібну довжину прихованої частини ключів, зокрема таку, що забезпечує практично нескінченну потужність способу.

Впорядкована пара початкових значень $\{v_1, v_2\}$ у випадку $v_1=0, v_2=0$ є тривіальною. Тривіальними є також пари початкових значень, в яких обидва числа з пари закінчуються нульовими цифрами, оскільки це впливає на фактичну довжину ключів. Такі пари початкових значень відкидаються за рахунок прокрутки внутрішнього генератора, або коригуються так, щоб останні цифри початкових значень не мали спільного множника, що ділить число цифр d обраної системи зчислення. Виключення довгих послідовностей нульових кодів перетворення даних або нульових початкових значень досягається перестановкою пари початкових значень після перевірки належності правих частин (потрібної довжини) цифрового представлення чисел до послідовності Фібоначчі з початковими значеннями $\{1, 1\}$. Крім того, початкові значення коригуються у випадку, коли виділювана для роботи пара чисел одночасно має послідовність нулів в лівій частині цифрового представлення чисел з довжиною, що на 2, або більше довшини використовуваної частини. Кодування і перетворення інформації при передачі даних з використанням генератора псевдовипадкових чисел дозволяє уникнути використання інформації сторонньою особою. Для забезпечення незалежності споживачів від виробника передбачена процедура ручного ініціювання генератора за рахунок невизначеності точного часу роботи генератора до моменту фіксації початкових значень. Для зберігання і розподілу початкових значень процедура ініціювання завершується копіюванням початкових даних на зовнішній носій інформації або в аналогічний пристрій абонента (процесу). Повторне ініціювання приведе до нових початкових значень. Для передачі великої кількості даних при перевищенні певної довжини передбачена автоматична гладка зміна початкових значень, які отримуються з допомогою внутрішнього генератора, що має великий (практично нескінченний) період. Ініційований внутрішній генератор формує пару незалежних початкових значень робочого генератора, або масив таких пар. Випадкові числа, що залежать від початкових значень, дозволяють перетворити інформацію унікальним чином, так що вона може бути правильно сприйнята тільки тими, хто має відповідні початкові значення на момент початку передачі даних. Передбачена холоста прокрутка основного (робочого) генератора псевдовипадкових чисел перед перетворенням кожного наступного повідомлення (нової порції даних), що додатково гарантує захист даних незалежно від можливих обставин. Всі початкові значення не можуть бути прочитані персоналом без спеціальних засобів (не є відомими користувачам). Передбачений режим подвійного захисту інформації, що робить розкриття її змісту у лініях зв'язку неможливим ні теоретично, ні практично. Цей результат досягається за рахунок використання лише незначної (і саме незначної) кількості бітів операндів в алгоритмі генератора Фібоначчі, що полягає в простому послідовному додаванні чисел в обмеженій цифровій сітці. Це реалізується за допомогою прокрутки адрес регістрів, які містять три послідовних згенерованих операндів (чисел), старші частини кожного з яких по одному по черзі використовується за призначенням. Використання способу генерації узагальнених послідовностей Фібоначчі вперше дає можливість створити пристрій, що без втручання персоналу гарантує абсолютну стійкість захисту інформації у лініях зв'язку за рахунок автоматичного врахування потенціалу початкових значень, який відновлюється після шифрування послідовності даних точно визначеної (з урахуванням холостих прокруток) довжини. При застосуванні способу для генерації паролів у системах масового обслуговування, наприклад у банківських системах, передбачається ефективна затримка відповіді після перевірки паролю, що дозволяє уникнути машинних засобів зламу паролів і не дуже впливає на час очікування відповіді легальних користувачів таких систем.

На підставі особливостей способу генерації псевдовипадкових чисел, викладених вище, визначено принцип і основні блоки пристрою генерації псевдовипадкових чисел.

Головний зміст генерації псевдовипадкових чисел, а саме принцип засобу генерації, проілюстрований на кресленні Фіг. 1, аркуш К1, блок-схемою, що відтворює відповідний циклічний дискретний процес (опосередкований певною апаратною затримкою, реалізованою лінією затримки, або тактовими імпульсами синхронізації цифрового пристрою): на початку генерації початкові значення і початковий напрям (адреси операндів та результату) додавання зчитуються з постійної пам'яті блоком зчитування за значенням змінної (сигналу) „перший цикл”, значення якої аналізується блоком вибору. Якщо перший цикл вже закінчено, блок вибору замість прочитаних даних подає на вхід трирегістрової схеми (довгого) додавання трійки чисел (поточні значення операндів і - необов'язково - результат), отримані у попередніх циклах, і поточний напрям додавання (адреси операндів та результату, які змінюються блоком прокрутки адреси -дивись Фіг. 2). Поточні (та кінцеві, що за сигналом „останній цикл” коригуються, Фіг. 2, або перетворюються блоком перетворення; Фіг. 3) записуються у постійну пам'ять. Значення і адреси результатів додавання використовуються у пристрої згідно з описом роботи пристрою, наведеним нижче. Принцип генерації реалізований блоками цифрової та двоїчної генерації - у кожному блоці відповідним до параметрів пристрою числом разів.

Типовий блок генерації, Фіг. 2, аркуш К1, складається з триадресного суматора 1, який використовує постійну 2 або оперативну 3 пам'ять (блоки вибору Фіг. 1 включено до суматора), поточні адреси додавання однієї або двох схем довгого додавання Фіг. 1 визначаються блоком (мікропрограмою) 4 прокрутки адреси, кінцеві значення доданків та суми після корекції тривіальності та запобігання появи довгої послідовності нулів блоком корекції 5 записуються у постійну пам'ять блоком запису 6. Робота блоку генерації визначається сигналами запуску («перший цикл») та зупинки («останній цикл»), а також засобами дискретизації процесу генерації Фіг. 1. На кресленні не відображені лінії, що відповідали б адресам та числам другого екземпляра схеми додавання. Дві схеми довгого додавання використовуються для d -їчної генерації пар початкових значень.

У склад пристрою входить також блок перетворення, Фіг. 3, аркуш К2, що складається з блоку 7 перетворення формату двох послідовностей вічних цифр, що надходять з блоку цифрової генерації у дві послідовності бітів (початкових значень основного генератора; зайві молодші біти відкидаються), які після виділення пари молодших

бітів схемою 8 перевіряються на одночасну парність схемою перевірки парності 9, і автоматично коригуються схемою корекції 10 одного з молодших бітів результатом перевірки і разом з їх максимальним потенціалом поступають у блок б запису в постійну пам'ять.

Спілкування абонентів, визначення постійних режимів роботи та інтеграція в системи обробки даних здійснюється блоком інтерфейсу пристрою генерації, що містить джерела сигналів (кнопки і тумблери), засоби індикації і, схему передачі або прийому запасу початкових значень разом із початковими значеннями блоку цифрової генерації, на яких базується запас, з постійної пам'яті пристрою в постійну пам'ять аналогічного пристрою засоба комунікації абонента або процесу (заповненням буферу передачі або зчитуванням з буферу прийому; необхідним додатковим реквізитом є власний, відповідно, отримуваний ідентифікатор (номер телефону) абонента або процесу).

Придатність збережених двоїчних пар початкових значень визначається блоком відстежування, Фіг. 4, аркуш К2, їх потенціалу, що зменшується при використанні. Блок відстежування потенціалу складається з схеми обчислення різниці між прочитаним з постійної пам'яті 2 значенням потенціалу і поточними розмірами даних в оновлюваному буфері шифрування, що одночасно ініціює звертання до блоку цифрової генерації, схеми комутації адреси зберігання початкових значень на момент початку шифрування поточного і попереднього буферу шифрування (забезпечує можливість відновлення початкових двоїчних значень для шифрування без втрат цілого поточного буферу - без поточного відліку циклів генерації), схемою комутації блоку двоїчної генерації на запасні початкові значення.

Основну роботу пристрою за сигналами блоку відстежування потенціалу виконує блок двоїчної генерації, Фіг. 5, аркуш К3, який містить блок генерації, Фіг. 2 (без блоку корекції та з однією схемою довгого (двоїчного) додавання), схему 11 виділення коду перетворення з поточного результату, схему комутації 12 на мікробуфер циклу шифрування; а також лічильник 13 холостих циклів генерації між повідомленнями (які зменшують корисну довжину періоду). Кінцеві дані генерації (трійка операнди-результат і адреси напрямку додавання для блоку прокрутки) згідно з Фіг. 2 надходять в блок б запису в постійну пам'ять - як оновлені початкові значення блоку двоїчної генерації.

Функціональне призначення пристрою забезпечується блоком шифрування, Фіг. 6, аркуш К3, що складається зі схеми 14 комутації буферів оперативної пам'яті 3, які по черзі доступні засобам прийому 15 та передачі 16 даних пристрою комунікації в лінії зв'язку і логічної схеми побітного додавання по модулю два вхідного і згенерованого двоїчних слів (операція «виключне АБО»), включеної до циклу шифрування 17 „елемент за елементом” оновлюваного буферу, або розмноженої в потрібному стеку (два входи і один вихід) для паралельного виконання (стек не показаний).

Для зручності сприйняття креслень Фіг. 2 ÷ Фіг. 6 деякі блоки, наприклад, оперативна пам'ять, можуть бути відображені на одній фігурі двічі. Блок адресації постійної та оперативної пам'яті на кресленнях не відтворений.

Функціонування пристрою полягає в тому, що блок цифрової генерації в процесі довільної ініціалізації пристрою користувачем створює дві пари незалежних d-ічних початкових значень для подальшого оновлення в процесі цифрової генерації, коригує кожну пару d-ічних початкових значень у випадку її тривіальності і записує її в постійну пам'ять, при кожному звертанні ініціалізований блок цифрової генерації використовує дві поточні пари d-ічних чисел для отримання на виході пари незалежних d-ічних чисел, яка блоком перетворення формату перетворюється у пару двоїчних чисел (скориговану у випадку їх одночасної парності), що використовується блоком двоїчної генерації як початкові значення після запису в постійну пам'ять разом з їх початковою корисною довжиною періоду; блок інтерфейсу пристрою для ініціалізації кожного нового абонента або процесу звертанням до блоків цифрової генерації-перетворення створює запас пар двоїчних початкових значень блоку двоїчної генерації, забезпечує заповнення/зчитування та під'єднання буферів до засобів передачі/прийому пристрою комунікації для встановлення відповідності („синхронізації”) початкових значень генераторів при безпосередньому з'єднанні пристрою до джерела або тимчасового носія початкових значень та ідентифікатора, а також блокує повторне їх зчитування назовні без видалення абонента або процесу з пам'яті засобу комунікації, супроводжуваного видаленням відповідних початкових значень з пам'яті пристрою генерації, залишок корисної довжини періоду для пар двоїчних початкових значень відстежується блоком відстежування залишку у межах визначених наявністю та розміром даних для шифрування (або розміром буферу шифрування), числом холостих циклів генерації (прокруток) після закінчення шифрування повідомлення (комунікації), відстежує прочитаний з постійної пам'яті потенціал (залишок корисної довжини періоду) пар двоїчних початкових значень, визначених за ідентифікатором абонента або процесу, якщо потенціал недостатній звертається до запасної пари двоїчних початкових значень і до блоків цифрової генерації-перетворення для поповнення запасу, оновлює значення потенціалу в постійній пам'яті при оновленні початкових значень, а також при переході до наступного буферу шифрування або при завершенні шифрування даних, блок двоїчної генерації використовує пари двоїчних початкових значень, що мають достатній потенціал, для генерації псевдовипадкових чисел, виділяє старші біти поточного результату генерації для використання в блоці шифрування, оновлює використану пару початкових двоїчних значень парою кінцевих - з урахуванням холостої прокрутки -результатів генерації записом в постійну пам'ять, блок шифрування відстежує наявність і розміри даних, стан процесу шифрування, комує вхідний, оновлювані і вихідні буфери, здійснює операцію шифрування кожного елемента даних псевдо випадковими числами, що надходять з блоку двоїчної генерації, в залежності від режиму подвійного шифрування використовує паралельний блок двоїчної генерації з запасом початкових двоїчних значень, отриманих в незалежному процесі ініціювання абонента (або процесу комунікації), додатковий оновлюваний буфер і додаткову операцію шифрування, блок живлення містить підзаряджуваний або резервний акумулятор, який забезпечує процес термінового зберігання стану і всіх даних пристрою блоком аварійного завершення комунікації для можливості відновлення процесу комунікації без втрати даних абонентом або процесом і без повторного контакту з абонентом або процесом для встановлення відповідності початкових значень генераторів.

Абсолютна стійкість шифрування в межах потенціалу початкових значень доводиться можливістю зміни

прихованої лівої (старшої) частини поточного ключа (крім першого розряду). Це змінює вихідну послідовність псевдовипадкових чисел непомітно для того, хто пробує розшифрувати дані (дивись статтю: В.В. Мясоєдов, Золотое сечение в шифровании данных. В зб.: Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.-Науково-технічний збірник.-Випуск 4.-К.:НДЦ „Тезіс” НТУУ „КПІ”. - 2002. - 214с. - С.105). Додатково може бути забезпечена перевірка цілісності даних.

Коди перетворення інформації (псевдовипадкові числа) застосовують за допомогою елементарної операції, що дозволяє однозначне звернене перетворення, наприклад, побітової операції „виключне „АБО” при перетворенні кожного елементу даних або послідовності таких кодів кодами перетворення, чи операції додавання коду перетворення до коду перетворюваного символу по модулю довжини текстового алфавіту. Використання псевдовипадкових чисел в генераторах терапевтичного шуму забезпечують цифро-аналоговими перетворювачами. Використання пристрою у гральних автоматах забезпечує імітацію реакції на натискання певних кнопок, індикацію псевдовипадкових чисел, визначення псевдовипадкового моменту і розміру виграшу з урахуванням показань касового лічильника монет. При застосуванні пристрою для генерації паролів у системах масового обслуговування, наприклад у банківських системах, передбачається ефективна затримка відповіді після перевірки паролю, що дозволяє уникнути машинних засобів зламу паролів і не дуже впливає на час очікування відповіді легальних користувачів таких систем.

Для кращого розуміння винаходу нижче наводиться опис однієї з можливих технологічних концепцій пристрою.

Після вмикання струму з блоку постійної пам'яті зчитуються постійні режими роботи генератора: генерація/шифрування, подвійне шифрування, тип взаємодії внутрішнього і основного генераторів (за викликом, чи по вичерпанню запасу початкових значень основного генератора), а також, можливо, додаткові режими в залежності від призначення пристрою. Ці режими представлені сигналами і можуть бути змінені в процесі експлуатації. Оперативні режими роботи мінімальні: основна робота, ініціювання (для початку незалежної від виробника експлуатації), відновлення (наприклад, внаслідок тестування, або зміни власника). Оперативні режими взаємно виключають один одного, що забезпечується відповідним блокуванням дії кнопок (зміною відповідних сигналів) і зберіганням/оновленням опису стану пристрою в блоці постійної пам'яті. Після вимикання струму (нормального, або аварійного) здійснюється запис поточних початкових значень і повного стану пристрою в блок постійної пам'яті в спеціальну область разом з признаком термінового завершення роботи (за винятком стану очікування в оперативному режимі основної роботи). Ці дані забезпечують автоматичний віртуальний режим повторного запуску пристрою. Їх запис забезпечується підзаряджуваним акумулятором. Дублювання і живлення блоків пристрою мінімізуються за допомогою комутаторів сигналів з урахуванням потрібної швидкодії і зв'язності пристрою. Режими визначають незалежні по живленню компоненти пристрою в лінійній послідовності функціонування пристрою. Тому комутатор живлення містить лише перемикач перевірки признаку термінового завершення роботи, що вмикає певний режим роботи, визначений з опису стану пристрою, і додатковий елемент вимикання/вмикання основного режиму роботи при занадто довгому очікуванні зовнішніх даних (сигналів). Залежність функціонування компонент визначається даними стану пристрою і, з другого боку, спільними блоками забезпечення функціонування. Підзаряджуваний акумулятор вмикається останнім, а вмикається першим.

Режим відновлення здійснюється блоком відновлення і встановлюється кнопкою „Відновлення” на закритій панелі управління, захищеною задвижкою. Сигнал відновлення викликає подвійний перезапис початкових значень внутрішнього генератора блоком перезапису з блоку постійної пам'яті в фіксовані адреси цього ж блоку і фіксується в описі оперативного стану пристрою (блок постійної пам'яті; біт відновлення: '1'). Цей перезапис заблокований за початковим оперативним станом (біт відновлення: '0'). Після відновлення згашений сигнал відновлення записується в опис оперативного стану пристрою (біт першого вмикання: '0'), який вмикає блок (і панель) ініціювання.

Режим ініціювання здійснюється блоком ініціювання і встановлюється при першому вмиканні пристрою (опис оперативного стану в блоці постійної пам'яті; біт першого вмикання: '0'), або після виконання режиму відновлення (той же біт). При цьому вмикається блок відновлення (запис біту відновлення: '0' в опис стану), незалежно від того, чи був блок відновлення ввімкнений, чи ні. На панелі ініціювання починає блимати одна з двох лампочок ініціювання, що починає рівно світити після натискання кнопки „Старт” і згасає після натискання кнопки „Стоп”; після цього процедура повторюється, з відповідною індикацією другою лампочкою. Час між натисканнями кнопок „Старт”/„Стоп” цілком визначається споживачем і не повинен бути коротким (від кількох хвилин в залежності від швидкодії). В результаті послідовного натискання кнопок в постійну пам'ять будуть записані два незалежних початкових значення внутрішнього генератора. Це забезпечується функціонуванням пристрою в режимі ініціювання, а саме: безпосередньо після вмикання компоненти ініціювання (біт першого вмикання і біт кнопки „Старт”) використовуються початкові значення і їх адреси з постійної пам'яті, що розміщуються в оперативній пам'яті. Трибуферний цифровий суматор разом з комутатором буферів оновлює оперативну пам'ять, доти, поки не буде натиснута кнопка „Стоп”, що викликає запис одного з початкових значень в постійну пам'ять і вимикання компоненти ініціювання, причому після згасання другої лампочки панель ініціювання готова до вимикання і буде вимкнута в основному режимі роботи. Записані початкові значення внутрішнього генератора використовуються для визначення початкових значень основного генератора і запису їх потенціалів у відповідності з фіксованими постійними режимами взаємодії внутрішнього генератора з основним генератором. Після ініціювання в опис оперативного стану в блоці постійної пам'яті записуються біт вмикання основного режиму ('1'), який вмикає блок основного режиму роботи та біти стану основного режиму роботи (біт продовження: '0'; біт очікування: '0'; а також біти постійних режимів, що залежать від тумблерів на закритій панелі управління, а саме - біт типу взаємодії: '0'- „за викликом”; біт подвійного шифрування: '0' - „звичайне”; біт застосування: '0' - шифрування).

Режим основної роботи визначається фіксованими режимами експлуатації. Зміна постійних режимів здійснюється тумблерами, або перемичками. Вплив такої зміни на функціональну придатність пристрою дуже

великий і враховується за схемою реакції на термінове вимикання живлення. При подвійному шифруванні режим ініціювання виконується двічі, а при простій генерації чисел без шифрування ініціювання проводиться за бажанням споживача. Додатковим засобом забезпечення зміни режимів шифрування, що враховує також комутацію абонентів, є запис на зовнішній технічний носій даних і в постійну пам'ять початкових значень генераторів для кожного фіксованого ідентифікованого абонента.

Побудова пристрою генерації визначається в залежності від параметрів вхідних і вихідних даних за схемою сервер-тема-інтерфейс-зв'язок. Детальний опис сигналів і даних міститься у викладі автоматичного віртуального режиму „термінового збереження”/”повторного запуску” пристрою. Вхідними даними пристрою є слова довжиною $L_{in}(=8)$ бітів. Вихідними даними є зашифровані вхідні слова довжиною $L_{out}(=8)$ бітів, або числа такої ж довжини. Режим подвійного шифрування забезпечується дублікатом серверу генерації для забезпечення потрібної швидкодії, або відповідною темою цього серверу. В режимі генерації псевдовипадкові числа просто експортуються з пристрою з урахуванням потрібного інтервалу їх величини. В режимі шифрування вхідний буфер змінюється після кожної операції, виконаної над усіма вхідними словами в буфері. При шифруванні вхідні слова сполучаються за логічною операцією „виключне «АБО»» (чи за додаванням по модулю довжини вихідного алфавіту) з псевдовипадковими словами (числами), що поставляються сервером генерації, і розміщуються у вихідному буфері експорту з пристрою.

Вихідні числа для деяких спеціалізованих застосувань пристрою, наприклад, у гральних автоматах, можуть бути представлені (і вираховані) у десятичній системі зчислення. Іншим спеціалізованим застосуванням цифрового пристрою генерації псевдовипадкових чисел є випадкова перестановка (комутація) бітів вхідного слова, що реалізується як матричне перетворення цього слова при рекурсивному використанні сервера генерації.

Сервер основної генерації починає роботу після перевірки потенціалу початкових значень, що співставляється з довжиною текста для шифрування або з довжиною заповненої частини буферу. При безбуферному шифруванні ця перевірка здійснюється для кожного слова з вхідного потоку. Якщо потенціал початкових значень недостатній, то його відновлення здійснюється (за лічильником залишку) після використання наявного потенціалу звертанням до внутрішнього генератора за новими початковими значеннями, або до резервних початкових значень з запасу, що асинхронно поповнюється сервером внутрішньої генерації. Вихідне слово серверу основної генерації є словом довжиною з L_{out} випадкових двоїчних (або десятичних в залежності від призначення пристрою) цифр. Це слово формується на інтерфейсі серверу однаковими допоміжними серверами генерації - по одному на кожну групу з $S(=1)$ цифр. Операнди допоміжних серверів генерації це двоїчні числа довжиною L ($=64$ або $=128$, залежно від типорозміру, що визначає частоту звертання до серверу внутрішньої генерації). При десятичній генерації у спеціалізованих версіях пристрою виходи допоміжних серверів формуються за модулем 10 з перших чотирьох бітів результату операції додавання (біт переповнення ігнорується) або просто певною кількістю цифр десятичного додавання. При двоїчній генерації в описуваному пристрої використовуються біти переповнення „довгої” операції додавання, крім останнього біту. Відповідно до кількості L_{out}/S допоміжних серверів визначена кількість незалежних пар початкових значень для кожного з них, їх адреси у постійній і регістровій пам'яті, а також кількість трійок регістрів. Ці адреси і початкові значення змінюються одночасно для всіх допоміжних серверів і зчитуються сервером основної генерації з постійної пам'яті разом з потенціалом початкових значень на початку кожної порції потоку перетворюваних даних. За сигналом від лічильника залишку довжини текста, залишку заповненої довжини буфера, або врешті решт від прямого сигналу кінця вхідного потоку сервер основної генерації відновлює готовність до шифрування нової порції даних:

зменшує поточний потенціал на величину $W(=6)$; якщо залишок недодатний, то відновлює у постійній пам'яті потенціал, адресу результату і початкові значення для допоміжних серверів (запасними, чи після звертання до внутрішнього генератора) і переходить в стан очікування; інакше блокує експорт з пристрою, викликає допоміжні сервери W разів, після чого записує у постійну пам'ять потенціал, початкові значення і початкову адресу результату допоміжних серверів генерації, розблоковує експорт з пристрою, і переходить в стан очікування. Так само відновлюється готовність у пристрої генерації відповідного абонента. Допоміжний сервер генерації є трирегістровим суматором, в якому поточний регістр результату операції додавання, отже і регістри операндів додавання, циклічно змінюються після кожного звертання до цього серверу (однаково по всіх допоміжних серверах генерації). Початкове визначення адреси регістра результату зберігається у постійній пам'яті разом з початковими значеннями допоміжної генерації і поставляється основним сервером.

В разі потреби збереження ідентифікованих порцій шифрованої інформації сервер основної генерації може передавати початкові значення для відповідної розшифровки через інтерфейс з інтегрованою системою обробки даних. Цей інтерфейс може бути поширений до управління постійними режимами експлуатації пристрою, або бути заблокованим за умовами комплектації. Сервер інтерфейсу шифрування забезпечує паралельне (без перезапису) використання трьох буферів: один заповнюється, в другому йде шифрування, з третього дані експортуються. Мінімальною функцією серверу інтерфейсу є сигналізація про зайнятість пристрою (або про стан очікування). При зміні постійних режимів експлуатації в поширеному інтерфейсі сигналізується зайнятість пристрою, вмикається віртуальний автоматичний режим запису, активація початкових значень відповідного абонента або ініціалізація пристрою для нового абонента, і нарешті сигналізується готовність пристрою прийняти дані для шифрування в підготовлений буфер (стан очікування).

Сервер внутрішньої генерації при звертанні з серверу основної роботи постачає в цей сервер (або в постійну пам'ять при поповненні запасу початкових значень) L_{out}/S пар початкових значень для допоміжних серверів генерації у вигляді пар двоїчних чисел при умові, що хоча б одне з чисел у кожній парі було непарним. Кількість серверів перетворення може бути збільшена до кількості допоміжних серверів генерації L_{out}/S , в іншому разі цей сервер працює в циклі потрібне число разів. (Аналогічно може бути зменшеним число допоміжних серверів генерації). Сервер перетворення отримує з інтерфейсу з трибуферними цифровими суматорами дві послідовності d -ічних цифр (чисел) достатньої довжини M ($d^M > 2^L$), перетворює їх у пару двоїчних чисел довжиною L бітів, перевіряє одночасну парність двоїчних чисел (у випадку одночасної парності ще раз звертається до

трибуферного цифрового суматора або коригує обидва числа додаванням одиниці) і виставляє одержану пару початкових значень в інтерфейс серверу основної роботи. Кожна з двох послідовностей d-ічних цифр поставляється в інтерфейс одним з двох трибуферних цифрових суматорів. (Кількість трибуферних цифрових суматорів може бути зменшена до одного в залежності від реалізації пристрою. В цьому разі інтерфейс з сервером перетворення заповнюється послідовно - два рази на кожне звертання до суматора). Трибуферний цифровий суматор за сигналом від серверу основної роботи (і/або від серверу перетворення залежно від реалізації пристрою) звертається до двох пар початкових значень внутрішньої генерації довжиною $L_{BIG}(=4000)$ і адреси результату додавання для відповідного абонента, зчитує ці значення порціями в два буфера, виконує додавання d-ічних чисел в третій буфер, зберігає біт переносу в старший розряд для врахування на наступному кроці (початкове значення біту - '0'; значення біту після останнього кроку ігнорується і встановлюється в '0'), записує отриману порцію суми в постійну пам'ять у відповідності з адресою результату додавання. По закінченню додавання перші M d-ічних цифр суми виставляються на інтерфейс сервера перетворення через буфер зчитування з постійної пам'яті. Оновлена адреса результату додавання записується в постійну пам'ять для використання при подальшому звертанні до суматора (цей запис може здійснюватись тільки один раз для фіксованої кількості L_{out}/S потрібних пар початкових значень; в залежності від рішень щодо дублювання серверів зчитування/запис адреси результату може бути визначеним як в сервері перетворення, так і в сервері внутрішньої генерації).

Початкові значення, що постачаються в допоміжні сервери генерації є незалежними як в парі, так і по всіх парах і по всіх абонентах, за рахунок використання двох незалежних пар початкових значень трибуферного цифрового суматора, утворених внаслідок подвійного незалежного ініціювання пристрою для кожного абонента і режиму подвійного шифрування.

Режим автоматичного віртуального „термінового збереження”/„повторного запуску” пристрою є необхідним процесом збереження/відновлення функціонування пристрою у довільний момент припинення/вмикання живлення, незалежний від стану переробки даних, оскільки вимагається можливість розшифровки переданих даних тотожним пристроєм абонента. Цей режим необхідний і при прийомі даних після відновлення комунікації, канал якої зберігає кількість переданих/прийнятих одиниць інформації. Реалізація цього режиму базується на детальному дослідженні зв'язності пристрою і зв'язності його функціонування для визначення переліку сигналів і даних, необхідних для повторного запуску. Зв'язність пристрою є прагматичною характеристикою, що визначає певні рішення про функції і конструкцію пристрою. Зокрема це стосується до дублювання серверів для паралельного виконання подібних (однакових) тем, обмеженого використанням спільних блоків, а також до синхронного, або асинхронного (за наявності даних) функціонування. Ці рішення є обмеженнями реалізації. Зв'язність пристрою у часі забезпечується постійною пам'яттю. Зв'язність пристрою у „внутрішньому” просторі забезпечується оперативною (буферною) пам'яттю. Операційна зв'язність пристрою вимагає поєднання в одному блоці всього необхідного для виконання закінченого операційного циклу, включаючи регістру (власну буферну) пам'ять. Кожний операційний блок входить в певний сервер і не залежить від визначеної сервером теми (здатен опрацьовувати будь-яку з визначених тем). Кількість і склад операційних блоків у сервері залежить від рішень про дублювання/циклічність (паралельність/послідовність) виконання операцій. Взагалі засобами запам'ятовування є також черги (буфери) та стеки. Подальший виклад стосується можливостей конструювання пристрою і ґрунтується на концепції, викладеній вище.

Можливість здійснення винаходу:

Обмеження реалізації (цифровий пристрій шифрування у засобах комунікації):

Інтегровність у засоби цифрового зв'язку (телефон, модем, факс-модем, телебачення; для останнього - періодичне ініціювання генераторів розшифровки позавізуальною компонентою сигналів телепередачі) безвідносно до інтегрованих систем обробки даних: до 10-ти абонентів з ініціалізацією генератора співрозмовника безпосередньо при зустрічі сполученням пристроїв або за допомогою технічного носія початкових значень, наприклад, візитної картки з вмонтованою мікросхемою.

Акцент на використанні дублювання блоків для забезпечення потрібної швидкодії за рахунок паралельного виконання однакових операцій.

Специфічні особливості згаданих засобів комунікації визначають типорозміри пристрою по певних параметрах, зокрема довжиною регістрів трирегістрових схем додавання, яка впливає на вибір систем зчислення.

Певність конструктивних рішень:

1) Сервер внутрішньої генерації, використовує два паралельних блока цифрової генерації. Прокрутка адрес результату додавання здійснюється однаковими блоками. У темі основної роботи кількість прокруток стала і визначена кількістю $L_{out}/S(=8)$ потрібних пар початкових значень. Для першої пари сервер під'єднує схеми (d-ічного) довгого додавання за допомогою блоків вибору до блоку зчитування поточних початкових значень внутрішнього генератора з постійної пам'яті, подальші прокрутки здійснюються в оперативній пам'яті, після останньої прокрутки поточні початкові значення внутрішнього генератора записуються в постійну пам'ять блоком запису в постійну пам'ять за адресами, що формуються блоком адресації. Після кожної прокрутки і додавання чисел блок внутрішньої генерації передає в два буфера сервера перетворення M перших d-ічних цифр кожної з пари сум і без паузи починає наступну прокрутку. Тривіальні пари початкових значень не відкидаються, а коригуються у сервері перетворення. Додавання здійснюється за схемою довгого додавання в циклі „заповнення вхідного буфера - додавання із збереженням біту переповнення - заповнення вихідного буфера” з відповідною установкою біту переповнення перед і після операції довгого додавання ('0'). Значення лічильника пар після підготовки потрібної кількості пар максимальне (воно встановлюється в нуль сервером основної генерації при звертанні, або на початку циклу поповнення запасу початкових значень). Тема основної роботи серверу внутрішньої генерації завершується блоками серверу перетворення через оперативну пам'ять перед процесом запису кожного з початкових значень основного генератора у постійну пам'ять. У темі ініціювання (дивись Режим ініціювання) для кожного абонента визначений потрібний запас початкових значень основного генератора

$P \cdot L_{out}/S$. Блоки внутрішньої цифрової генерації створюють цей запас послідовно порціями по L_{out}/S пар після невизначеної наперед кількості $P(t_1)$, $P(t_2)$ незалежних прокруток кожного з двох паралельних трибуферних цифрових суматорів. Ці прокрутки починаються одночасно при натисканні кнопки „старт”, а закінчуються після натискання по одній кнопці „стоп” (одночасне натискання обох кнопок заблоковано механічним способом). Перед першою прокрутою сервер внутрішньої генерації під'єднує блоки двох паралельних трибуферних цифрових суматорів до буферу зчитування початкових значень внутрішнього генератора, підготовлених виробником пристрою, за сталими адресами, що надходять у блок адресації. Після останньої прокрутки ці значення оновлюються (=встановлюються споживачем кнопками „стоп”) через буфер запису у постійну пам'ять (а саме - закінчується поточна прокрутка, і починається фінальна, супроводжувана записом). Після цього за лічильником запасу початкових значень основного генератора виконується тема основної роботи, що кожного разу завершується записом початкових значень основного генератора, у постійну пам'ять за сталими адресами, що відстежуються блоком адресації.

Тема ініціювання встановлюється для першого вживання пристрою, після виконання відновлення, після запису у постійну пам'ять ідентифікатора (номеру телефону, тощо) нового абонента (останнє - за бажанням при натисканні кнопки „старт”), закінчується при вимиканні пристрою і продовжується при наступному вмиканні (альтернативою є використання кнопок „стоп”, або тільки другої з них) з індикацією процесу ініціювання. Для зручності споживача тема ініціювання може виконуватись додатковим блоком внутрішньої генерації (приклад ситуації: запущений режим ініціювання і лунає вхідний дзвінок по телефону від захищеного пристроєм абонента). Для дорогих версій пристрою ініціювання може здійснюватись за допомогою додаткових блоків запису/зчитування (адресація постійної пам'яті, таким чином, має щонайменше три рівня: абонент-запас-одна пара початкових значень). Споживач за бажанням може зупинити захист комунікації (такий сигнал „відкритості тексту” проходить від пристрою до пристрою безпосередньо при з'єднанні). Для можливості розшифровки споживач і абонент користуються зовнішнім технічним носієм початкових значень (і ідентифікаторів кореспондентів), який може бути вставлений у засіб зв'язку для запису/зчитування аналогічними до роботи з постійною пам'яттю за вільними адресами, визначеними блоком адресації, і приведеним в дію натисканням кнопки „встановлення контакту”. Відновлення довіри до конфіденційності зв'язку відбувається при повторній зустрічі кореспондентів при видаленні і записі ідентифікаторів і відповідного ініціювання в контексті відображення ідентифікаторів абонента в пам'яті пристрою комунікації.

Реєстр інформації серверу внутрішньої генерації (параметри, сигнали, дані, адреси):

Тема основної роботи - ідентифікатор абонента, співвідношення довжини d-ічних чисел з довжиною буфера зчитування/запису ($=125$), кількість прокруток на одне звертання ($=8$), довжина буфера з сервером перетворення ($=20$); сигнал основної роботи, сигнал звертання, сигнал оновлення буфера з сервером перетворення; лічильник запасу (прокруток на одне звертання), дві послідовності d-ічних чисел у буфері з сервером перетворення, лічильник циклу довгого додавання, вхідний буфер суматора, оперативна пам'ять суматора, адреса результату в оперативній пам'яті, біт переповнення; адреси в постійній пам'яті, що можуть бути встановлені (співставлені з) лічильниками. Мінімально достатньою інформацією є сигнали і значення лічильників, а також ідентифікатор абонента.

Тема ініціювання - ідентифікатор абонента, співвідношення довжини d-ічних чисел з довжиною буфера зчитування/запису ($=125$), кількість прокруток на одне звертання ($=8$), кількість запасних наборів початкових значень ($=$ від типорозміру, $=2$); сигнал введення ідентифікатора абонента, сигнал відновлення (по абоненту, по всіх абонентах), сигнал першого вмикання, сигнал „стоп1”, сигнал «стоп2», сигнал закінчення відновлення, сигнал основної роботи; лічильник запасних пар початкових значень, лічильник прокруток на одне звертання, -, -, -, -, -; адреси в постійній пам'яті, що можуть бути встановлені (співставлені з) лічильником прокруток. Мінімально достатньою інформацією є сигнали, за якими може бути повторно ввімкнена панель ініціювання (бо параметри визначені і сталі, а точне відтворення поточних початкових значень внутрішнього генератора не має сенсу при ініціюванні).

2) Сервер перетворення практично зводиться до блоку з двох однакових перетворювачів послідовностей d-ічних цифр з вхідних буферів у двоїчні числа. Сервер починає роботу після кожного оновлення вхідних буферів, виставляє сигнал зайнятості буферів, перетворює числа в оперативній пам'яті, перевіряє пару отриманих чисел результату на тривіальність. (Якщо пара тривіальна, то числа пари коригуються у непарні додаванням одиниць блоком перевірки і корекції.), записує одержану пару в постійну пам'ять разом з потенціалом спільним для всіх пар, гасить сигнал зайнятості вхідних буферів після перевірки лічильника пар. Врешті решт, цей сервер можна вважати блоком в сервері внутрішньої генерації.

Реєстр інформації серверу перетворення (параметри, сигнали, дані, адреси):

Тема перетворення - довжина послідовностей d-ічних цифр, довжина початкових значень основного генератора; сигнал оновлення вхідних буферів, сигнал зайнятості вхідних буферів; вміст вхідних і вихідних буферів; -. Мінімально необхідною інформацією є сигнали (оскільки вхідні дані можуть бути прочитані з постійної пам'яті за збереженими даними сервера внутрішньої генерації). Сигнал звільнення буферів при добре підібраній швидкодії блоків не має іншого значення, крім фіксації стану пристрою для можливого термінового завершення або повторного запуску (рестарту). Такий же сигнал для вихідних буферів, що встановлюється сервером основної генерації, дозволяє вирішити проблему відновлення вихідних даних: якщо вихідні буфери вільні, то відновлення непотрібне. Взагалі, такі сигнали визначають асинхронний засіб функціонування пристрою за оновленням і звільненням буферів. Стан очікування джерела даних має бути виключеним при вдалому виборі швидкодії блоків.

3) Сервер основної генерації координує асинхронну роботу блоків пристрою, містить блок основної генерації, і починає свою роботу з підготовленими парами початкових значень за сигналом готовності для шифрування даних з вхідного буферу, що виставляється сервером інтерфейсу пристрою. (До певної міри весь пристрій можна вважати сервером шифрування у визначеному засобі зв'язку), а також відстежує інтервал між порціями даних: коли цей інтервал перевищує заданий час очікування припиняється живлення блоків без вимикання самого блоку

живлення. Початок і закінчення порції інформації для шифрування визначаються сигналами безпосередньо при з'єднанні/роз'єднанні зв'язку або після натискання кнопки конфіденційності („відкритості тексту”) розмови (телефон). За сигналом початку сервер основної генерації зчитує з постійної пам'яті залишковий потенціал, під'єднує весь потрібний набір пар початкових значень з постійної пам'яті блоком вибору разом з початковою адресою результату додавання до блоку основної генерації і за визначеною довжиною буфера відстежує перехід до шифрування наступного буфера. Затримка комунікації на заповнення і шифрування буфера не повинна перевищувати 0,4 секунди (краще - 0,1 секунди). За сигналом закінчення (і при переході до наступного вхідного буфера - це може бути виключено за типорозміром основної генерації) сервер основної генерації перевіряє поточний потенціал початкових значень. (Якщо потенціал недостатній для шифрування наступного буфера, то здійснюється під'єднання запасних початкових значень і запускається тема основної роботи сервера внутрішньої генерації для поповнення запасу за поточним адресом блоку адресації використаного набору початкових значень.) Після закінчення шифрування порції інформації сервер основної генерації перевіряє поточний потенціал набору поточних початкових значень основної генерації (довжина буфера + довжина холостої прокрутки(від 6)), відстежує холосту прокрутку блоку основної генерації і оновлює поточні початкові значення разом з поточною адресою результату і поточне значення потенціалу в постійній пам'яті. При суворій дисципліні шифрування нульові шифруючі байти перехоплюються, оскільки вони. власне кажучи, не перетворюють вхідну інформацію, при цьому лічильник залишку довжини перетворюваного буфера не змінюється. (В режимі подвійного шифрування в такій дисципліні немає потреби, оскільки збіг двох послідовностей нульових шифруючих байтів, що й так вельми короткі і не часті, є неймовірним. Тому почути і розпізнати щось „натуральне” сторонній особі, що має доступ до лінії зв'язку, просто неможливо.) Блок основної генерації складається з восьми однотипних трирегістрових суматорів, що використовують поточні значення операндів у регістрах і адресу регістру результату. Біти переповнення регістрів результату перетворюються у шифруючий байт, доступний у сервері інтерфейсу (по черзі в одному з двох місць - мікробуфер для можливого підвищення швидкодії). Статистичні дослідження показують, що цілком прийнятним варіантом генерації є генерація шифруючих байтів одним трирегістровим суматором. В цьому випадку шифруючий байт отримують просто із старшого байту результату двоїчного додавання. Сервер основної генерації веде лік байтів і цикл повторюється до зупинки або паузи, що визначається сервером інтерфейсу шифрування.

Реєстр інформації серверу основної генерації (параметри, сигнали, дані, адреси):

Тема координації - інтервал часу очікування нових порцій даних, довжина регістрів початкових значень і результату, довжина шифруючих слів, кількість трирегістрових суматорів, кількість холостих прокруток між порціями даних; сигнали готовності буферів, сигнал першого циклу, лічильник довжини буфера, залишковий потенціал початкових значень, лічильник холостої прокрутки, сигнал звернення до запасу початкових значень; початкові значення і адреса результату основного генератора, їх поточні і кінцеві значення, шифруючі байти (слова); адреси для запису всього стану пристрою при терміновому завершенні/відновленні роботи пристрою.

4) Сервер інтерфейсу шифрування відстежує наявність даних для шифрування, готовність вхідного буфера, звільнення вихідного та закінчення шифрування активного буфера. При відсутності нових даних для обробки сервер інтерфейсу переводить пристрій у стан очікування, що відстежується сервером основної генерації. Після закінчення обробки даних активного буфера змінює ролі цих трьох буферів (циклічно - додаванням одиниці по модулю 3; на початку обробки - послідовно виконується заповнення вхідного буфера, активний буфер пустий, вихідний вважається вільним, бо пустий, а далі вихідний стає вхідним, активний стає вихідним, вхідний стає активним і в ньому починається обробка, і, нарешті, на третьому циклі починається передача зашифрованих даних; подальша обробка - аналогічно; закінчення обробки порції даних наступає на два кроки пізніше початку надходження даних). При відповідній швидкодії трьохбуферний інтерфейс може бути замінений двобуферним. Четвертий буфер (раніше названий мікробуфером серверу основної генерації) є джерелом шифруючих слів, що поєднуються блоком логічної операції „виключення „АБО” з елементами даних активного буфера.

Реєстр інформації серверу інтерфейсу шифрування (параметри, сигнали, дані, адреси):

Тема буферизації - кількість і довжина буферів; сигнал наявності даних, сигнал закінчення порції даних, номер поточного активного „мікробуфера” і сигнал звільнення „мікро буфера” серверу основної генерації, сигнал очікування в сервер основної генерації, індикація (сигнал) закінчення процесу передачі даних; лічильник поточної залишкової довжини буфера; поточна довжина даних у буфері (може відрізнятися від довжини буфера для останнього буфера порції даних), вміст буферів інтерфейсу шифрування і „мікро буферів” серверу основної генерації, поточний розподіл призначення буферів (включаючи початковий і кінцевий стан обробки і передачі даних), номер поточного активного „мікро буфера”; -.

Таким чином, режим „термінового збереження”/„повторного запуску” дозволяє уникнути втрати бодай одного байту в шифруванні, що є критичним для можливості відтворення зашифрованої інформації.

Режим вмикання/відмикання пристрою полягає в тому, що при терміновому вимиканні (немає сигналу очікування наступного повідомлення) пристрій автоматично переводиться в режим термінового збереження і, після завершення запису стану пристрою і даних в спеціальну область постійної пам'яті - разом з признаком аварійного завершення, вимикається підзаряджуваний акумулятор. При вмиканні пристрою цей акумулятор під'єднується для підзарядки, перевіряється признак аварійного завершення, в разі необхідності повністю відновлюється весь стан пристрою і всі поточні дані (зчитуванням із спеціальної області постійної пам'яті), і пристрій готовий продовжувати обробку даних, що передаються, або приймаються.

Режим подвійного шифрування здійснюється фактичним дублікатом пристрою за винятком серверу інтерфейсу шифрування, блоку живлення, тощо.

Взаємодія основних блоків пристрою описана в термінах серверів і тем і має бути відтворена з урахуванням потреби в деяких елементах контролю (лічильників, логічних схем, тригерів, тощо), згрупованих у блоки вибору (скінчені автоматом) відповідних тем за сигналами стану, режимами і таким іншим. Перекомпоновка схем пристрою в блоках для спрощення контролю може бути здійснена після формальної постановки задачі згідно з технологією

виготовлення скінчених автоматів. При цьому визначення теми опрацьовуваної блоком представляють в блоках флажками (при потребі), а зайнятість/звільнення/готовність компонент пристрою представляють семафорами (при потребі). Це залежить відповідно від дублювання схем пристрою і швидкодії. Тому відтворення взаємодії компонентів пристрою у викладі суті винаходу, наведеному вище, є максимально лаконічним.

Використання нових компонент електронних схем (трирегістровий суматор та паралельний стек) доцільне в швидкісних лініях зв'язку. Ці схеми можуть бути замінені традиційними конструктивними компонентами.

Спосіб генерації псевдовипадкових чисел і цифровий пристрій, що його реалізує

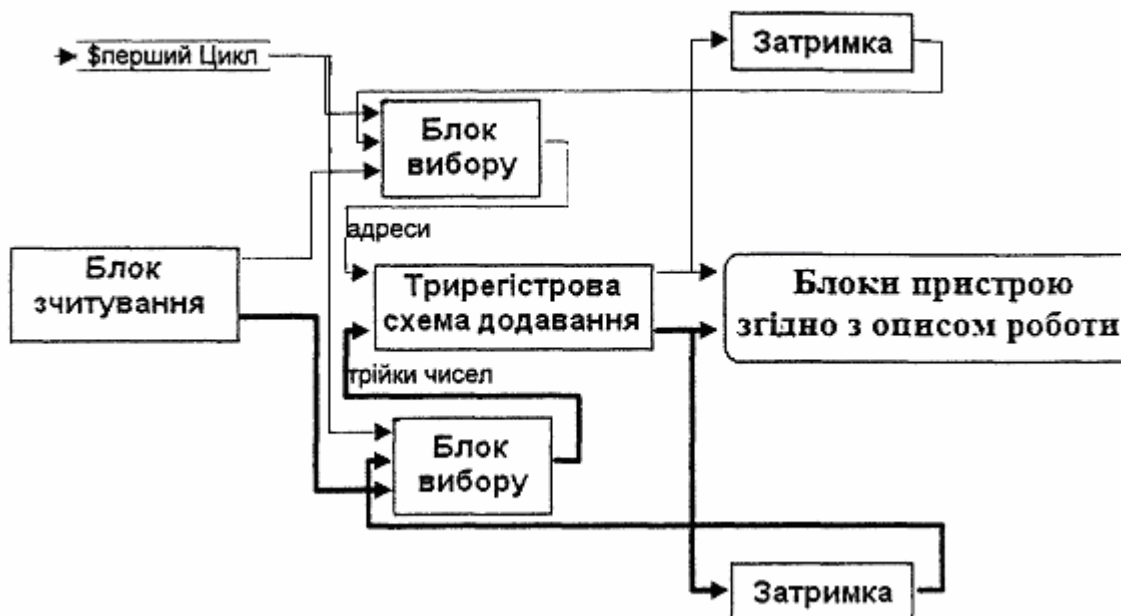


Fig. 1

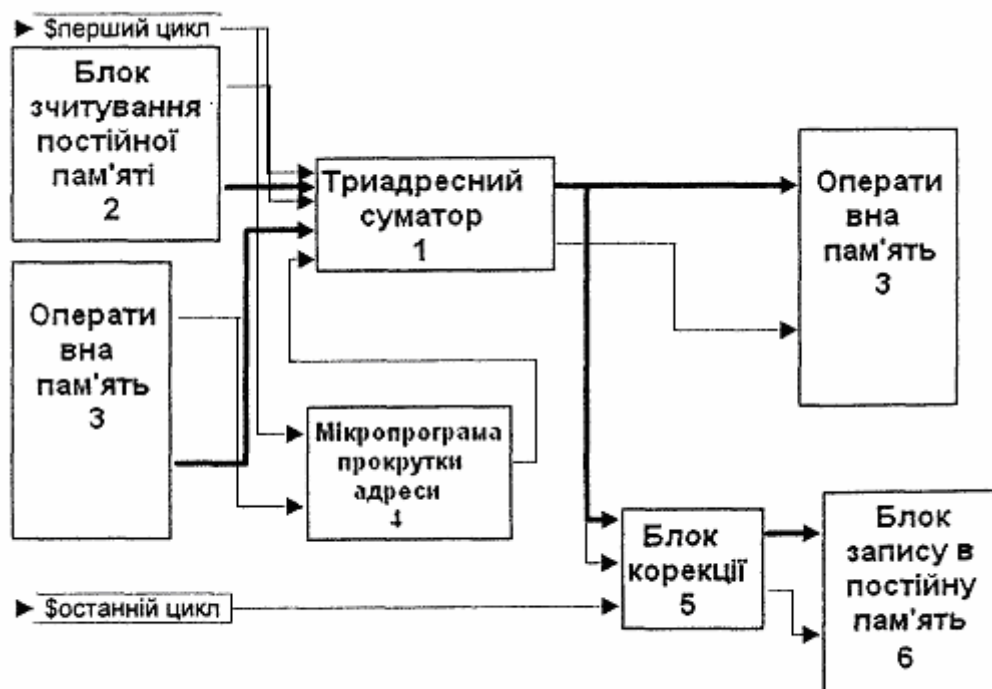
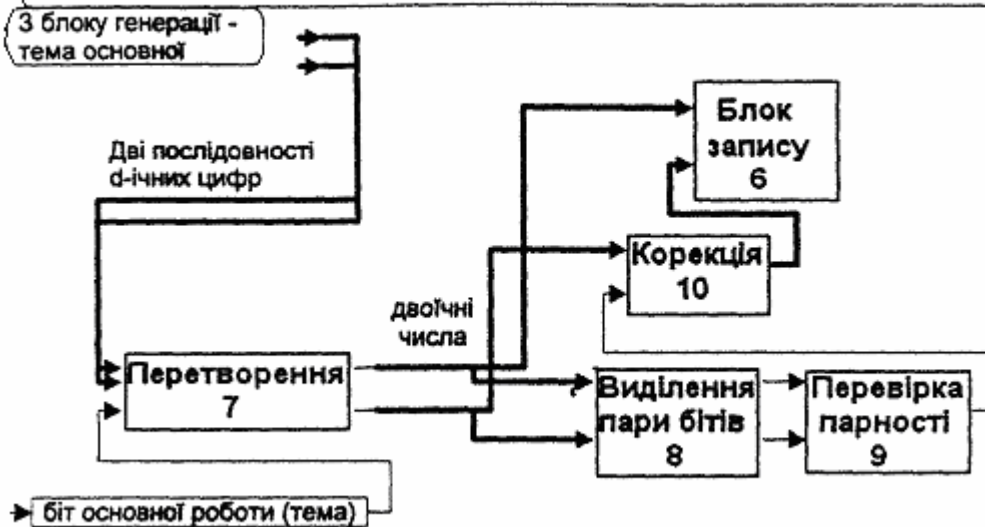
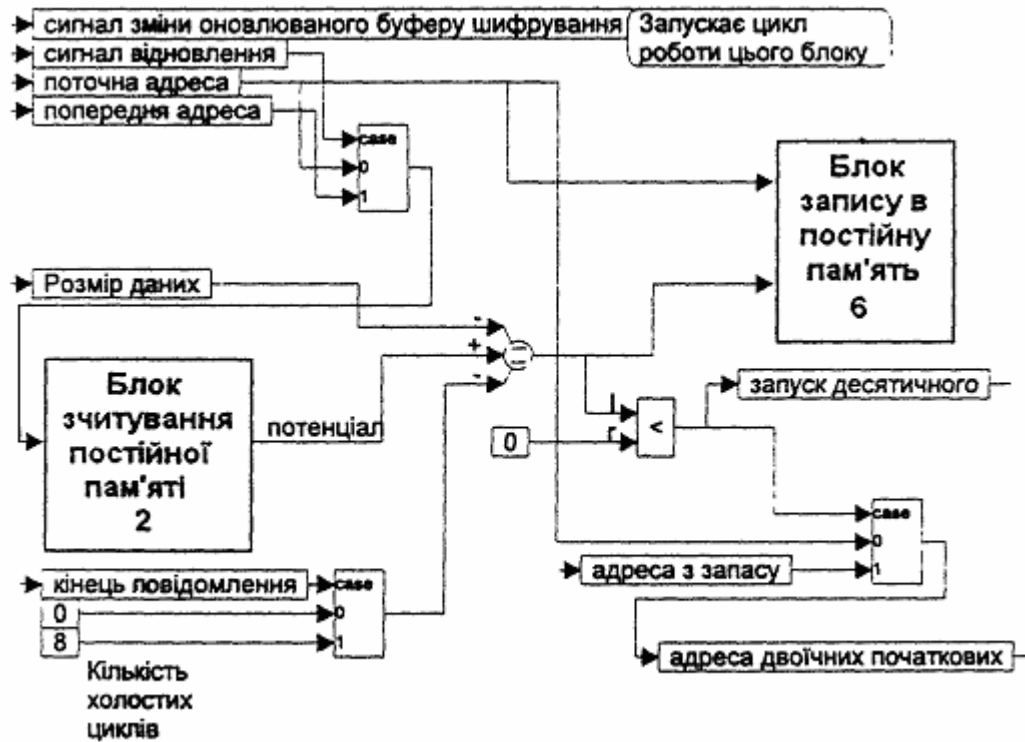


Fig. 2

Спосіб генерації псевдовипадкових чисел і цифровий пристрій, що його реалізує



Фіг. 3



Фіг. 4

Спосіб генерації псевдовипадкових чисел і цифровий пристрій, що його реалізує



Фіг. 5



Фіг. 6