ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки
Кафедра ЕОМ

Методи покращення параметрів алгоритму потокового шифрування

Кваліфікаційна робота
Другий (магістерський) рівень

Автор:
Науменко М.В.,
студ. гр. СПм-22-2

Керівник:
Торба А.А.,
проф. каф. ЕОМ

1

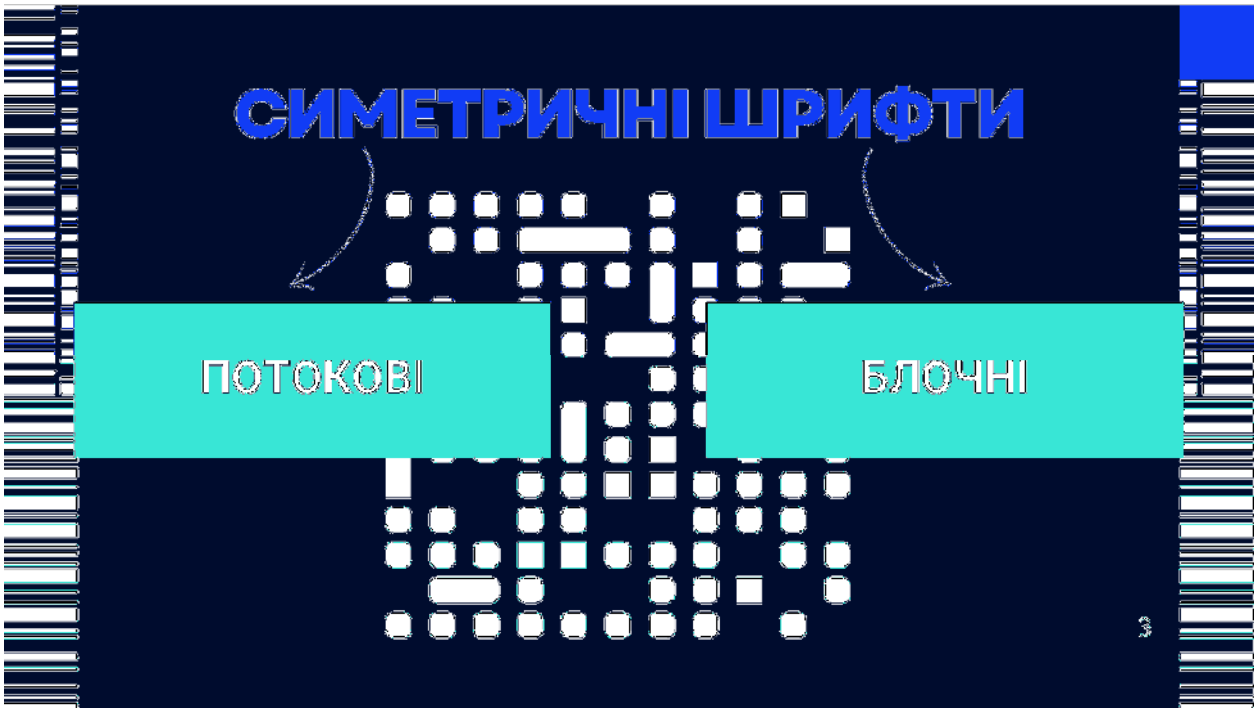
Мета і задачі роботи:

Мета:
визначити ефективні механізми поліпшення криптостійкості алгоритмів потокового шифрування

Завдання:

- аналіз існуючих алгоритмів потокового шифрквання і методів покращення їх криптостійкості;
- розробка відчизняних алгоритмів потокового шифрування на основі ДЛРР і методів покращення їх криптостійкості;
- аналіз криптостійкості потокових шифрів при зміні параметрів ДЛРР.

2


СИМЕТРИЧНІ ШРИФТИ
ПОТОКОВІ
БЛОЧНІ
3


ПЕРЕВАГИ
ПОТОКОВІ
Висока швидкість шифрування
Шифрування аудіо- або відеопотоків в реальному масштабі часу
Більше підходять для апаратної реалізації
БЛОЧНІ
Легше реалізовувати програмно
Уникання трудомістких маніпуляцій з бітами
Оперування зручними для комп'ютера блоками даних
4

ДЛЯ ПОТОКОВИХ ШИФРІВ ХАРАКТЕРНИМ Є ПОБІТОВА ОБРОБКА ІНФОРМАЦІЇ

Загальна схема передачі інформації потоковими шифрами

5

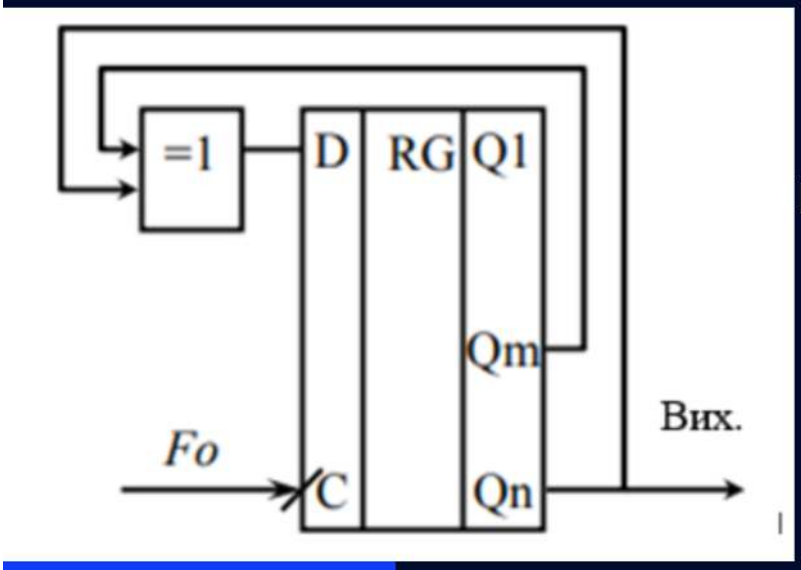
ДЛЯ ПОТОКОВИХ ШИФРІВ ХАРАКТЕРНИМ Є ПОБІТОВА ОБРОБКА ІНФОРМАЦІЇ

Загальна схема передачі інформації потоковими шифрами

5

Узагальнена схема шифрування поточними шифрами (із прикладом)

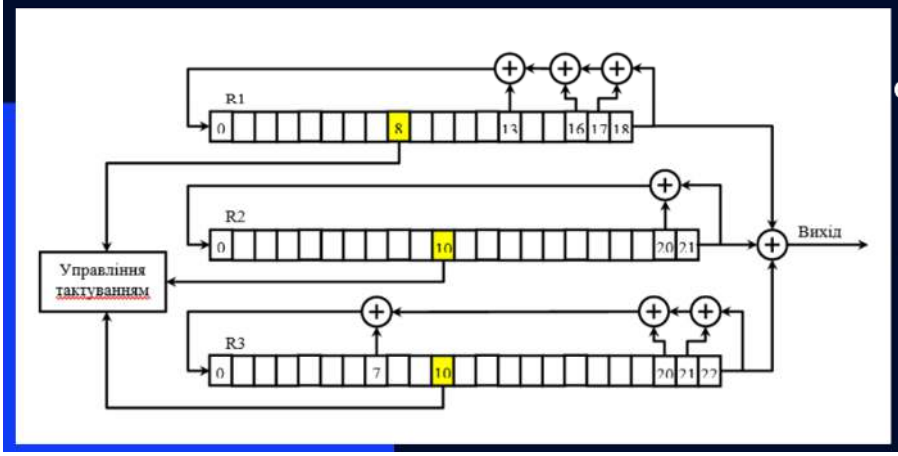
6



ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ лінійного рекурентного регістру

7

СТРУКТУРНА СХЕМА АЛГОРИТМУ А5



Конфіденційність переданих даних між телефоном і базовою станцією в європейській системі мобільного цифрового зв'язку GSM (Group Special Mobile)

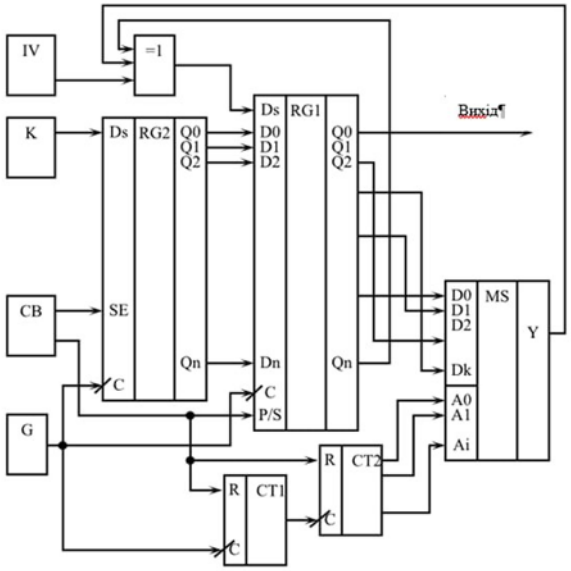
8

Відомі теоретичні критерії Райнера Рюппеля для проектування Потокових Шифрів:

- довгі періоди вихідних гамуючих псевдовипадкових послідовностей, що наближає такі шифри до теоретично незламного шифру – «відривний блокнот»;
- велика лінійна складність;
- дифузія – розсіювання надлишковості в підструктурах, «розмазування» статистики по всьому гамуючому потоку;
- кожен біт гамуючої послідовності повинен бути складним перетворенням більшості бітів ключа;
- критерій нелінійності для логічних функцій.

9

Алгоритм потокового шифрування «AUGUST-1»

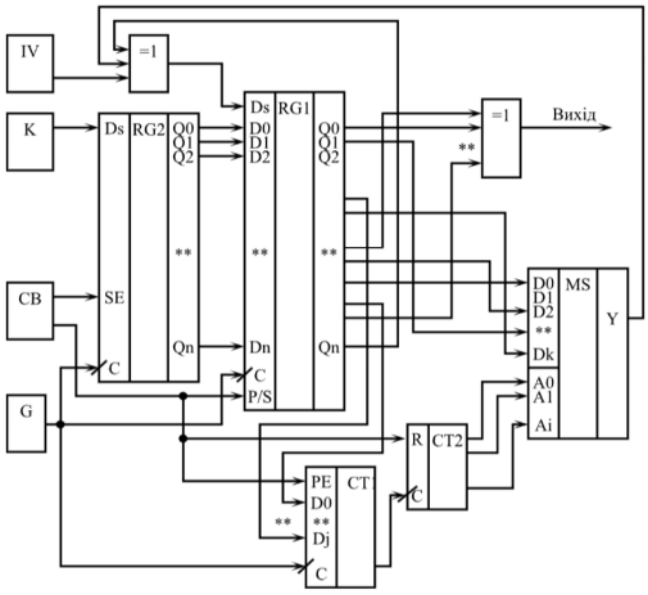


ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР ,РЕАЛІЗОВАНИЙ НА РЕГІСТРІ ЗСУВУ

Руйнує лінійні залежності в сформованій псевдовипадковій гамуючий послідовності

10

Алгоритм потокового шифрування «AUGUST-2»



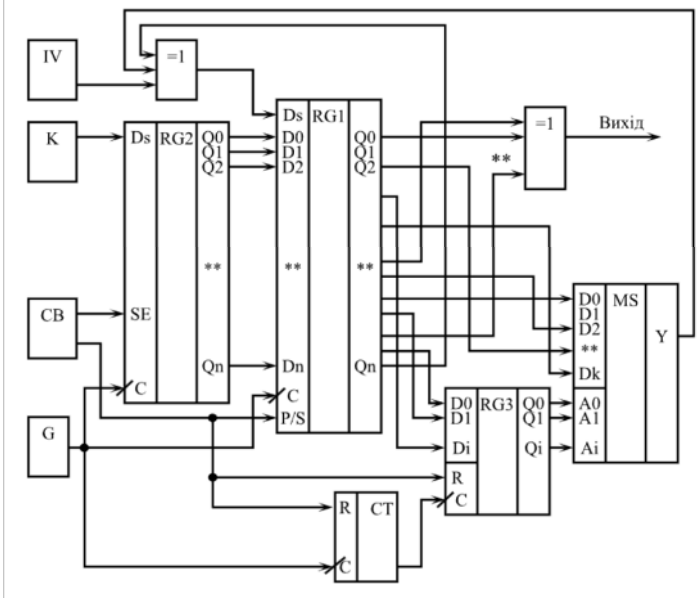
ДИНАМІЧНИЙ ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР

Змінює величини інтервалів часу між змінами параметрів рекуренти в псевдовипадковому порядку.

Введення другого вихідного елемента «ВИКЛЮЧНЕ АБО».

11

Алгоритм потокового шифрування «AUGUST-3»

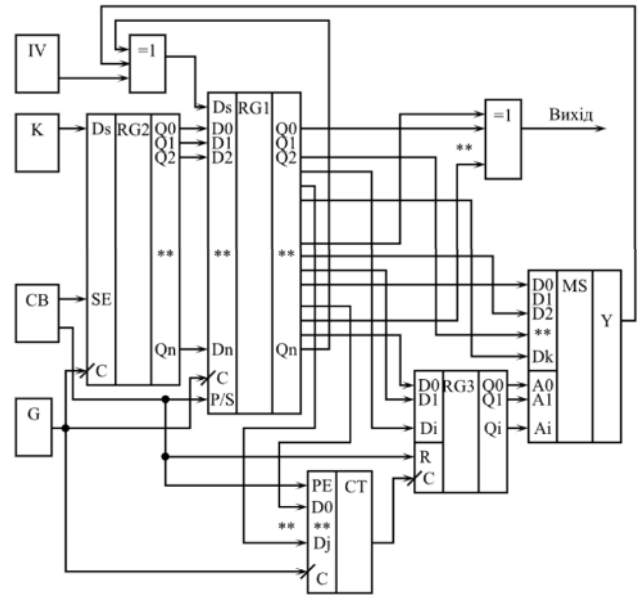


ДИНАМІЧНИЙ ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР

Зміна параметрів рекуренти в псевдовипадковому порядку

12

Алгоритм потокового шифрування «AUGUST-4»



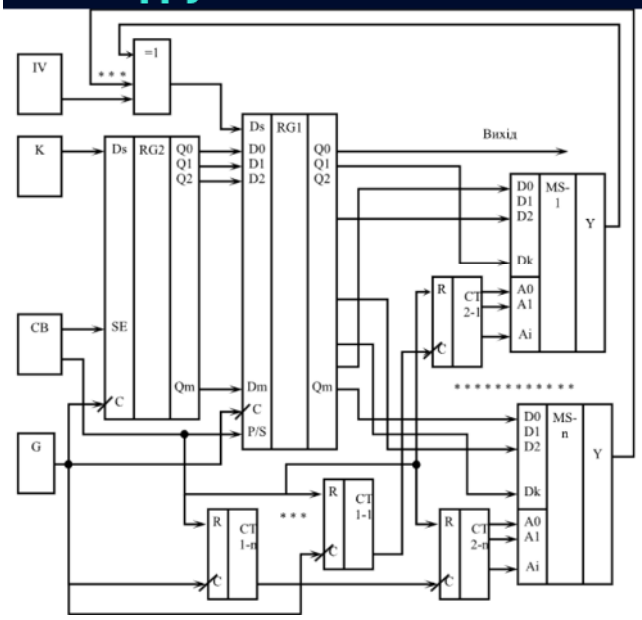
ДИНАМІЧНИЙ ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР

Параметри рекуренти ДЛРР на основі регістру зсуву змінюються у псевдовипадковому порядку

Зміна параметрів рекуренти в псевдовипадковому порядку

13

Алгоритм потокового шифрування «AUGUST-5»

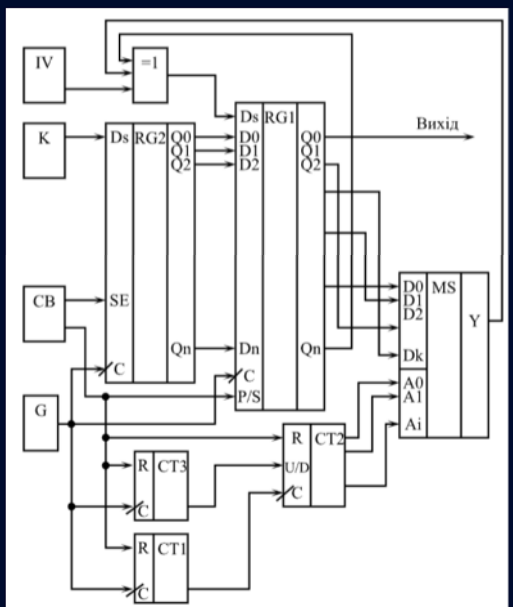


ДИНАМІЧНИЙ ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР ТА МУЛЬТИПЛЕКСОРИ

Мультиплексори (MS-1…MS-n), що змінюють параметри рекуренти – довжину регістру зсуву та номери відводів

14

Алгоритм потокового шифрування «AUGUST-6»



ДИНАМІЧНИЙ ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР ТА МУЛЬТИПЛЕКСОРИ

Реверсивний лічильник CT2 визначає порядок зміни параметрів рекуренти.

Інтервали зміни параметрів рекуренти визначаються дільником CT1.

Інтервали перемикання реверсивного лічильника CT2 визначаються дільником CT3.

15

КРИПТОГРАФІЧНЕ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Напрямки методів криптоаналізу

- Статистичний криптоаналіз
- Диференціальний криптоаналіз
- Алгебраїчний криптоаналіз
- Лінійний криптоаналіз

16

«AUGUST-1» … «AUGUST-6» дають такі переваги:

- Розрядність ДЛЗР, що може становити від 100 до кількох тисяч біт.
- Руйнують лінійні властивості ЛРР і тим самим роблять такі системи криптографічно більш стійкими.
- Присутня дуже велика кількість довготривалих секретних параметрів.

17

ВИСНОВКИ

- **Найважливішою перевагою потокових шифрів перед блочними є висока швидкість шифрування.**
- **Запропоновані і запатентовані в Україні генератори псевдо-випадкових гамуючих послідовностей для потокового шифрування на основі ДЛРР дають змогу усунути більшість недоліків відомого алгоритму А5.**
- **Такі криптоалгоритми на основі ДЛРР наближаються за криптостійкістю до теоретично незламного шифру з «відривним блокнотом», коли довжина одноразового ключа дорівнює довжині всього тексту.**

18

Додаток Б

СЕРТИФІКАТ ПУБЛІКАЦІЇ