Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Методи покращення параметрів алгоритмів потокового шифрування
(тема)

Виконав:

студент II курсу, групи СПм-22-2

Науменко М.В
(прізвище, ініціали)

Спеціальність

123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма

Системне програмування
(повна назва освітньої програми)

Керівник: проф. Торба А.А
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри ЕОМ _____ Коваленко А.А.
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти другий (магістерський)

Спеціальність 123 «Комп'ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Системне програмування
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
"____" _____ 20___ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Науменку Максиму Вікторовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Методи покращення параметрів алгоритмів потокового шифрування

затверджена наказом по університету від " 06 " листопада 2023 р. № 1299Ст

2. Термін подання студентом роботи до екзаменаційної комісії 15 січня 2024 р.

3. Вхідні дані до роботи

Розробка алгоритмів потокового шифрування на основі ЛРР.
Розробка методів зміни параметрів рекуренти при формуванні гамуючої послідовності.
Багатоканальні методи зміни параметрів рекуренти.
Дослідження криптостійкості потокових шифрів при зміні параметрів рекуренти.

4. Перелік питань, що потрібно опрацювати у роботі

Аналіз стану сучасних потокових шифрів.
Аналіз стану потокових шифрів на основі ЛРР.
Зміна параметрів рекуренти потокового шифру.
Вплив зміни параметрів рекуренти на криптостійкість потокового шифру.
Висновки.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) Презентація доповіді – 19 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області	06.11.23 - 21.11.23	
2	Розробка алгоритмів потокового шифрування		
3	на основі ЛРР	15.11.23 - 15.12.23	
	Дослідження криптостійкості потокових		
	шифрів	01.12.23 - 30.12.23	
	Оформлення матеріалів кваліфікаційної роботи	18.12.23 - 10.01.24	
	Подання кваліфікаційної роботи керівникові та	10.01.24 - 11.01.24	
	її попередній захист		
	Подання кваліфікаційної роботи на	12.01.2024	
	рецензування		

Дата видачі завдання 06 листопада 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Торба А.А
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 51 с., 11 рис., 1 табл., 2 дод., 14 джерел.

ПОТОКОВИЙ ШИФР, ГАМУЮЧА ПОСЛІДОВНІСТЬ, ЛІНІЙНИЙ РЕКУРЕНТНИЙ РЕГІСТР, ШВИДКОДІЯ ШИФРУВАННЯ, КРИПТОСТІЙКІСТЬ.

Метою кваліфікаційної роботи є визначення ефективних механізмів поліпшення криптостійкості алгоритмів потокового шифрування

У ході виконання кваліфікаційної роботи проаналізували існуючі алгоритми потокового шифрквання і методів покращення їх криптостійкості. Розроблені відчизняні алгоритми потокового шифрування на основі ДЛРР і методів покращення їх криптостійкості. Проведений аналіз криптостійкості потокових шифрів при зміні параметрів ДЛРР.

ABSTRACT

Master’s thesis: 51 pages, 11 figures, 1 tables, 2 appendices, 14 sources.

FIREWALL, GATE, INTERNET, PROTOCOL, ROUTER, SERVER, WI-FI, WIRELESS NETWORK, WLAN.

The purpose of the qualification work is to identify effective mechanisms for improving the cryptographic security of streaming encryption algorithms

In the course of the qualification work, we analysed existing streaming encryption algorithms and methods for improving their cryptographic strength. The authors developed native streaming encryption algorithms based on the PRNG and methods for improving their cryptographic strength. An analysis of the cryptographic resistance of streaming ciphers when changing the parameters of the PRNG is carried out.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AES – англ. Advanced Encryption Standard – сучасний стандарт шифрування.

БШ – блочний шифр.

ВП – випадкова послідовність.

ГПВБ– генератор псевдовипадкових бітів.

ДЛРР – динамічний лінійний рекурентний регістр.

ЕЦП – електроний цифровий підпис.

КА – криптоалгоритм.

ЛРР – лінійний рекурентний регістр.

ПВП – псевдовипадкові послідовності.

ПЛІС – програмована логічна інтегральна схема.

ПШ – поточний шифр.

РЗП – регістр загального призначення.

ВСТУП

В сучасному інформаційному суспільстві, де обмін електронною інформацією відіграє ключову роль, забезпечення безпеки цієї інформації стає надзвичайно важливим завданням для державних та комерційних структур. Криптографія, яка вивчає методи захисту інформації від несанкціонованого доступу, використовує різноманітні криптоалгоритми для шифрування та розшифрування даних. Криптоалгоритми визначаються як математичні процедури, що виконують перетворення даних з одного вигляду в інший з метою захисту конфіденційності та цілісності інформації.

Криптоалгоритми (КА) можливо класифікувати за різними критеріями, враховуючи їхні властивості та призначення. Одним із важливих аспектів класифікації є тип ключа, використаного для шифрування та розшифрування даних. У цьому контексті розрізняють симетричні та асиметричні криптоалгоритми.

Також криптоалгоритми поділяються в залежності від кількості ключів, які застосовуються у конкретному алгоритмі:

- безключові КА – не використовують в обчисленнях ніяких ключів;
- одноключові КА – працюють з одним додатковим ключовим параметром (якимось таємним ключем);
- двоключові КА – на різних стадіях роботи в них застосовуються два ключових параметри: секретний та відкритий ключі.

В задежності від характеру впливів, що виробляються над даними, алгоритми підрозділяються на:

- перестановочні - блоки інформації (байти, біти, більші одиниці) не змінюються самі по собі, але змінюється їх порядок проходження, що робить інформацію недоступною сторонньому спостерігачеві.
- підстановочні - самі блоки інформації змінюються за законами криптоалгоритму. Переважна більшість сучасних алгоритмів належить цій групі.

Залежно від розміру блоку інформації криптоалгоритми поділяються на:

Потокові шифри (ПШ) - одиницею кодування є один біт. Результат кодування не залежить від минулого раніше вхідного потоку. Схема застосовується в системах передачі потоків інформації, тобто в тих випадках, коли передача інформації починається і закінчується в довільні моменти часу і може випадково перериватися. Потокові шифри використовуються при побітовому шифруванії за допомогою програмованих логічних інтегральних схем (ПЛІС). Найбільш поширеними представниками потокових шифрів являються скремблери.

Блочні шифри (БШ) – одиницею кодування є блок з декількох бітів (в даний час від 32 до 512). Результат кодування залежить від усіх вхідних бітів цього блоку. Розмір блоку співпадає з розміром регістірів загального призначення (РЗП) комп'ютера. Схема застосовується при пакетній передачі інформації та кодування файлів.

Крім того, криптоалгоритми можливо класифікувати за їхньою основною функціональністю, такою як шифрування, хешування та цифровий підпис. Кожен з цих видів криптоалгоритмів виконує унікальні завдання забезпечення безпеки інформації в різних контекстах.

Симетричні криптоалгоритми використовують один і той же ключ для обох операцій шифрування та розшифрування. Вони відомі своєю ефективністю та швидкістю, але вимагають надійного каналу для обміну ключами між взаємодіючими сторонами. З іншого боку, асиметричні криптоалгоритми використовують пару ключів: публічний та приватний. Публічний ключ використовується для шифрування даних, а приватний - для їхнього розшифрування. Цей тип криптоалгоритмів забезпечує безпеку обміну ключами, але може бути менш ефективним з точки зору швидкодії порівняно з симетричними алгоритмами.

Головною умовою при використані технічних або програмних засобів захисту важливої інформації є використання відчизняних криптосистем, що

виключає вплив на процеси перетворення інформації, так званих, «закладок», які дозволяють втручатися (проникати) в процес шифрування та дешифрування небажаним порушникам (зловмисникам).

Мета, основні завдання і напрями досліджень, відбиті в кваліфікаційній роботі.

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.

1 ПОТОКОВІ ШИФРИ

1.1 Потокові шифри

Існує велика кількість досліджень в напрямку розробки потокових шифрів, оскільки симетричні алгоритми почали розвиватися значно раніше асиметричних. Для потокових шифрів характерним є побітова обробка інформації (рисунок.1.1). Обробка інформації такого типу може бути представлена у вигляді автомату, що на кожному такті:

- генерує за певним алгоритмом біт шифруючої (гамуючої) послідовності;
- деяким зворотнім перетворенням накладає на один біт відкритого потоку інформації шифруючий біт і в результаті отримує зашифрований біт.

Причиною достатності одного біта на біт вихідного тексту при шифруванні послідовності є наявність оборотних операцій алгебри логіки або комп'ютерної арифметики за модулем 2, а саме: додавання за модулем два та відрахування за модулем два.

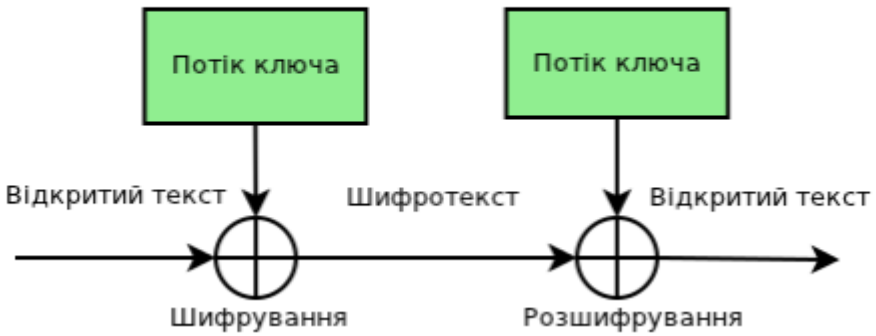

Рисунок. 1.1– Загальна схема передачі інформації потоковими шифрами

Обортною операцією є та, в якій при відомому результаті та всіх операндах, крім одного, можливо відновити цей невідомий операнд. Іншими словами: при таких перетвореннях не втрачається частина інформації. Отже при шифруванні можливим є застосування лише оборотних операцій і

фактично усі алгоритми такого шифрування організовані таким чином, що на один біт первісного тексту накладаються шифруючі біти (скільки б їх не було створено) шляхом комбінацій з зазначених вище двох операцій – XOR та заперечення (інверсія). Заперечення можливо вставити в середину операції XOR, тобто для будь яких значень *a* і *b* є вірним: NOT (*a* XOR *b*) = *a* XOR (NOT *b*) XOR *b*.

Звідси висновок, що композицію з вихідного та шифруючих бітів, можливо розділити та представити у вигляді: *p* XOR *F* (g1, g2, g3),

де *p* – первісний біт,

g – шифруючий біт,

F – певна функція, що містить XOR та заперечення.

В підсумку вся формула матиме вигляд: *c* = *p* XOR *g*

Загальна схема шифрування поточним шифром (рисунок.1.2)

Рисунок. 1.2 – Узагальнена схема шифрування поточними шифрами (із прикладом)

За даною схемою працюють усі поточні шифри. Символом гама (γ) прийнято позначати біт шифрування чи цілий набір таких біт, що з’являються на кожному кроці автомату. Через це такі алгоритми іменують деколи гама шифрами. За умови апаратної реалізації ці шифри значно швидші за блочні, а при програмній зазвичай не мають переваг у швидкості.

Три основних складових над якими обчислюється функція, що

породжує гаму:

- ключ;
- номер поточного кроку шифрування;
- найближчі від поточної позиції біти первісного і (або) зашифрованого тексту.

1.2 Особливості генерації ПВП на основі ЛРР

Найвідомішим криптографічним алгоритмом генератором псевдовипадкових послідовностей (ГПВП) є лінійний рекурентний регістр – ЛРР (Рисунок 1.3)

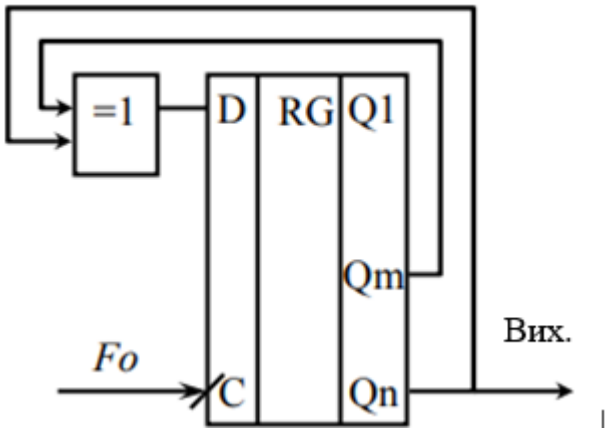

Рисунок 1.3 – ГПВП на основе ЛРР

Бітові послідовності, що знімаються з будь-якого розряду регістра зсуву, проходять усі статистичні тести на випадковість.

Послідовний регістр RG довжиною «*n*» здійснює зсув збереженого коду після кожного тактового імпульсу з частотою *Fo*. Вхідний сигнал D першого тригера регістра формується за допомогою елемента ВИКЛЮЧНЕ АБО (суматора за модулем 2), на входи якого надходять сигнали від *m*-того та останнього (*n*-того) розрядів регістра.

Така схема проходить через безліч станів, які після *K* тактів починають повторюватися, тобто послідовність станів є циклічною з періодом *K*.

Максимальне число можливих станів *n*-розрядного регістра дорівнює: $K = 2^n$, тобто числу *n*-бітових двійкових комбінацій. Однак стан «усі нулі» для цієї схеми є «тупиковим», оскільки на входах і на виході елемента "ВИКЛЮЧНЕ АБО" постійно з'являються нулі, які надходять на вхід схеми і зациклюються.

Якщо для формування вхідного сигналу використовувати елемент «ВИКЛЮЧНЕ АБО з інверсією», то «тупиковою» буде комбінація – «усі одиниці».

Таким чином, послідовність максимальної довжини, яку може сформувати ця схема, містить $K = (2^n - 1)$ біт.

У таблиці 1.1 наведено розрахункові значення періодів повторення ПВП на основі ЛРР при тактовій частоті *Fo* = 100 МГц.

Таблиця 1.1 - Періоди ЛРР для різних довжин «*n*»

n	$K = 2^n - 1$	сек	год	днів	років
40	1,09951E+12	10995,11628	3,054198966		
50	1,1259E+15	11258999,07	3127,499741	130,3125	
60	1,15292E+18	11529215046	3202559,735	133440	365,589
70	1,18059E+21	1,18059E+13	3279421169	1,37E+08	374363,1
80	1,20893E+24	1,20893E+16	3,35813E+12	1,4E+11	3,83E+08
90	1,23794E+27	1,23794E+19	3,43872E+15	1,43E+14	3,93E+11
100	1,26765E+30	1,26765E+22	3,52125E+18	1,47E+17	4,02E+14

Виявляється, що таку послідовність максимальної довжини можливо отримати тільки при правильному виборі «*m*» і «*n*». Критерієм максимальної довжини є непривідність і примітивність многочлена $1 + x^n + x^m$ над полем Галуа [1,2,3].

Регістри зсуву максимальної довжини можливо виконати з числом відводів у ланцюзі зворотного зв'язку понад 2 (у цьому разі використовується кілька елементів «ВИКЛЮЧНЕ АБО», з'єднаних у вигляді стандартного

«дерева парності») (рисунок 1.4). Для деяких значень *n* регістр максимальної довжини можливо реалізувати тільки з числом відводів понад 2 [2, 3].

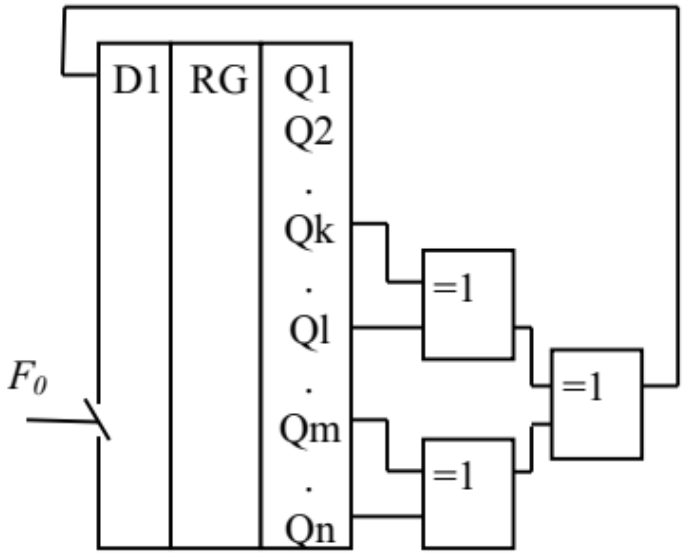

Рисунок 1.4 – ЛРР з 4-ма відводами

Генератори ПВП на зсувних регістрах (ЛРР) можливо використовувати для шифрування повідомлень і даних, оскільки ідентичний генератор ПВП на приймальному кінці формує таку ж саме гамуючу послідовність до шифру. ПВП широко використовуються в кодах, що виявляють і виправляють помилки, оскільки вони дозволяють видозмінити блоки даних таким чином, що правильні кодові повідомлення будуть перебувати одне від одного на максимально можливій «відстані Хеммінга» (вимірюється числом позицій з різними даними) [2,3].

1.3 Потоковий шифр А5 на основі ЛРР

Відомий потоковий алгоритм шифрування А5 використовується для забезпечення конфіденційності переданих даних між телефоном і базовою станцією в європейській системі мобільного цифрового зв'язку GSM (Group Special Mobile).

Шифр ґрунтується на побітовому додаванні за модулем два (булева операція XOR) генерованої псевдовипадкової послідовності (гами) і інформації, яка підлягає шифруванню.

В A5 псевдовипадкова послідовність гами реалізується на основі трьох лінійних рекурентних регістрів (ЛРР) зсуву зі зворотним зв'язком. Регістри мають довжини: L(R1) = 19, L(R2) = 22 і L(R3) = 23 біти (рисунок 1.5). Зсувами керує спеціальна схема.

У кожному регістрі є біти синхронізації: R1(8), R2(10) і R3(10), над якими обчислюється мажоритарна функція:

$$F = (x \,\&\, y)\ V\ (x \,\&\, z)\ V\ (y \,\&\, z),$$

де: *x, y, z* - біти синхронізації.

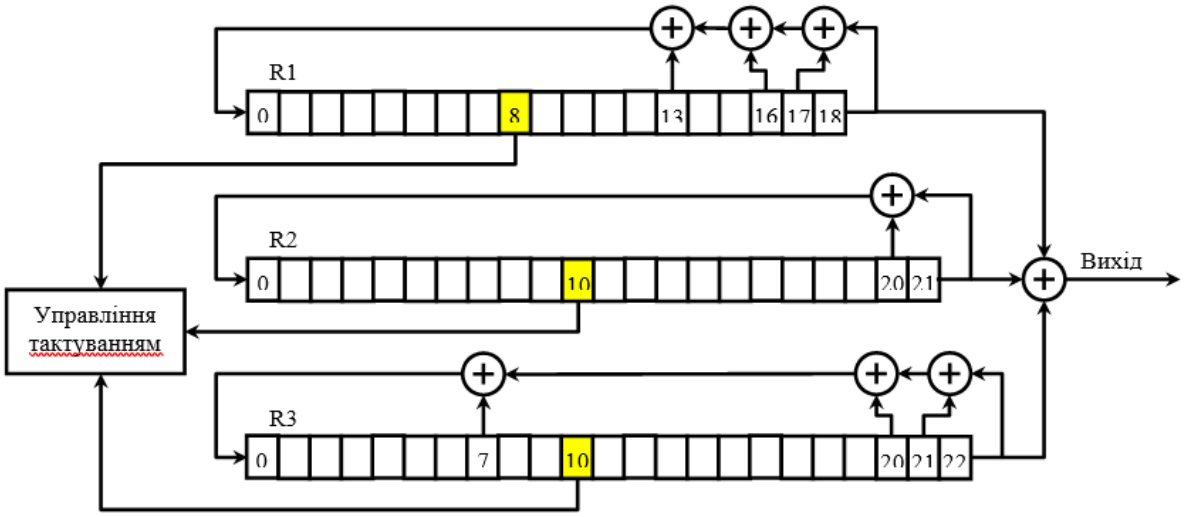

Рисунок.1.5 – Структурна схема алгоритму A5

У кожному такті зміщується тільки той регістр, у якого біт синхронізації дорівнює функції *F*, тобто на кожному кроці зміщується два або три регістри, що призводить до їхнього нерівномірного руху. Результуюча псевдовипадкова послідовність формується шляхом операції XOR над вихідними бітами трьох регістрів (рисунок. 1.5).

Недоліком алгоритму A5 є неприпустимо мала криптостійкість, що визначається довжиною сеансового ключа – 64 біти (яка визначається

сумарною довжиною всіх ЛРР), тому складність атаки, заснованої на прямому переборі, не перевищує: 2^{64}.

З огляду на те, що в алгоритмі А5 примусово обнулено 10 біт ключа, криптостійкість цього алгоритму навіть нижча, ніж в алгоритму DES (з довжиною ключа – 56 біт).

Практика показує, що понад 40 % сеансових ключів в алгоритмі А5 призводять до мінімальної довжини періоду псевдовипадкової послідовності, що генерується, а саме: $T = 2^{23} - 1$.

Відома також атака Андерсона на відкритому тексті, заснована на припущенні про зміст перших двох ЛРР і спробі визначення найдовшого третього ЛРР за ключовою послідовністю.

1.4 Методи підвищення криптостійкості потокових шифрів

Більшість існуючих симетричних шифрів однозначно можуть бути віднесені або до потокових (ПШ), або до блочних шифрів (БШ). Але теоретична межа між ними є досить розмитою. Наприклад, алгоритми блокового шифрування часто використовуються в режимі потокового шифрування.

Найважливішою перевагою потокових шифрів перед блочними є висока швидкість шифрування, яка співпадає зі швидкістю надходження вхідної відкритої інформації, що дозволяє шифрувати аудіо- або відеопотоки в реальному масштабі часу.

Потокові шифри, які шифрують і дешифрують дані по одному біту, не дуже підходять для програмних реалізацій. А блочні шифри легше реалізовувати програмно, оскільки вони дозволяють уникнути трудомістких маніпуляцій з бітами і оперують зручними для комп’ютера блоками даних, співмірними з розрядністю регістрів загального призначення (РЗП). З іншого боку, потокові шифри на регістрах зсуву більше підходять для апаратної реалізації [8].

Згідно з Райнером Рюппелем можливо виділити чотири основні підходи до проектування потокових шифрів [5,6]:

- системно-теоретичний підхід заснований на створенні для криптоаналітика складної, раніше недослідженої проблеми;
- складностно-теоретичний підхід заснований на складній, але відомій проблемі (наприклад, факторизація чисел або дискретне логарифмування);
- інформаційно-технічний підхід заснований на спробі приховати відкритий текст від криптоаналітика – незалежно від того скільки часу витрачено на дешифрування, криптоаналітик не знайде однозначного рішення;
- рандомізований підхід заснований на створенні об'ємної задачі; криптограф тим самим намагається зробити рішення задачі розшифрування фізично неможливим.

Відомі теоретичні критерії Райнера Рюппеля для проектування ПШ:

- 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.

Велика кількість реальних потокових шифрів (ПШ) заснована на регістрах зсуву з лінійним зворотним зв'язком – лінійних рекурентних регістрах (ЛРР). Головні переваги ЛРР [5, 6]:

- висока швидкодія криптографічних алгоритмів;
- застосування тільки найпростіших логічних операцій: кон'юнкції, диз'юнкції і XOR (виключне АБО), апаратно реалізованих у всіх обчислювальних пристроях;

- хороші криптографічні властивості (генеровані послідовності мають великий період і хороші статистичні властивості);

- легкість аналізу з використанням алгебраїчних методів за рахунок лінійної структури.

Самі по собі ЛРР є хорошими генераторами псевдовипадкових послідовностей, але вони мають деякі небажані невипадкові властивості [4]:.

Навіть якщо параметри рекуренти (номери відводів «m_k» зворотного зв'язку) зберігаються в секреті, вони можуть бути визначені по $2n$ вихідним бітам генератора за допомогою алгоритму Берлекемпа-Мессі.

Існує кілька методів проектування генераторів псевдовипадкового гамуючого потоку, які руйнують лінійні властивості ЛРР і тим самим роблять такі системи криптографічно більш стійкими:

- використання нелінійної функції, що об'єднує виходи декількох ЛРР (генератор Геффа та ін.);

- використання нелінійної фільтруючої функції для вмісту кожної комірки єдиного ЛРР;

- використання виходу одного ЛРР для управління синхросигналом одного (або декількох) ЛРР (алгоритм А5 та ін.) [8];

- динамічна зміна параметрів рекуренти (довжини регістру «n» і номерів відводів «m_k») в процесі формування псевдовипадкової гамуючої послідовності, – так звані динамічні лінійні рекурентні регістри (ДЛРР) [8].

2 АЛГОРИТМИ ПОТОКОВОГО ШИФРУВАННЯ AUGUST

2.1 Алгоритм потокового шифрування «AUGUST-1»

Основу найпростішого алгоритму формування гамуючої послідовності для потокового шифрування «AUGUST-1» [4,5,8] становить лінійний рекурентний регістр (ЛРР), реалізований на регістрі зсуву (RG1) (рисунок 2.1). На інформаційний вхід послідовного зсуву (Ds) цього регістру подається сигнал із виходу елемента «ВИКЛЮЧНЕ АБО» (елемента «XOR»), а до входів цього елементу підключені: останній вихід регістра зсуву Qn і вихід мультиплексора MS.

Інформаційні входи (D0...Dk) мультиплексора (MS) під'єднані у довільному (випадковому) порядку до відводів регістра зсуву (RG1). Номери всіх відводів «m_k» повинні задовольняти відомій умові для ЛЛР: поліном, обчислений на коефіцієнтах –

$$1 + x^m + x^n \qquad 2.1$$

– має бути примітивним і неприведеним над полем Галуа [4, 5, 6, 7].

Номери відводів «m_k», які задовольняють умові (2) для довжин ЛРР до 400 розрядів, наведені у монографії [7].

На адресні входи мультиплексора MS (A0...Ai) подаються послідовні двійкові коди з виходів лічильника CT2. Коефіцієнт ділення лічильника CT1 визначає періодичність зміни параметрів рекурренти (зазвичай ця періодичність у кілька разів менша за розрядність регістра зсуву «n»). Треба обирати коефіцієнт ділення лічильника CT1 і довжину ДЛРР (тобто розрядність «n» регістра зсуву RG1) як взаємно прості числа.

Швидкість формування псевдовипадкової гамуючої послідовності визначається частотою тактового генератора (G) і може становити від 10 МГц до 1 ГГц.

До початку шифрування абоненти обмінюються секретними короткочасними (сеансовими) ключами Кс. Алгоритм Діффі-Хеллмана (англ.

Diffie-Hellman, D-H) дає змогу двом або більше користувачам обмінятися без посередників секретним ключем, який буде використаний потім для симетричного шифрування.

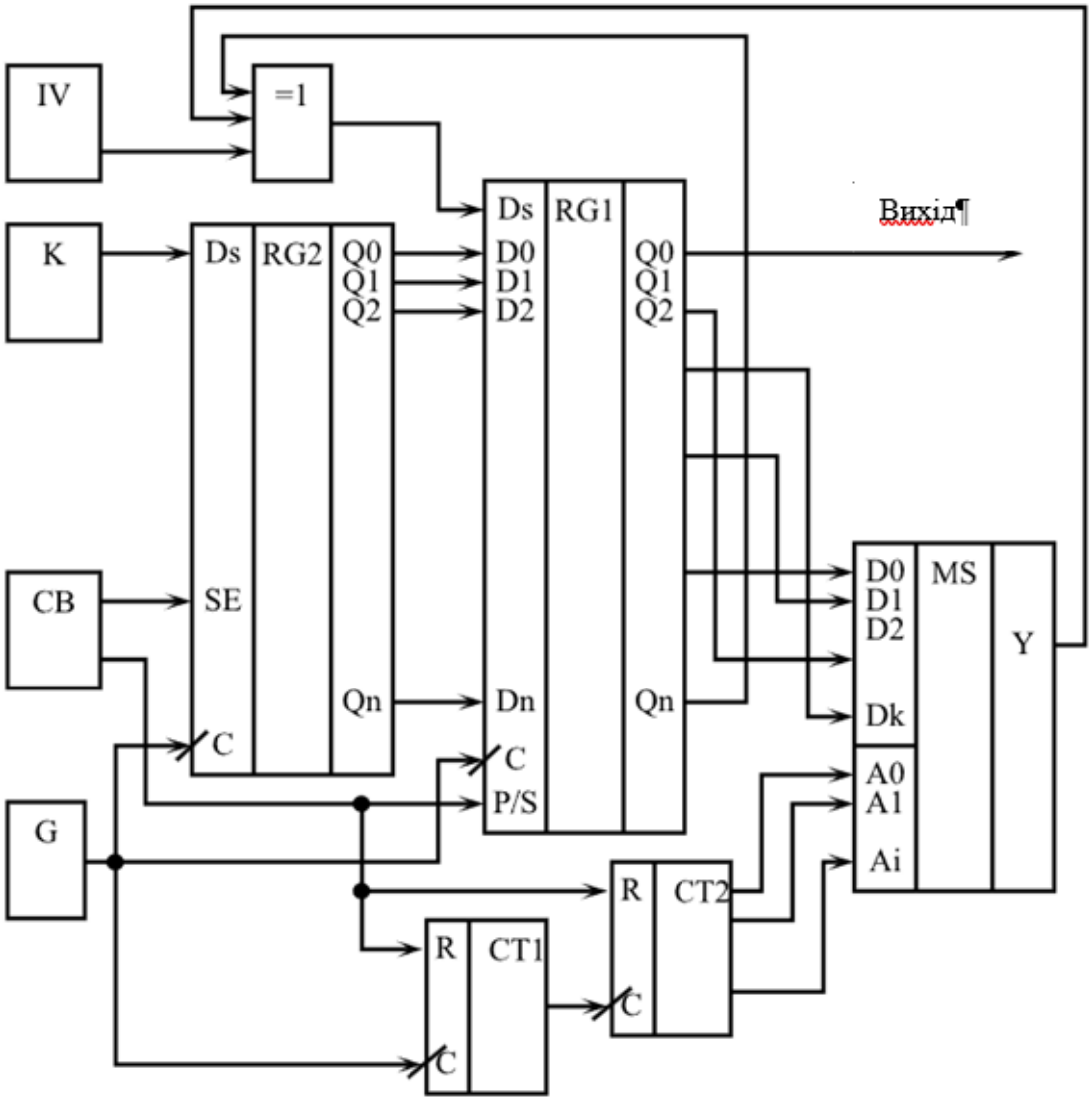

Рисунок 2.1 – Алгоритм потокового шифрування «AUGUST-1»

Довжина секретного ключа Кс у бітах визначає криптостійкість алгоритму потокового шифрування і дорівнює розрядності «*n*» регістра зсуву RG1. У разі використання сучасних програмованих логічних інтегральних схем (ПЛІС) розрядність регістра RG1 (і секретного ключа Кс) може становити від 100 до кількох тисяч біт.

До початку шифрування сформований секретний ключ Кс вводиться в

регістр RG2.

Після введення секретного ключа в регістр RG2 – цей ключ у паралельному форматі записується у регістр зсуву RG1. Для цього блок керування (СВ) формує логічний сигнал, який переводить перший регістр RG1 у режим паралельного завантаження, а також утримує в нульовому стані перший і другий лічильники СТ1, СТ2.

Перед шифруванням у канал зв'язку передається випадкове значення ініціалізації IV (Initialisation Value, або синхропосилка). Це значення ініціалізації не є секретним і передається відкритим каналом зв'язку перед кожним сеансом шифрування. Використання для всіх повідомлень окремих випадкових значень ініціалізації IV дає змогу формувати різні значення псевдовипадкової гамуючої послідовності для кожного нового повідомлення. При цьому навіть однакові початкові тексти повідомлень будуть зашифровані по-різному.

Одночасно з передачею в канал зв'язку значення ініціалізації IV воно також у послідовному форматі вводиться в регістр зсуву RG1 через третій вхід елемента «ВИКЛЮЧНЕ АБО» (елемента «XOR»). На перший і другий входи цього елемента «XOR» подаються сигнали з останнього виходу послідовного регістра RG1 і виходу мультиплексора MS для формування рекурентної псевдовипадкової послідовності гами.

Для зміни параметрів рекуренти регістра зсуву RG1 логічні рівні з його проміжних виходів «m_k» подаються на інформаційні входи мультиплексора MS, а адресні входи цього мультиплексора під'єднані до виходів другого лічильника СТ2.

Вихідна псевдовипадкова послідовність гами, яка може зніматися з будь-якого виходу першого регістра зсуву RG1, є детермінованою (тобто може бути повністю відновлена на приймальному боці каналу зв'язку) і залежить від секретного значення короткочасного (сеансового) ключа Кс, від випадкового значення ініціалізації IV та довготривалих секретних параметрів (довготривалих ключів):

довжини короткочасного (сеансового) секретного ключа «*n*», розміру і вмісту матриці комутації мультиплексора MS і коефіцієнта ділення першого лічильника СТ1.

Робота генератора гаммуючої послідовності за динамічної зміни параметрів рекурренти не може бути описана системою лінійних рівнянь. Тому криптоаналітику необхідно буде провести повний перебір усіх значень секретних довготривалих параметрів і для кожного значення цих параметрів провести лобову атаку з перебору всіх короткочасних (сеансових) ключів Кс, що робить процес дешифрування в розумні терміни – фізично неможливим.

2.2 Алгоритм потокового шифрування «AUGUST-2»

В алгоритмі формування гамуючої послідовності для потокового шифрування «AUGUST-2» [4,5,10] на основі ДЛРР для збільшення криптостійкості гамуючої послідовності запропоновано змінювати величини інтервалів часу між змінами параметрів рекуренти в псевдовипадковому порядку (рисунок 2.2).

Ці часові інтервали задаються дільником СТ1 з програмованим коефіцієнтом ділення (ДПКД), інформаційні входи якого підключені в випадковому порядку до відводів регістра зсуву ЛРР. Тому величини часових інтервалів будуть залежати від початкового значення сеансового ключа Кс, значення ініціалізації IV і поточного стану регістру.

Ще однією перевагою алгоритму «AUGUST-2» є введення другого вихідного елемента «ВИКЛЮЧНЕ АБО» (елемента «XOR»), входи якого підключені у довільному порядку до відводів регістра зсуву ЛРР. Обов’язковою умовою є максимально велика відстань між між відводами регістру зсуву. З виходу цього елемента «ВИКЛЮЧНЕ АБО» знімається псевдовипадкова гамуюча послідовність. Це покращує статистичні властивості формованої гами, а саме: зменшує різницю ймовірностей «нулів» і «одиниць» вихідної послідовності, а також зменшує нормовані коефіцієнти

автокореляційної функції [7].

У цьому алгоритмі додано нові секретні довготривалі параметри:

- діапазон зміни коефіцієнта ділення лічильника ДПКД та номери відводів регістру RG1, які підключені до інформаційних входів ДПКД.

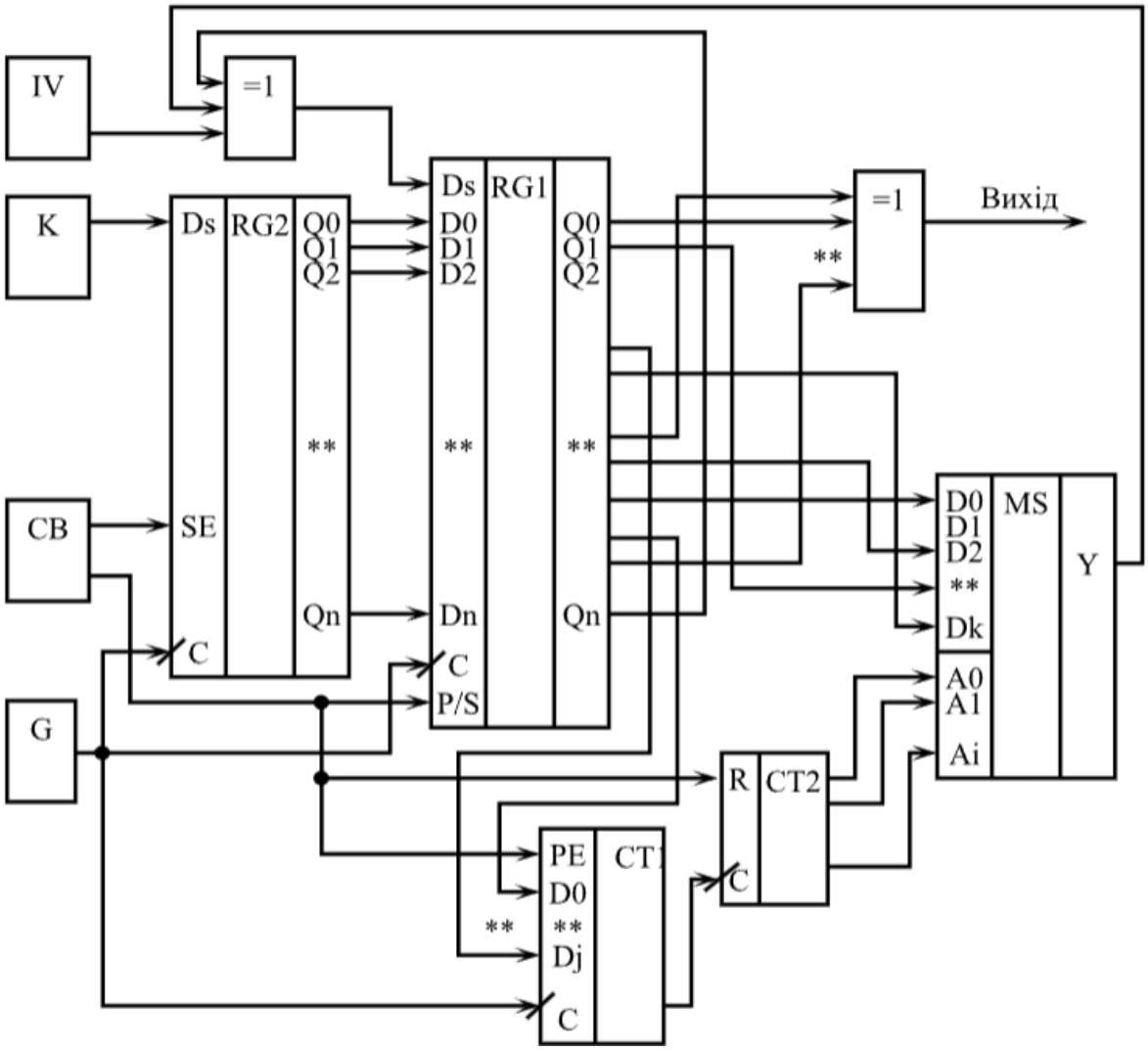

Рисунок 2.2 – Алгоритм потокового шифрування «AUGUST-2»

2.3 Алгоритм потокового шифрування «AUGUST-3»

В алгоритмі потокового шифрування «AUGUST-3» [4,5,11] для збільшення криптостійкості генератора гамуючої послідовності на основі ДЛРР запропоновано змінювати параметри рекуренти в псевдовипадковому порядку (рисунок 2.3). Для цього на адресні входи мультиплексора MS

подаються сигнали з виходу додаткового паралельного регістра RG3, у якому через фіксовані інтервали часу зберігаються коди з довільних виходів регістра зсуву ЛРР.

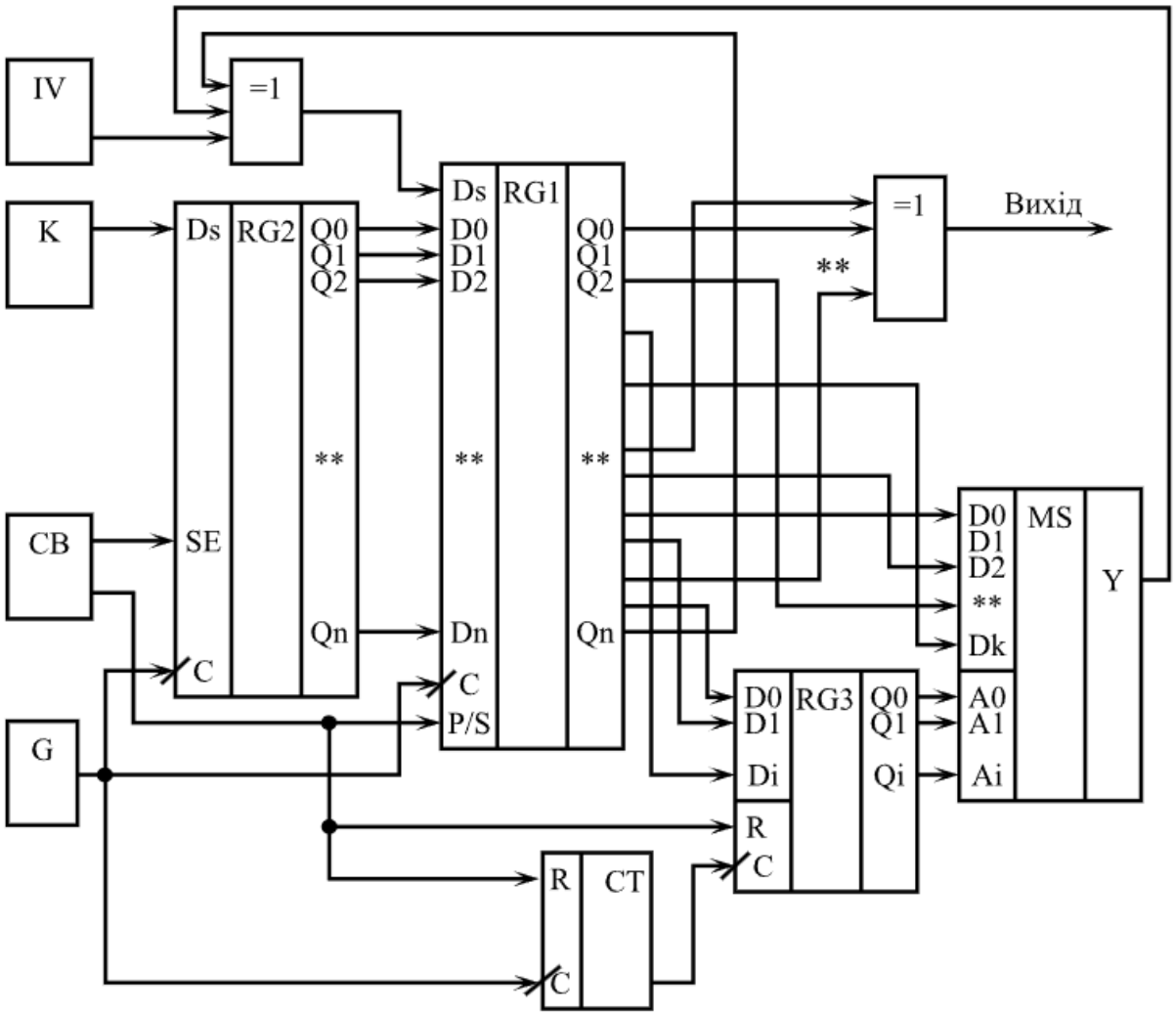

Рисунок 2.3 – Алгоритм потокового шифрування «AUGUST-3»

Таке технічне рішення ще більше ускладнює криптоаналіз, здійснити який (навіть без цих нововведень) у розумні терміни – фізично неможливо.

2.4 Алгоритм потокового шифрування «AUGUST-4»

В алгоритмі потокового шифрування «AUGUST-4» (рисунок 2.4) [6,12] для збільшення криптостійкості генератора гамуючої послідовності на основі ДЛРР об’єднані переваги алгоритмів «AUGUST-2» і «AUGUST-3».

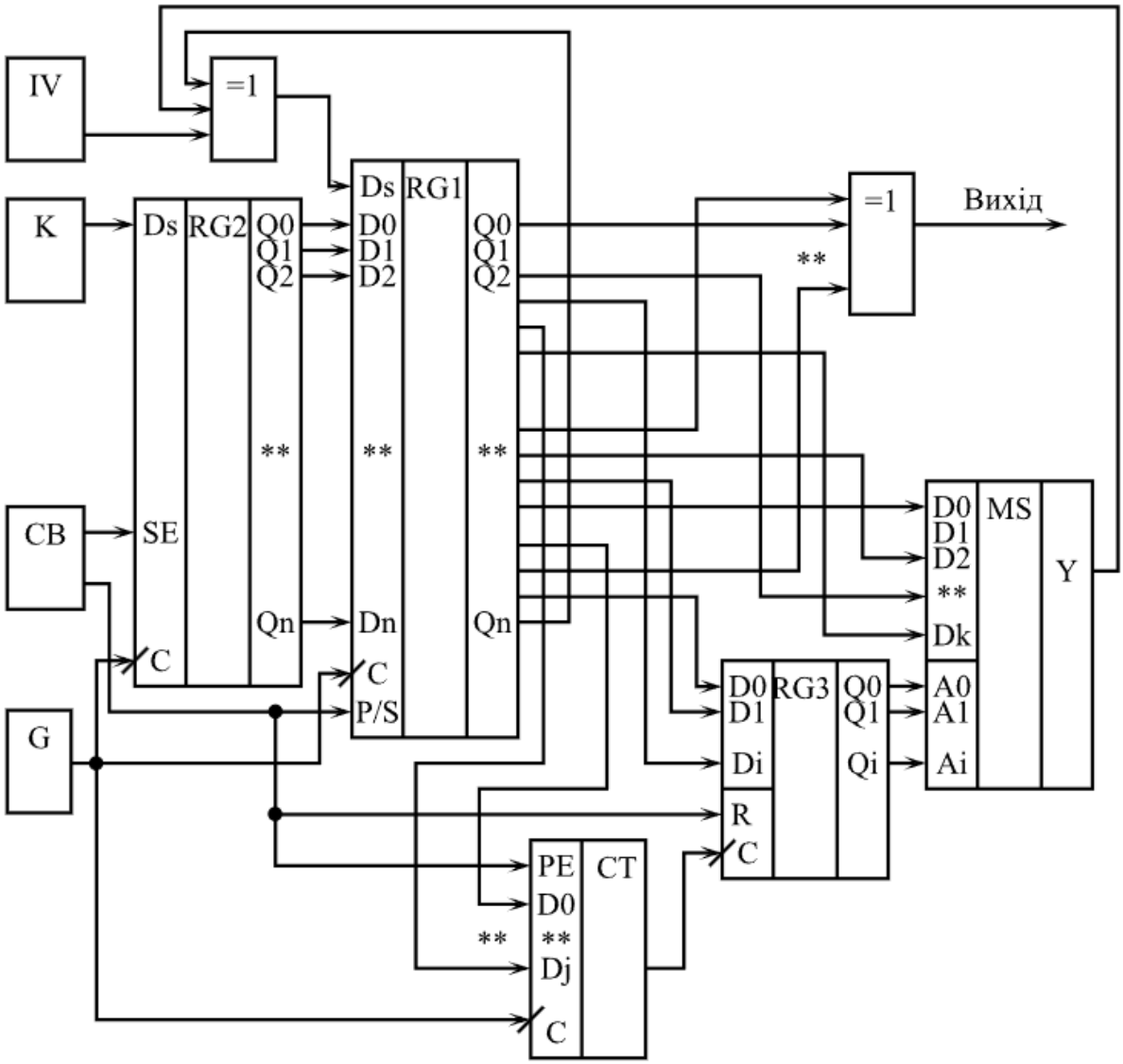

Рисунок 2.4 – Алгоритм потокового шифрування «AUGUST-4»

Параметри рекуренти (номери відводів «m_k») ДЛРР на основі регістру зсуву RG1 змінюються у псевдовипадковому порядку (як у алгоритмі «AUGUST-3»).

Для цього на адресні входи мультиплексора MS подаються логічні рівні з виходів додаткового паралельного регістру RG3, який запам’ятовує

псевдовипадкові коди з довільних виходів регістра зсуву ЛРР (RG1).

Псевдовипадкові часові інтервали між змінами параметрів рекуренти задаються дільником СТ з програмованим коефіцієнтом ділення (ДПКД) (як у алгоритмі «AUGUST-2»).

Це дає змогу реалізувати один із критеріїв Райнера Рюппеля: «Кожен біт гамуючої послідовності має бути складним перетворенням більшості бітів ключа».

2.5 Алгоритм потокового шифрування «AUGUST-5»

В алгоритмі потокового шифрування «AUGUST-5» (рисунок 2.5) [6,13] для збільшення криптостійкості генератора гамуючої послідовності на основі ДЛРР введено кілька мультиплексорів (MS-1…MS-n), що змінюють параметри рекуренти. Наприклад, один мультиплексор комутує відводи рекурентного регістру зсуву RG1, які визначають довжину ДЛРР «n», а інші мультиплексори змінюють номери відводів регістра зсуву ДЛРР «m_k».

Можлива також ситуація, при якій, відведення регістру зсуву RG1, що визначає довжину ДЛРР «n» на виході конкретного мультиплексора, в наступному такті може стати проміжним відведенням «m_k», а довжина ДЛРР формується іншим мультиплексором.

На (рисунок 2.5) наведено випадок, коли номери відводів ДЛРР комутуються в постійному порядку і через фіксовані часові інтервали, які визначаються дільниками «СТ 1-1» і «СТ 1-n». Коефіцієнти ділення цих дільників обираються, як взаємно прості числа.

Також можливо введення другого вихідного елемента «ВИКЛЮЧНЕ АБО» (елемента «XOR») (як на рисунок 2.2, рисунок 2.3, рисунок 2.4), входи якого підключені у довільному порядку до відводів регістра зсуву ЛРР. З виходу цього елемента «ВИКЛЮЧНЕ АБО» знімається псевдовипадкова гамуюча послідовність. Це покращує статистичні властивості формованої гами, а саме: зменшує різність ймовірностей «нулів» і «одиниць» вихідної

послідовності, а також зменшує нормовані коефіцієнти автокореляційної функції [7].

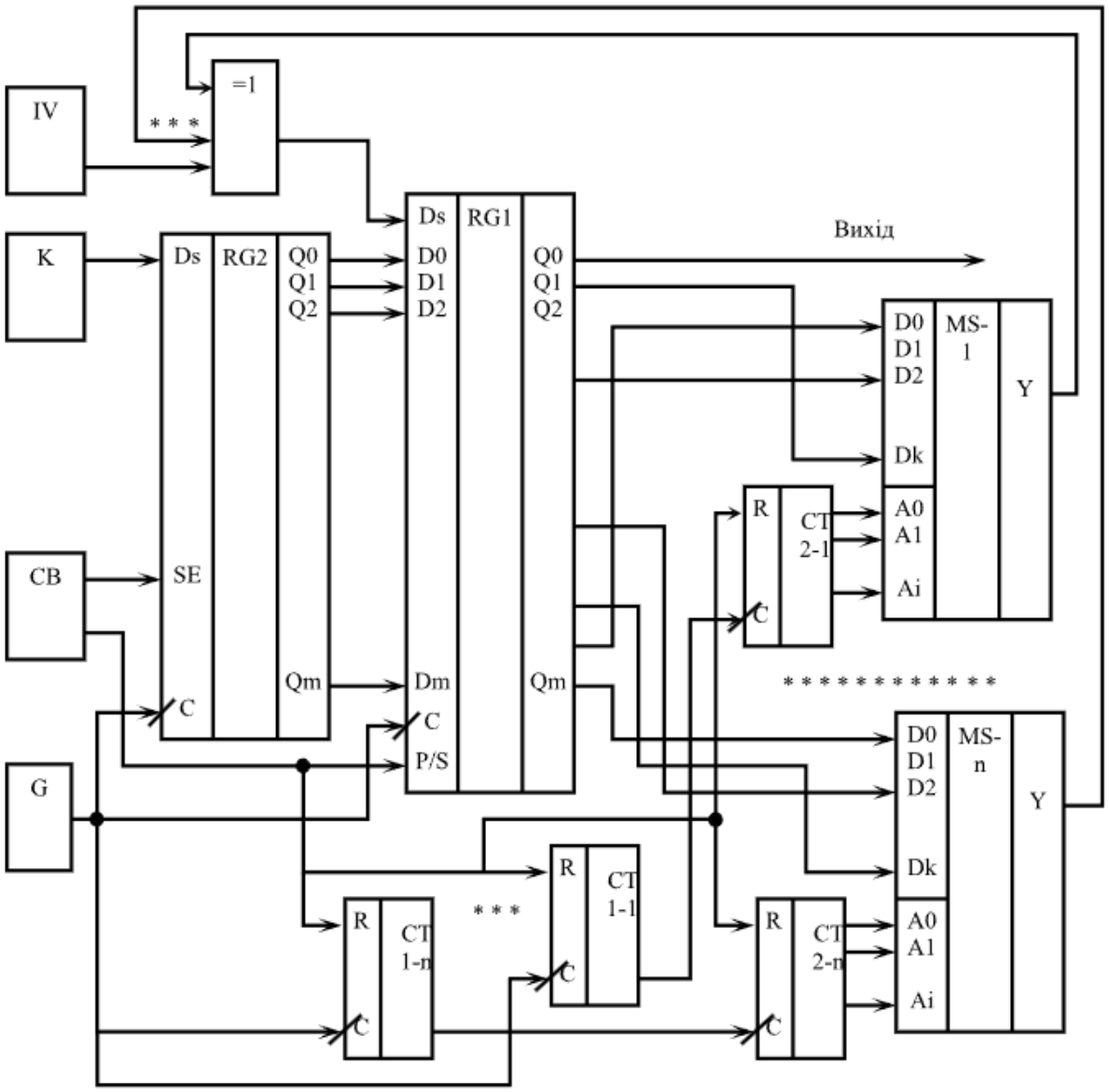

Рисунок 2.5 – Алгоритм потокового шифрування «AUGUST-5»

2.6 Алгоритм потокового шифрування «AUGUST-6»

В алгоритмі потокового шифрування «AUGUST-6» (рисунок 2.6) [14] порядок зміни параметрів рекуренти визначається реверсивним лічильником CT2, виходи якого під’єднані до адресних входів мультиплексора MS.

Інтервали зміни параметрів рекуренти визначаються дільником CT1, а інтервали перемикання реверсивного лічильника CT2 в режими U/D (вгору/вниз) – лічильником CT3. Коефіцієнти ділення лічильників CT1 і CT3 обираються, як взаємно прості числа.

Такий псевдовипадковий порядок зміни параметрів рекуренти підвищує криптостійкість алгоритму «AUGUST-6».

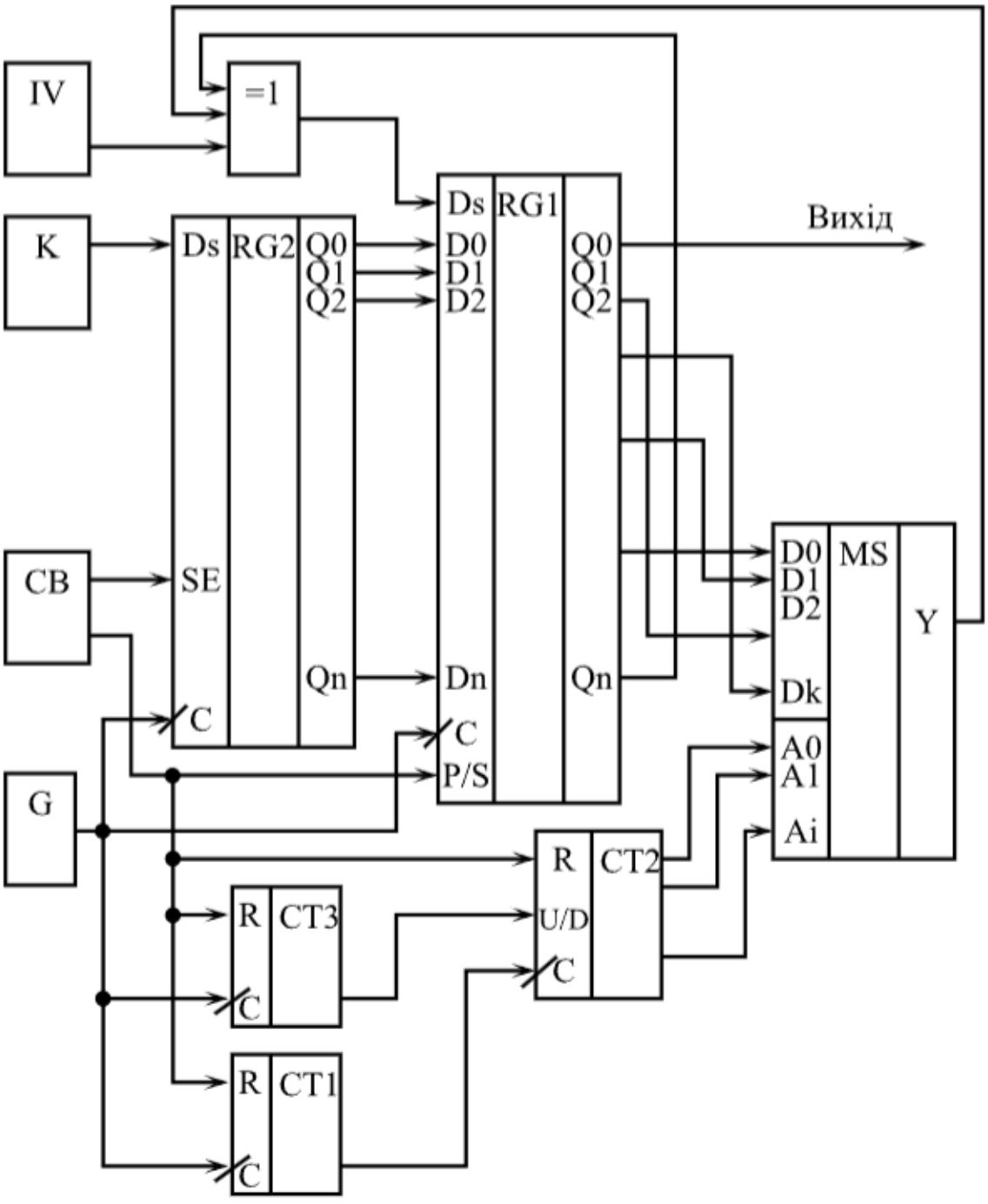

Рисунок 2.6 – Алгоритм потокового шифрування «AUGUST-6»

3 АНАЛІЗ КРИПТОСТІЙКОСТІ ПОТОКОВИХ ШИФРІВ ПРИ ЗМІНІ ПАРАМЕТРІВ РЕКУРЕНТИ

3.1 Визначення криптостійкості

Криптографічне перетворення інформації – це перетворення інформації з метою приховування або відновлення її змісту, підтвердження її автентичності, цілісності, авторства, захисту від несанкціонованого доступу до інформації та ресурсів тощо, яке здійснюється з використанням спеціальних (ключових) даних.

Ще в 19-му столітті голландець А. Керкгоффс сформулював головну вимогу до криптографічних систем, яка залишається актуальною і понині, – принцип Керкгоффса: секретність шифрів повинна бути заснована на секретності ключа, але не алгоритму. Шеннон сформулював цей принцип (ймовірно, незалежно від Керкгоффса) наступним чином: «Ворог знає систему».

Принцип Керкгоффса спрямований на те, щоб зробити безпеку алгоритмів і протоколів незалежною від їх секретності; відкритість не повинна впливати на безпеку.

Більшість широко використовуваних систем шифрування, відповідно до принципу Керкгоффса, використовують відомі, не секретні криптографічні алгоритми. З іншого боку, шифри, використовувані в урядовому і військовому зв'язку, як правило, засекречені (обов’язковою умовою є – вітчизняні розробки криптоалгоритмів з метою усунення «заклкдок»); таким чином створюється «додатковий рубіж оборони».

Вимоги до криптосистеми вперше викладені в книзі Керкгоффса «Військова криптографія» – Auguste Kerckhoffs, «La Cryptographie Militaire» (видана в 1883 році). Шість основних вимог до криптосистеми, всі з яких до теперішнього часу визначають проектування криптографічно стійких систем, в перекладі з французької звучать так:

1 система повинна бути фізично, якщо не математично, неприхованою;

2 потрібно, щоб не було потрібно збереження системи в таємниці; потрапляння системи в руки ворога не повинно завдавати незручностей;

3 зберігання і передача ключа повинні бути здійсненні без допомоги паперових записів; кореспонденти повинні мати можливість змінювати ключ на свій розсуд;

4 система повинна бути придатною для повідомлення через телеграф;

5 система повинна бути легко переноситься, робота з нею не повинна вимагати участі декількох осіб одночасно;

6 нарешті, від системи вимагається, враховуючи можливі обставини її застосування, щоб вона була проста у використанні, не вимагала значної розумової напруги або дотримання великої кількості правил.

Друга з цих вимог і стала відома як «принцип Керкгоффса».

Також важливим, вперше строго сформульованим висновком «Військової криптографії» є твердження про криптоаналіз, що лобова атака з перебору усіх ключів є єдиним вірним способом випробування шифрів.

Секретний ключ є тимчасовим (змінним) параметром шифру і може бути легко замінений без зміни криптостійкості алгоритму.

Головною дійовою особою в криптоаналізі виступає порушник (зловмисник, дешифрувальник або криптоаналітик). Під ним розуміють особу (групу осіб), метою яких є прочитання або підробка захищених криптографічними методами повідомлень.

Відносно порушника приймається ряд припущень, які, як правило, кладуться в основу математичних або інших моделей:

1 порушник (дешифрувальник) знає алгоритм шифрування (або вироблення ЕЦП) і особливості його реалізації в конкретному випадку, але не знає секретного ключа.

2 порушнику доступні всі зашифровані тексти. Порушник може мати доступ до деяких вихідних текстів, для яких відомі відповідні їм зашифровані тексти.

3 порушник має в своєму розпорядженні обчислювальні, людські, часові та інші ресурси, обсяг яких виправданий потенційною цінністю інформації, яка буде здобута в результаті криптоаналізу.

Спробу прочитання або підробки зашифрованого повідомлення, обчислення ключа методами криптоаналізу називають криптоатакою або атакою на шифр. Вдалу криптоатаку називають зломом.

Криптостійкістю називається характеристика шифру, що визначає його стійкість до дешифрування без знання ключа (тобто криптоатаки). Показник криптостійкості - головний параметр будь-якої криптосистеми. В якості показника криптостійкості можливо обрати:

- кількість всіх можливих ключів або ймовірність підбору ключа за заданий час із заданими ресурсами;
- кількість операцій або час (із заданими ресурсами), необхідний для злому шифру із заданою ймовірністю;
- вартість обчислення ключової інформації або вихідного тексту.

Однак слід розуміти, що ефективність захисту інформації криптографічними методами залежить не тільки від криптостійкості шифру, але і від безлічі інших факторів, включаючи питання реалізації криптосистем у вигляді пристроїв або програм. При аналізі криптостійкості шифру необхідно враховувати і людський фактор. Наприклад, підкуп конкретної людини, в руках якого зосереджена необхідна інформація, може коштувати на декілька порядків дешевше, ніж створення суперкомп'ютера для злому шифру.

Сучасний криптоаналіз спирається на такі математичні науки як теорія ймовірностей і математична статистика, алгебра, теорія чисел, теорія алгоритмів і ряд інших. Всі методи криптоаналізу в цілому укладаються в чотири напрямки.

1 Статистичний криптоаналіз досліджує можливості злому крипто-систем на основі вивчення статистичних закономірностей вихідних і зашифрованих повідомлень. Його застосування ускладнене тим, що в

реальних крипто-системах інформація перед шифруванням піддається стисненню (перетворюючи вихідний текст у випадкову послідовність символів), або у випадку гамування використовуються псевдовипадкові послідовності великої довжини.

2 Алгебраїчний криптоаналіз займається пошуком математично слабких ланок криптоалгоритмів. Наприклад в 1997 році в системах на основі еліптичних кривих був виявлений клас ключів, які істотно упрощали криптоаналіз.

3 Диференціальний (або різницевий) криптоаналіз заснований на аналізі залежності зміни шифрованого тексту від змін вихідного тексту. Вперше використаний Мерфі, поліпшений Біхемом і Шаміром для атаки на DES.

4 Лінійний криптоаналіз заснований на пошуку лінійної апроксимації між вихідним і шифрованим текстом. Запропонований Мацуї, також був застосований при зломі DES. Як і диференціальний аналіз в реальних криптосистемах може бути застосований тільки для аналізу окремих блоків криптоперетворень.

Досвід зломів криптосистем (зокрема, конкурсів, які регулярно влаштовує RSA Data Security) показує, що головним методом залишається «лобова» атака – проба на ключ.

Прийнято розрізняти кілька рівнів криптоатаки залежно від обсягу інформації, доступної криптоаналітику. Можливо виділити три рівня криптоатаки з наростання складності.

1 Атака по шифрованому тексту (Рівень КА1). Порушнику доступні всі або деякі зашифровані повідомлення.

2 Атака по парі «вихідний текст - шифрований текст». (Рівень КА2). Порушнику доступні всі або деякі зашифровані повідомлення і відповідні їм вихідні повідомлення.

3 Атака по вибраній парі «вихідний текст - шифрований текст». (Рівень КА3). Порушник має можливість вибирати вихідний текст, отримувати для

нього шифрований текст і на основі аналізу залежностей між ними обчислювати ключ.

Всі сучасні криптосистеми мають достатню стійкість навіть до атак рівня КАЗ, тобто коли порушнику доступний по суті шифруючий пристрій.

Найбільш ефективним в економічному плані може стати, так званий, «бандитський криптоаналіз». Криптоаналітик може використовувати «людський фактор», тобто намагатися за допомогою шантажу, підкупу, тортур або інших засобів отримати інформацію про систему шифрування або навіть сам ключ шифрування. Таким чином, методика розкриття побудована на слабкості людей як складової частини системи захисту інформації.

3.2 Аналіз криптостійкості потокових алгоритмів сімейства «AUGUST»

Атака по вибраній парі «вихідний (початковий) текст - шифрований текст». (рівень КАЗ або рівень КА2). Порушник має можливість обирати вихідний текст, отримувати для нього шифрований текст і на основі аналізу залежностей між ними обчислювати ключ.

Наявність початкового тексту і відповідного йому шифротексту дозволяє відновити гамуючу послідовність (в двох варіантах: при використані операції «ВИКЛЮЧНЕ АБО без інверсії», чи оперції «ВИКЛЮЧНЕ АБО з інверсією»).

Якщо відомо, що гамуюча послідовність формується ЛРР фіксованої довжини «n», то можливо відновити параметри ЛРР і початковий стан ЛРР (тобто одноразовий ключ), аналізуючи $2n$ псевдовипадкових бітів за допомогою алгоритму Берлекемпа-Мессі.

Сама процедура займає небагато часу, але довжина «n» може бути в діапазоні від десятків до сотень розрядів. Для кожної довжини ЛРР треба проводити нову «атаку на ключ».

Навіть успішна атака на ключ – не має значного сенсу, тому що зламаний ключ (при відомому початковому тексті і відомому шифротексті)

зазвичай є одноразовим і в новому повідомлені буде згенеровано інший ключ.

Атака по шифрованому тексту (Рівень КА1) і невідомому початковому тексті, якщо відомо, що гамуюча послідовність формується ЛРР фіксованої довжини «*n*», вимагає проводити перебір усіх значень ключа для усіх припустимих довжинах ЛРР від десятків до сотень розрядів. Така атака при довжині ключа більше 70 біт займає мільярди років (згідно з таблицею 1.1), що є неприпустимим.

Використання комп'ютерних серверів з тисячами багатоядерних процесорів дозволить скоротити час криптоатаки до тисяч років, що також є неприпустимим.

Атака по вибраній парі «вихідний (початковий) текст - шифрований текст». (рівень КАЗ або рівень КА2) при використанні криптоалгоритмів на основі ДЛРР значно збільшує час криптоатаки (в порівнянні з криптоалгоритмами на основі ЛРР).

Атака по шифрованому тексту (Рівень КА1) і невідомому вихідному (початковому) тексті при використанні криптоалгоритмів на основі ДЛРР (з невідомими довготривалими параметрами-ключами) неможлива у розумні терміни навіть з використанням квантових багатокубітових комп'ютерів. Такі криптоалгоритми наближаються за криптостійкістю до теоретично незламного шифру з «відривним блокнотом», коли довжина одноразового ключа дорівнює довжині всього тексту.

На відміну від відомих «класичних» криптоалгоритмів AES, A5 та інших, у яких відомі не тільки алгоритми (перелік операцій), а й усі параметри алгоритму, а невідомим є тільки короткочасний ключ, у алгоритмів на основі ДЛРР є дуже багато секретних довготривалих параметрів-ключів, повний перебір яких займає мільярди років.

ВИСНОВКИ

Забезпечення безпеки інформації, яка передається між сторонами інформаційного обміну, стає надзвичайно важливим завданням для державних та комерційних структур. Криптографія, яка вивчає методи захисту інформації від несанкціонованого доступу, використовує різноманітні криптоалгоритми для шифрування та розшифрування даних. Криптоалгоритми визначаються як математичні процедури, що виконують перетворення даних з одного вигляду в інший з метою захисту конфіденційності та цілісності інформації.

Більшість існуючих симетричних шифрів однозначно можуть бути віднесені або до потокових (ПШ), або до блочних шифрів (БШ). Але теоретична межа між ними є досить розмитою. Наприклад, алгоритми блокового шифрування часто використовуються в режимі потокового шифрування.

Найважливішою перевагою потокових шифрів перед блочними є висока швидкість шифрування, яка співпадає зі швидкістю надходження вхідної відкритої інформації, що дозволяє шифрувати аудіо- або відеопотоки в реальному масштабі часу.

Запропоновані і запатентовані в Україні швидкодіючі детерміновані генератори псевдовипадкових гамуючих послідовностей для потокового шифрування «AUGUST-1» … «AUGUST-6» дають змогу усунути більшість недоліків відомого алгоритму А5, який використовує лінійні рекурентні регістри (ЛРР) для формування гамуючої псевдовипадкової послідовності, а також для управління синхросгналом. Криптостійкість алгоритму А5 не відповідає сучасним вимогам з огляду на недостатню довжину ключа, а також відомі атаки на цей алгоритм, які дозволяють розкривати зміст повідомлень в розумні терміни

Криптостійкість запропонованих алгоритмів формування гамуючої псевдовипадкової послідовності для потокового шифрування визначається

розрядністю ДЛЛР (довжиною короткочасного секретного ключа Кс), що може становити від 100 до кількох тисяч біт. Тому час на проведення лобової атаки з перебору всіх короткочасних ключів у мільярди разів перевищує вік Всесвіту [7]. Причому секретним є не тільки значення ключа Кс, а й його довжина.

Запропоновані алгоритми «AUGUST-1» … «AUGUST-6» руйнують лінійні властивості ЛРР і тим самим роблять такі системи криптографічно більш стійкими за рахунок динамічної зміни параметрів рекурренти в процесі формування псевдовипадкової гамуючої послідовності.

На відміну від відомих криптоалгоритмів (DES, AES, A5 та ін.), у яких повністю відомий математичний апарат криптоперетворень, а невідомим є тільки єдиний секретний параметр – короткочасний сеансовий ключ, у запропонованих алгоритмах на основі ДЛРР присутня дуже велика кількість довготривалих секретних параметрів (повний перебір яких може зайняти мільярди років).

Тому криптоаналіз таких алгоритмів із перебором усіх довготривалих секретних параметрів і значень секретного короткочасного (сеансового) ключа є фізично неможливим у розумні терміни.

Такі криптоалгоритми на основі ДЛРР наближаються за криптостійкістю до теоретично незламного шифру з «відривним блокнотом», коли довжина одноразового ключа дорівнює довжині всього тексту.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Менезис А., Руководство по прикладной криптографии // [Текст]. А. Менезис, П. ван Оршоа, С. Ватсон – CRC: Press, 1996. – 816с.

2. Хоровиц П. Искусство схемотехники: в 3-х томах; пер. с англ. [4-е изд.]. // [Текст]. П. Хоровиц, У. Хилл – М.: Мир, 2003.

3. Торба А.А. Аналоговая и цифровая электроника [учебное пособие]. // [Текст]. А.А. Торба, А.А. Торба – Харьков: Смит, 2016.– 404 с.

4. Торба А.А. Быстродействующий детерминированный генератор псевдослучайных последовательностей для потокового шифрования // [Текст]. А.А. Торба, В.А. Бобух, А.А. Бобкова. – Прикладная радиоэлектроника: научн.-техн. журнал. – 2014.– Том 13.– №3.– с. 316-318.

5. Торба А.А. Методы повышения криптостойкости алгоритмов потокового шифрования // [Текст]. А.А. Торба, В.А. Бобух, М.О.Торба, А.О.Торба.– // Радиотехника : Всеукр. межвед. науч.-техн. сб. – 2016. – Вып. 184. – С. 178 – 183.

6. Торба А.А. Детерминированные генераторы псевдослучайных последовательностей для потокового шифрования на основе ДЛРР // [Текст]. А.А. Торба, В.А. Бобух, М.О.Торба, А.О.Торба – Прикладная радиоэлектроника: научн.-техн. журнал. – 2016.– Том 15.– №3.– с. 191-194.

7. Торба А.А. Методы и средства генерации случайных битовых последовательностей // [Текст]. А.А. Торба, А.А. Бобкова, Ю.И. Горбенко, В.А. Бобух.– Под ред. д.т.н., профессора Горбенко И.Д. – Харьков: Изд-во «Форт», 2012.– 232 с. ISBN 978-617-630-000-7.

8. URL: http://ru.wikipedia.org/wiki/A5.

9. Патент України на корисну модель № 85039, опубл. Бюл. № 21, 2013 г.

10. Патент України на корисну модель № 93477, опубл. Бюл. № 19, 2014 г.

11. Патент України на корисну модель № 93117, опубл. Бюл. № 18, 2014 г.

12. Патент України на корисну модель № 99194, опубл. Бюл. № 10, 2015 р.

13. Патент України на корисну модель № 97734, опубл. Бюл. № 7, 2015 р.

14. Патент України на корисну модель № 109675, опубл. Бюл. № 16, 2016 р.

15. Торба А. Алгоритми потокового шифрування // [Текст]. – А. Торба, Ю. Мегель, М. Науменко – POLISH SCIENCE JOURNAL.– Warsaw: Sp. z o. o. "iScience", 2023. ISSUE 10(66), – S. 61…71.