Вінницький національний технічний університет
Факультет інформаційних технологій та комп'ютерної інженерії
Кафедра обчислювальної техніки

БАКАЛАВРСЬКА ДИПЛОМНА РОБОТА

на тему:

Цифрові скремблери на основі лінійних автоматів

ПОЯСНЮВАЛЬНА ЗАПИСКА

Виконав студент 4 курсу, групи 2КІ-18б
спеціальності 123 — Комп'ютерна інженерія
Салата О. Л.

Керівник к.т.н., доц. каф. ОТ
Семеренко В.П.

Рецензент д.т.н., проф. каф. ЗІ
Карпінець В.В.

Допущено до захисту
д.т.н., проф. Азаров О.Д.

"23" червня 2022 р.

ВНТУ 2022

Вінницький національний технічний університет

Факультет інформаційних технологій та комп'ютерної інженерії

Кафедра обчислювальної техніки

Освітньо-кваліфікаційний рівень бакалавр

Спеціальність 123 — «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри

обчислювальної техніки

проф. Азаров О.Д.

«08» 02 2022 р.

З А В Д А Н Н Я

НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Салаті Олександру Леонідовичу

1 Тема проекту «Цифрові скремблери на основі лінійних автоматів», керівник роботи к.т.н., доц. каф. ОТ Семеренко В. П. затверджені наказом вищого навчального закладу від «24» березня 2022 року № 66

2 Строк подання студентом проекту 22.06. 2022 р.

3 Вихідні дані до проекту: призначення — цифрові скремблери; основні підтримувані функції — автоматне скремблювання; використовувані сторонні ресурси — автоматне дескремблювання.

4 Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): вступ, основні поняття, реалізація автоматного скремблювання та дескремблювання.

5 Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень).

6 Консультанти розділів роботи приведено в таблиці 1.

7 Дата видачі завдання « 24 » березня 2022 р.

3

8 Календарний план виконання БДР приведений в таблиці 2.

Таблиця 1 — Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		Завдання видав	Завдання прийняв
Спеціальна частина	Семеренко В. П. доцент кафедри ОТ		

Таблиця 2 — Календарний план

№ з/п	Назва етапів виконання комплексної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	09.03.22	вик.
2	Аналіз предметної області	10.03-18.03.22	вик.
3	Аналіз характеристик скремблювання	21.03-31.03.22	вик.
4	Аналіз завадостійкості кодування в МЗ	05.04-13.04.22	вик.
5	Огляд математичних апаратів лінійних автоматів	14.04-22.04.22	вик.
6	Програмно-апаратна реалізація скремблерів	25.04-.06.05.22	вик.
7	Програмна реалізація скремблерів	09.05-13.05.22	вик.
8	Апаратна реалізація скремблерів	17.05-22.05.22	вик.
9	Підготовка матеріалів та опис розробки інформаційної системи	23.05-26.05.22	вик.
10	Аналіз виконання роботи, висновки, додатки	27.05-31.05.22	вик.
11	Перевірка якості виконання бакалаврського проекту та усунення недоліків	02.06 -17.06.22	вик.

Студент _____ Салата О. Л.

Керівник роботи _____ Семеренко В. П.

СПИСОК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

ЕОМ — електронно-обчислювальна машина

ПП – програмний продукт

ПЗ – програмне забезпечення

ПВБП – псевдовипадкові бінарні послідовності

ЗКЗІ – засоби криптографічного захисту інформації

ГПВЧ - генератори псевдовипадкових чисел

АНОТАЦІЯ

Пояснювальна записка викладена на 50 сторінках та включає 10 ілюстрацій та 11 джерел за переліком посилань.

Метою роботи є всебічний аналіз застосування моделей цифрових скремблерів на основі лінійних автоматів.

В даній роботі розглядаються різновиди технологій шифрування сигналу, зокрема скремблювання та дескремблювання. Визначаються їхні переваги та недоліки, область застосування. Розглядаються технічні методи, що застосовуються в скремлюванні. Приведені варіанти програмних рішень для скремлювання та розглянуті апаратні моделі скремблерів.

Ключові слова: скремблер, лінійний автомат, скремблювання, дескремблювання.

ABSTRACT

The 50-page explanatory note includes 10 illustrations and 11 reference sources.

The aim of the work is a comprehensive analysis of the application of digital scrambler models and the construction of linear automata based on them.

This paper considers the types of signal encryption technologies, in particular scrambling and descramming. Their advantages and disadvantages, scope are determined. The technical methods used in scrambling are considered. Variants of software solutions for scrambling are given and hardware models of scramblers are considered.

Keywords: scrambler, linear automaton, scrambling, descramming.

ЗМІСТ

ВСТУП

Актуальність обраної теми є розвитком систем зв’язку з якої витікає проблема захисту інформації від різних ризиків, а також проблема діагностування цифрової апаратури. Це не тільки захист від доступу сторонніх осіб, а також від помилок. В цих сферах знайшли своє місце і широко використовуються генератори псевдовипадкових послідовностей такі як цифрові скремблери на основі лінійних автоматів. Такі скремблери використовуються в великій кількості в різноманітних захищених телекомунікаційних систем.

Не можна також забувати про діагностування цифрових схем у складі великих комплексів, де лінійні цифрові фільтри дозволяють будувати прості і надзвичайно компактні пристрої для ефективного і швидкого знаходження несправностей.

Об’єктом дослідження є процеси оптимізації застосування лінійних автоматів, зокрема в скремблерах.

Предметом дослідження є структурні схеми побудови лінійних цифрових скремблерів.

Метою роботи є всебічний аналіз застосування моделей цифрових скремблерів на основі лінійних автоматів.

Для досягнення поставленої мети необхідно вирішити задачі:

— докладне ознайомлення з функціями регістрів зсуву зі зворотними зв’язками та їх можливостями;

— дослідження основних сфер застосування ПВБП;

— дослідження основних засобів діагностування несправностей в цифрових системах та участю лінійних цифрових фільтрів в них;

— дослідження принципів побудови генераторів псевдовипадкових послідовностей на регістрах зсуву зі зворотнім зв’язком по модулю два, методи підбору поліномів для них та перспектив розширення можливостей таких генераторів;

— визначення основних можливостей таких фільтрів для систем шифрування інформації;

— аналіз вимог до ПВБП, генераторів, тестів NIST.

Методи дослідження, що використовується для виконання поставлених задач, є порівняння різних принципів побудови цифрових скремблерів на основі лінійних автоматів на основі літературних джерел з даної тематики та їх аналіз.

1 ОСНОВНІ ПОНЯТТЯ ЦИФРОВОГО СКРЕМБЛЮВАННЯ

1.1 Основні задачі цифрового скремблювання

Зазвичай, користувача найбільше цікавить питання, який скремблер забезпечить найбільший захист інформації. Слід сказати, що представлені аналогові скремблер не можуть забезпечити гарантовану стійкість інформації, тому їх не можна розглядати як засоби криптографічного захисту інформації (ЗКЗІ). Йдеться лише про утруднення прослуховування конкурентом або зловмисником переговорів, що ведуть за допомогою радіозасобів, оснащених скремблерами, у реальному масштабі часу. Як було зазначено, деяке уявлення про ступінь закриття інформації може дати кількість ключових параметрів і кількість ключів. Причому слід розглядати ці параметри в сукупності, при рівній кількості ключів перевагу мають скремблер з більшою кількістю ключових параметрів.

Проблемою симетричного шифрування є необхідність передачі ключа, для розшифрування інформації, таким чином ключ може бути перехоплений кимось іншим.

Будь-яку інформацію, зашифровану за допомогою відкритого ключа можна розшифрувати лише застосовуючи той самий алгоритм, але з використанням відповідного приватного ключа. Також всю інформацію, зашифровану за допомогою приватного ключа, можна розшифрувати лише за допомогою відповідного відкритого ключа. Це означає, що немає необхідності хвилюватись за передачу ключа, відкритий ключ повинен бути публічним. Але асиметричне шифрування є значно повільнішим від симетричного. Також потребує значно більше обчислювальної потужності як для шифрування, так і для розшифрування інформації. Розглянемо з цього погляду представлені види скремблерів.

У смугово—зсувних інверторах як основний ключовий параметр виступає частота розбиття смуги мовного сигналу Fp, розмірність якої зіставна з розмірністю ключового параметра частотного інвертора. Якщо частота розбиття є єдиним ключовим параметром, цей спосіб аналогового

скремблювання забезпечує закриття мовленнєвої інформації, порівнянне з частотною інверсією. Якщо можуть змінюватися і частоти інверсії в кожній зі смуг, число ключів, відповідно і рівень закриття інформації, збільшуються.

У смугових скремблерах ключовими параметрами системи є число частотних смуг та кодова комбінація їхньої перестановки. Реально кількість смуг не перевищує 4-х, тому число можливих комбінацій — 24 (одна з них не є перестановкою).

Скремблери з тимчасовими перестановками мають кілька ключових параметрів: тривалість сегмента промови, тривалість тимчасового відрізка та правило перестановки тимчасових відрізків у сегменті. Різні поєднання значень цих параметрів можуть дати можливість реалізації кількох сотень ключів.

Ролінгові скремблер надають можливість використання в мережі радіозв'язку такої кількості ключових комбінацій, яка може вимірюватися мільйонами або навіть мільярдами. У цьому рівень захисту визначається кількістю градацій параметра сигналу, довжиною ключа, т. е. числом можливих комбінацій параметра, швидкістю зміни параметра.

Однак підвищення ступеня закриття інформації набагато більшою мірою залежить від кількості градацій ключового параметра (наприклад, кількості частот інверсії сигналу), ніж від довжини послідовності їх перебору.

Слід зазначити, що при низькій швидкості зміни частоти інверсії (наприклад, 1 раз на секунду) ще зберігається можливість розуміння якоїсь частини інформації, що передається при її прослуховуванні за допомогою радіостанції, оснащеної скремблером з фіксованою частотою інверсії. Однак при збільшенні швидкості до 5—10 разів на секунду можливість такого розуміння різко знижується. Необхідність подальшого збільшення швидкості зміни параметра перетворення викликає певні сумніви.

Перехоплення повідомлень у реальному масштабі часу в каналах зв'язку, захищених за допомогою скремблерів з параметрами перетворення, що змінюються в часі, можливий при застосуванні спеціальних технічних засобів, що дозволяють спочатку визначити ключову послідовність (тобто правила

зміни параметрів перетворення сигналу), а потім підлаштуватися під виявлену ключову послідовність. Водночас це обладнання має бути значно складнішим порівняно із засобами перехоплення переговорів абонентів, радіостанції яких оснащені скремблерами з фіксованими параметрами.

У багатьох цифрових системах передачі використовують скремблер для рандомізації послідовностей цифрових сигналів в лініях. Хоча ці скремблер і аналогічні використовуваним для засекречування, їх основним завданням є запобігання передачі послідовностей, що повторюються, а не засекречування обміну. Повторювані послідовності створюють лінійний спектр сигналу, який призводить до більших спотворень, ніж безперервний спектр, що відповідає випадковій цифровій послідовності. Так, наприклад, можна допустити роботу модемів у каналах тональних частот з підвищеними рівнями потужності, якщо вони містять скремблер для рандомізації даних. Федеральна комісія зв'язку США також вимагає, щоб у цифрових радіосистемах не передавався лінійний спектр, що, по суті, означає необхідність виключення цифрових послідовностей, що повторюються.

Навіть коли це і не потрібно, скремблер цифрових сигналів корисні при перетворенні цифрових послідовностей з низькими щільностями переходів в послідовності зі значними складовими складовими. Скремблювання не використовується в низькошвидкісних системах передачі типу Т (Т1 та Т2), але застосовується в коаксіальних лініях передачі типу Т4М зі швидкістю передачі 274 Мбіт/с фірми Bell System [5].

Сигнал -зміна фізичної величини (наприклад, температури,тиску повітря, світлого потоку) тощо що використоується для пересилання даних.Саме завдяки цій зміні сигнал може нести в собі якусь інформацію. Інше визначення сигнал це фізичний процес якого визначається взаємодією між матерільним обєктом та засобом його дослідження.

Скремблери цифрових сигналів (з рівними швидкостями передачі на вході та виході) в абсолютному сенсі не запобігають появі довгих послідовностей нулів. Вони просто гарантують, що відносно короткі

комбінації, що повторюються, будуть перетворені до рандомізованого сигналу з мінімальною щільністю переходів. Якщо скремблированию піддається суто випадковий цифровий сигнал, то вихідний сигнал також є суто випадковим і, отже, є певна статистична можливість появи послідовності нулів будь-якої довільної довжини. Однак ймовірність такої випадкової події є прийнятною, якщо зіставити її з ймовірністю появи невипадкових послідовностей, що відповідають паузам мови або стану спокою терміналів даних. Для визначення того, яка з цифрових послідовностей, що здається випадковою, створює одні нулі на виході скремблер, подайте всі нулі на вхід відповідного дескремблера.

У коаксіальній системі передачі типу Т4М використовується скремблер цифрового сигналу як основний засіб отримання достатньої інформації, що хроніює. Ця система може допустити істотно довші послідовності нулів, оскільки в ланцюгах відновлення хронуючого сигналу в регенераторах використовуються схеми з фазовою автопідстроювання, що підтримує хронування протягом відносно довгих періодів часу. На відміну від цього, у системі типу Т1 хронуючий сигнал виділяється за допомогою резонансних контурів, резонанс у яких виникає при збудженні їх прийнятими імпульсами на потрібній тактовій частоті передачі зі швидкістю 1,544 Мбіт/с. Оскільки резонансні контури мають меншу ефективну добротність, ніж ланцюг із фазовим автопідстроюванням, частота коливань може уникнути необхідного значення, а коливання швидше загасають. Внаслідок цього для приймача системи типу Т1 неприпустимі послідовності нулів такої ж довжини, як для приймачів системи типу Т4М.

Умисне введення помилок. П'ятий метод підтримування достатньої хронуючої інформації в лінійних сигналах полягає у навмисному введенні іноді помилки в передавальному кінцевому пристрої для того, щоб перервати тривалу, не містить переходів послідовність цифрового сигналу. Якщо досить довгі послідовності без переходів є досить рідкісними, то навмисні помилки можуть бути більш рідкісними, ніж випадкові помилки в цифровій лінії передачі. Отже, навмисні помилки можуть вносити значного додаткового

погіршення. Проте введення умисних помилок як частина процедури перетворення коду передачі зазвичай не рекомендується і згадується для повноти викладу.

Як уже згадувалося, у каналоутворюючих блоках, що застосовуються в країнах Північної Америки, при передачі кодової комбінації з одних нулів навмисне вводиться помилка в передостанній за значенням розряд, щоб гарантувати достатню кількість переходів у сигналі. Важливим аспектом цієї процедури є те, що вона здійснюється у джерелі сигналу, де значення помилки відоме. Якби помилки виникали в самій лінії передачі, ефект був некерованим, особливо коли лінія надається для передачі різних видів сигналів.

У разі навмисного введення помилок виникає і більш тонка проблема, якщо цифрова лінія передачі використовується для передачі даних з автоматичним перезапитом. Лінія передачі даних з автоматичним перезапитом розрахована на забезпечення безпомилкової, незважаючи на випадкові помилки в каналі, передачі за рахунок введення надмірності в потік даних та перевірки прийнятих даних на відсутність помилок. Виявлення помилки потребує повторної передачі. Якщо помилки є не випадковими, а навмисне введеними в лінію передачі, то система з автоматичним перезапитом перестане працювати, якщо будь-коли зустрінеться послідовність (хоч би малоймовірно це не було), на передачу якої накладені обмеження. І ще раз: якщо використовуються навмисні помилки, їх слід вводити не в лінії передачі, а в джерела як один із видів обмежень, що накладаються на цифровий сигнал джерела.

1.2 Основні характеристики скремблювання

Основними технічними характеристиками скремблерів є рівень закриття інформації, залишкова розбірливість і якість відновлення сигналу.

Найбільш важливою характеристикою скремблера для користувача, який бажає забезпечити захист інформації у каналах зв'язку, є рівень закриття інформації. Слід зазначити, що, якщо для складних цифрових систем передачі мови та даних поняття рівня закриття суворо регламентується і визначається

криптографічною стійкістю інформації, то для аналогових скремблерів (особливо в системах рухомого радіозв'язку) дане поняття носить умовний характер, тому що на цей час з цього приводу не вироблено чітких стандартів чи правил.

У ряді випадків як критерії рівня закриття інформації при порівнянні різних засобів рухомого радіозв'язку з аналоговим скремблированием можна використовувати кількість ключових параметрів і кількість можливих ключів скремблера.

При скремблюванні генерується псевдовипадкова послідовність біт. Біт вхідного сигналу що надходить у скремблер додається за модулем 2 з бітом псевдовипадковою послідовності. Після чого біт відправляється на вихід, скремблер бере наступний вхідний біт псевдовипадкової послідовності і вхідної послідовності і повторює операцію. Зворотне перетворення здійснюється в зворотному порядку. Псевдовипадкова послідовність використовується циклічно. Скремблювання застосовується в багатьох сучасних системах цифрового звязку.

Під ключовим параметром аналогового скремблер зазвичай розуміють який-небудь параметр перетворення мовного сигналу, значення якого необхідно знати для здійснення зворотного перетворення сигналу на приймальній стороні.

Ключом аналогового скремблера (за аналогією з цифровими системами шифрування) зазвичай називають конкретний секретний стан деяких параметрів перетворення мовного сигналу. Кількість ключів скремблер визначається безліччю всіляких значень ключа. Для скремблер з одним ключовим параметром воно визначається числом можливих станів цього параметра, для скремблер з кількома ключовими параметрами — кількістю можливих комбінацій значень цих параметрів (як правило, добутком чисел станів всіх ключових параметрів).

Якість відновлення сигналу визначається спотвореннями сигналу за його частотних чи тимчасових перетвореннях. Фактично, ця характеристика

відображає розбірливість та впізнаваність відновленої мови. Прийнятною або комерційною якістю відновленої на приймальному кінці мовлення вважається таке, коли слухач без зусиль може визначити голос того, хто говорить, і сенс повідомлення.

Найкращою якістю відновлення сигналу володіють частотні інвертори, які практично не погіршують розбірливість і впізнаваність мови за умови правильної реалізації. Більш складні методи частотних перетворень можуть вносити деякі спотворення мовного сигналу. Реалізація високої якості відновлення мови при тимчасових перетвореннях потребує досить складної обробки.

Під залишковою розбірливістю розуміють відсоток відновлених фрагментів скремблированного мовного сигналу під час прослуховування переговорів з допомогою звичайних УКХ-приймачів чи радіостанцій, не оснащених аналогічним скремблером.

Слід зазначити, що переважна більшість відомих аналогових мовних скремблерів тією чи іншою мірою зберігають залишкову розбірливість. У прослуховуваному мовному сигналі, захищеному скремблером, зберігається інформація про темп мовлення, вловлюються паузи. При нескладних способах захисту досвідчений оператор може розібрати (залежно від наявності відомостей про тематику переговорів, що ведуться) від 10 до 50% переданої інформації.

1.3 Математичний апарат скремблювання

В Генератор псевдовипадкових чисел можна створити таку послідовність чисел, властивості якої будуть схожі на властивості послідовності випадкових чисел. Такі послідовності називаються псевдовипадковими.

Псевдовипадкові бінарні послідовності (ПВБП) широко використовуються в телекомунікаційних системах для криптозахисту інформаційного трафіку при потоковому і блочному шифруванні. Для створення ПВПБ застосовують апаратні або програмні генератори

псевдовипадкових чисел (ГПВЧ). На сьогодні відомо досить велика кількість реалізацій таких генераторів і виникає проблема об'єктивної оцінки їх якості з точки зору використання генеруються послідовностей в якості ключів при блочному шифруванні або параметрів генератора при Скремблювання.

У кожному конкретному випадку для обгрунтованого вибору ГПВЧ проводять тестування ПВБП «на випадковість». При великій довжині ПВБП процес тестування виявляється досить трудомістким по тимчасових витратах, що пов'язано з універсальністю більшості відомих тестів [1,2]. Тому бажано тестування проводити цілеспрямовано (селективно), вибираючи той чи інший тест відповідно до деякими зовнішніми вимогами, обумовленими або областю застосування ПВБП, або алгоритмом її генерації.

Так, методика, запропонована в 1999 році [1], передбачає використання набору з 16 тестів, кожен з яких орієнтований на виявлення конкретного властивості ПВБП, характерного для дійсно випадкової послідовності. Наприклад, найпростіший з них (Monobit, Block Frequence Cummulative Sums Forward reserve) заснований на тривіальної ідеї підрахунку відносних частот нулів і одиниць в послідовності або її фрагментах. Очевидно, що навіть проста послідовність чергуються нулів і одиниць буде успішно протестована як задовільна. Наступними за складністю є тести типу Runs або Long Runs of Queues, контролюючі довжини, що виникають у досліджуваній послідовності так званих стаціонарних ділянок (що складаються тільки з нулів або тільки одиниць). Фактично, ці тести (як і попередні) виявляють використання примітивних процедур генерації ПВБП, наприклад, формування послідовності шляхом нарощування її довжини за рахунок повторення стаціонарних фрагментів.

Група тестів, які контролюють періодичність в послідовності (Discrete Fourier Transform, Periodic Templates, Aperiodic Templates) також орієнтована на виявлення спрощених процедур генерації, їх принциповим обмеженням є орієнтація на короткі періоди повторення фрагментів.

Тести, які перевіряють «випадковість блукання» (Random Excursions,

Random Excursions Variant) є вельми перспективними з теоретичної точки зору. Однак, з іншого боку, способи маскування, щоб забезпечити проходження тестів, досить прості і. втой же час, ефективні.

Тест Linear Complexity виявляє умовну складність послідовності з точки зору її аналітичного опису, але обмежений лише лінійними формами уявлення.

До останньої групи належать тести інформаційного характеру (Universal Statistical Test, Approximate Entropy, Lempel-Ziv Complexity), що базуються на вимірюванні кількості інформації, яка міститься в тестованої ПСБП. Використовується підхід, заснований на вимірюванні ефективності компресії або порівняння частот перекриваються фрагментів з можливостями таких подій для дійсно випадкової послідовності.

В цілому, тести NIST, які отримали на сьогодні найбільше поширення і визнання, є хорошим інструментом для порівняльної оцінки різних ПВБП в деякій умовній системі координат.

Однак, строго кажучи, отримані оцінки можна розглядати як в певній мірі суб'єктивні, оскільки вони жорстко прив'язані до вибраного набору тестів. Найбільш перспективним, є інформаційний підхід і тому може бути поставлена задача побудови деякої універсальної процедури обчислення таких характеристик ПВБП, які дозволили б оцінити, наскільки конкретна бітова послідовність близька до дійсновипадкової.

При цьому істинно випадкової будемо вважати таку послідовність, в якій будь-який фрагмент довільної довжини з'являється приблизно з однаковою частотою. Наприклад, уявімо собі, що 2^S фрагмент ПСБП спостерігається через деякий уявне «вікно» шириною S біт, і для істинно випадкової послідовності все різновидів фрагмента є рівноімовірними.

У цих припущеннях може бути поставлена наступна задача.

Задана конкретна бітова послідовність.

$$W = (w_1, w_2, \ldots, w_n)$$

Необхідно оцінити кількісно, наскільки ця послідовність близька до

дійсно випадковою. Тобто мова йде про спробу об'єктивної оцінки якості конкретної ПВБП.

В інших випадках, наприклад, відносяться до криптоанализу, постановка задачі може бути конкретизована за рахунок деякої додаткової інформації, відомої спочатку криптоаналітику.

Як і в попередньому випадку задана конкретна ПВБП. Крім того, відомий загальний алгоритм формування послідовності. Наприклад, імовірно відомо, що генератором ПВБП є регістр зсуву з зворотними зв'язками по модулю 2 (LFSR - linear feedback shift register), а тестування має підтвердити або спростувати цю гіпотезу і виявити (виявити) кореляційні залежності між окремими фрагментами ПВБП. Отриманий результат в цьому випадку може бути використаний для організації відповідної атаки, тобто обчислення конкретних зворотних зв'язків в регістрі генератора і його початкові установки.

Очевидно, при вирішенні другого завдання корисно використати цю додаткову інформацію з тим, щоб зменшити трудомісткість обчислень при тестуванні.

Основний і, в багатьох випадках, доступною є інформація про клас апаратних або програмних засобів, які використовуються для генерації ПСБП.Найчастіше відомо, наприклад, що в якості генератора ПВБП застосований лінійний фільтр з зворотними зв'язками по модулю 2.

У цьому випадку конкретна ПВБП однозначно може бути обчислена криптоаналітиків на основі таких параметрів: довжина регістра d; коефіцієнти многочлена, що задає конкретний вид зворотних зв'язків регістра.

2 ЗАВАДОСТІЙКЕ КОДУВАННЯ В МЗ

2.1 Математичний апарат лінійних автоматів

Розглянемо побудову цифрового передавача з прикладу формування сигналу формату 64КАМ. На рис. 2.1 наведено спрощену структурну схему передавального кінцевого обладнання (цифрового передавача). Згідно з Рекомендацією F.59б, МСЕ-Р цифрові системи радіозв'язку можуть з'єднуватися з іншим обладнанням тільки на цілком певних ієрархічних цифрових швидкості.

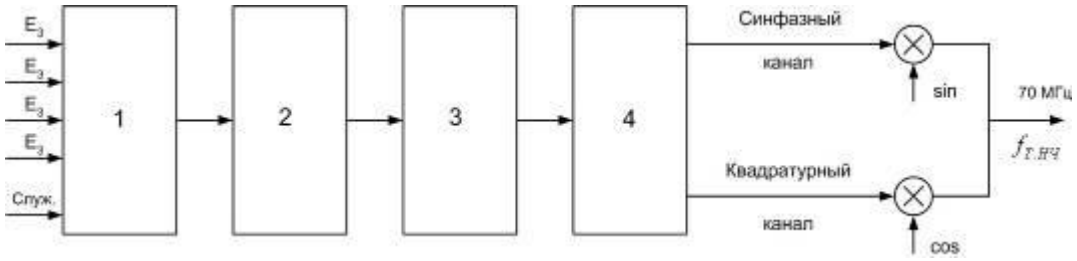

Рисунок 2.1 — Цифровий передавач

Припустимо, що на вхід пристрою формування синфазного та квадратурного потоків цифрового передавача надходить 4 цифрові потоки Е3. та службова інформація. Ці потоки об'єднуються та кодуються самоортогональним згортковим кодом зі швидкістю 18/19 для забезпечення можливості виправлення помилок. В результаті швидкість цифрового потоку має ефективну швидкість передачі 150 Мбіт/с.

Цей процес групування є внутрішньою справою для радіосистеми та не стандартизований МСЕ-Т, що не має жодних негативних наслідків для замовника, тому що входи та виходи цифрових систем мають стандартизовані ієрархічні швидкості. Інформаційні біти далі скремблюються в синхронізованому скремблері, що дозволяє забезпечує гладкий випромінюваний спектр, вільний від спектральних ліній, які могли б викликати значні перешкоди в аналогових радіоканалах, а також гарантує ефективну синхронізацію та відновлення несучої. Далі сформований цифровий потік розбивається на два потоки, що мають вдвічі меншу швидкість — 75 Мбіт/с.

Ці потоки використовуються для формування синфазного цифрового потоку (J) та квадратурного цифрового потоку (Q). Потім у цифроаналогових перетворювачах (Ц/А) із трьох імпульсів кожного потоку формуються 8-рівневий імпульсно-амплітудний формат як у синфазному (J), так і квадратурному (Q) каналах. Синфазний (J) і квадратурний (Q) канали, що перемножуються з синфазної (cos(Ці потоки використовуються для формування синфазного цифрового потоку (J) та квадратурного цифрового потоку (Q). Потім у цифроаналогових перетворювачах (Ц/А) із трьох імпульсів кожного потоку формуються 8-рівневий імпульсно-амплітудний формат як у синфазному (J), так і квадратурному (Q) каналах.

Синфазний (J) і квадратурний (Q) канали, що перемножуються з синфазної (cos(Ці потоки використовуються для формування синфазного цифрового потоку (J) та квадратурного цифрового потоку (Q). Потім у цифроаналогових перетворювачах (Ц/А) із трьох імпульсів кожного потоку формуються 8-рівневий імпульсно-амплітудний формат як у синфазному (J), так і квадратурному (Q) каналах. Синфазний (J) і квадратурний (Q) канали, що перемножуються з синфазної (cos(ωt) та квадратурної (sin(ωt) складовими сигналу проміжної частоти, наприклад, 70 МГц. Це дозволяє формувати 64 (8 x 8 = 64) різні значення комплексного вихідного сигналу цифрового передавача, що призводить до швидкості вихідного сигналу 25 Мбод.

Аналіз обчислювальних процесів на основе симетрії часу. Якщо розглядати категорію часу лише з позицій математики, то можна помітити, що фундаментальні закони і класичної, і квантової динаміки відразу мають еквівалентність причин і наслідків, що тягне за собою еквівалентність “минулого” та "Майбутнього" [10]. Іншими словами, теореми, які справедливі при зміні часу від "справжнього" в "майбутнє", будуть також справедливі при зміні часу від справжнього" в "Минуле".

Розглянемо динамічні системи (ДС), які характеризуються множинами входів, виходів і станів, а також двома функціями: переходів та виходів.

У генератора псевдовипадкових послідовностей повинен бути великий період. А також генератор повинен пройти строгі тести на незалежність і рівномірність. Існує досить багато методів отримання нормального Розподілення випадкових чисел. В ході дослідження була проведена адаптація методу перетворення Бокса-Мюллера. У підході «Один генератор випадкових числі на потік» ідея полягає в тому, що кожен потік, що виконується паралельно організований таким чином, щоб генерувати випадкові послідовності не залежно від інших. Так велика частина алгоритмів генерації (Mersenne Twister і Lagged Fibonacci), які використовують рекурсивне перетворення дозволяють отримати (n +1)-е число не знаючи n-го числа. Кількість одержуваних таким методом чисел, яке, в загальному випадку, залежить від вибору параметрів для генераторів псевдовипадкових послідовностей, має дорівнювати числу потоків N або кратному числу M × N.

2.2 Реалізація автоматного скремблювання

Для алгоритмів скремблювання виключно важливі швидкість роботи і випадковий характер послідовності, щоб його не можна було відновити в разі перехоплення противником. Процес скремблювання може включати в себе додавання певних компонент до вихідного сигналу або зміна важливих час- тин сигналу для того, щоб ускладнити відновлення виду вихідного сигналу або для додання сигналу певних статистичних властивостей. Скремблери за- стосовуються в телефонних мережах загального користування, супутниково- го та радіорелейного зв’язку, цифровому телебаченні, а також для захисту ла- зерних дисків від копіювання.

Головною рисою потокових шифрів є побітна обробка інформації. Шифрування і дешифрування в таких схемах може обриватися в довільний момент часу, як тільки з'ясовується, що потік що передається перервався, і також відновлюється при виявленні факту продовження передачі.

Найбільш поширеними представниками потокових шифрів являються скремблери (рис 2.2).

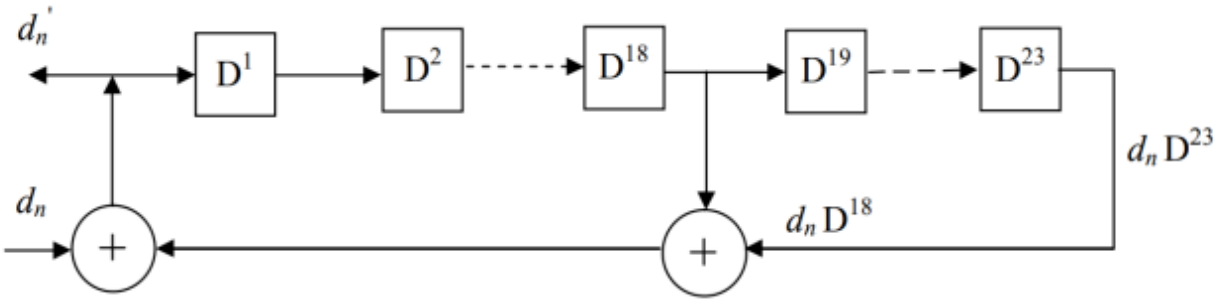

Рисунок 2.2 — Скремблер

Двійковий сигнал на вході може мати довільну статистичну структуру, яка не завжди задовольняє вимогам, які пред'являються синхронним способом передачі. Серед цих вимог основними є такі.

Частота зміни символів (1, 0) повинна забезпечувати надійне виділення тактової частоти безпосередньо з сигналу.

Спектральна щільність потужності сигналу, що передається, повинна бути, по можливості, постійною і зосередженою в заданій області частот з метою зниження взаємного впливу каналів.

Наведені вимоги повинні виконуватися незалежно від структури повідомлення, що передається. Сенс такої обробки полягає у отриманні послідовності, у якій статистика появи нулів і одиниць наближається до випадкової, що дозволяє задовольнити двом названим вище вимогам.

Одним із способів такої обробки є скремблювання (scramble — перемішування). Скремблювання — це оборотне перетворення структури цифрового потоку без зміни швидкості передачі з метою отримання властивостей випадкової послідовності.

Скремблювання проводиться на стороні, що передає, за допомогою скремблера, що реалізує логічну операцію підсумовування по модулю два вихідного і псевдовипадкового двійкових сигналів. На приймальній стороні здійснюється зворотне перетворення — дескремблювання, що виконується дескремблером. Дескремблер виділяє із прийнятої послідовності вихідну

інформаційну послідовність. На рис. 2.3 показано включення скремблера та дескремблера до каналу зв'язку.

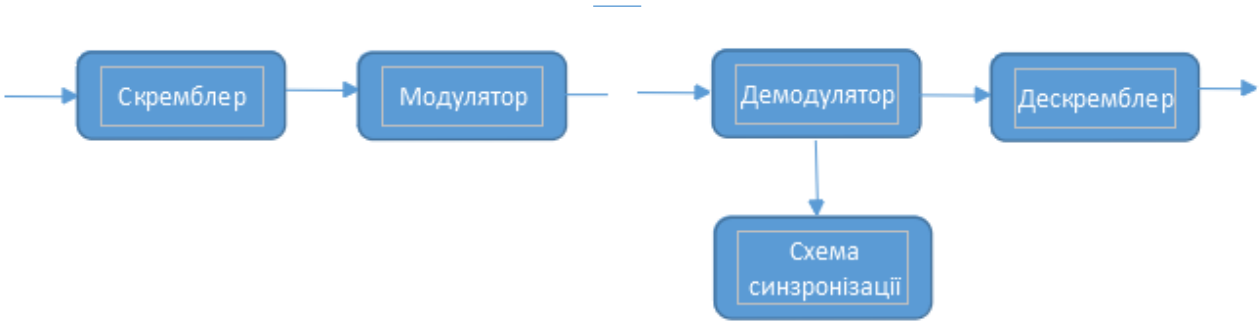

Рис. 2.3 — Схема включення скремблера та дескремблера до каналу зв'язку

Основною частиною скремблера є генератор псевдовипадкової послідовності (ПВП) у вигляді лінійного-каскадного регістру зі зворотними зв'язками, що формує послідовність максимальної довжини 2-1. Розрізняють два основних типи скремблерів-дескремблерів — самосинхронізуються та з початковою установкою (адитивні).

Схема пари самосинхронізованих скремблер-дескремблер представлена на рис. 2.4. Особливістю самосинхронизирующего скремблера і те, що він управляється скремблированной послідовністю, тобто. тієї, що надходить у канал.

Тому в даному випадку не потрібно спеціальної установки станів скремблер і дескремблера, оскільки вони виявляються ідентичними в результаті запису в їх регістри зсуву скрембльованої послідовності.

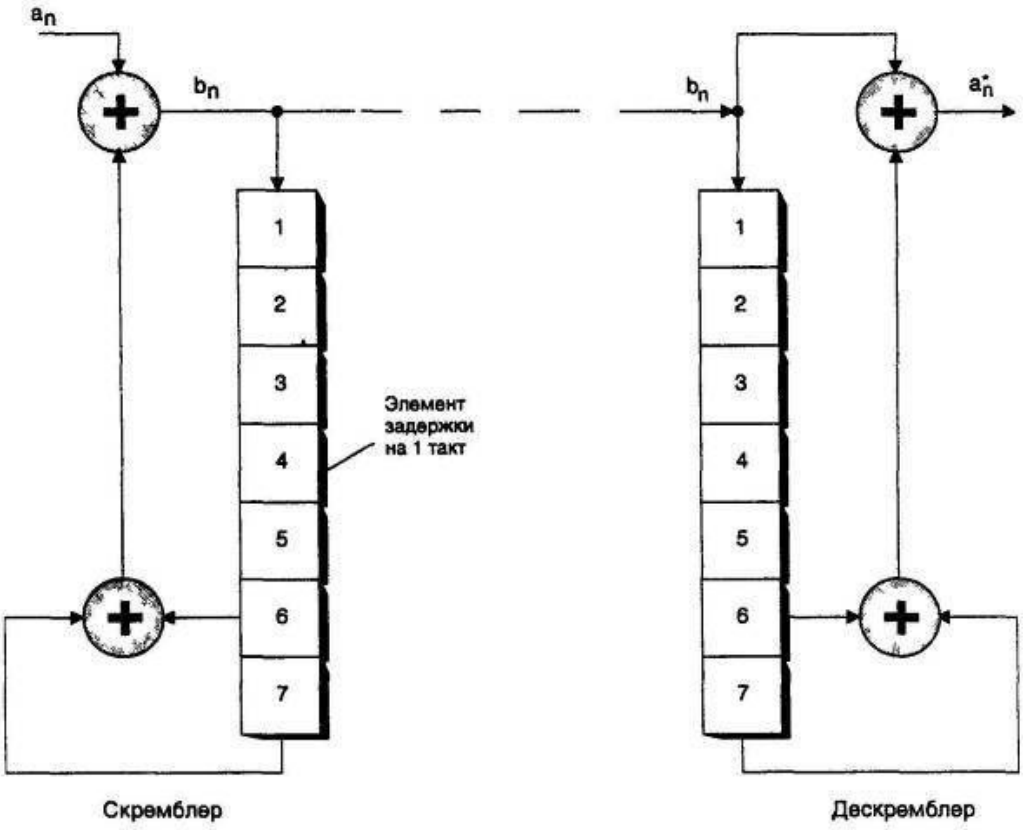

Рис. 2.4 — Схема скремблювання з самосинхронізацією

При втраті синхронізму між скремблером і дескремблером час його відновлення вбирається у числа тактів, рівного числу осередків регістру скремблера. На приймальній стороні виділення інформаційної послідовності відбувається додаванням по модулю два прийнятої скрембльованої послідовності з псевдовипадковою послідовністю (ПВП) регістру. Наприклад, для схеми, зображеної на рис. 2.5, вхідна послідовність an за допомогою скремблера відповідно до виразу перетворюється на двійкову послідовність bn, що посилається в канал. У приймачі з цієї послідовності таким же регістром зсуву, як і передачі, формується послідовність яка ідентична послідовності an .

$$bn = an + (bn - 6 + bn - 7)$$

$$an * bn + (bn - 6 + bn - 7)$$

Це легко перевіряється при перетворенні першого виразу до виду та порівнянні отриманого виразу з попереднім.

$$an = bn + (bn - 6 + bn - 7)$$

Одним із недоліків самосинхронізуючих скремблерів-дескремблерів є властива їм властивість розмноження помилок. Так, для схеми на рис. 2.5 при одній помилці в послідовності bn помилковими виявляються також 6-й та 7-й символи.

Реконструкція самосинхронізованих скремблер. Адитивні скремблери на основі автономних ЛПС працюють при нульових вхідних впливах, тому вони є лінійними автоматами Мура. Функціонування самосинхронізації низуючих скремблерів залежить від вступника з їхньої вхід інформаційної послідовності , що дозволяє віднести такі скремблер до більш складної автоматної моделі – лінійним автоматам Милі, або ЛПС Мілі

Загалом вплив помилково прийнятого біта виявлятиметься α раз, де α — число зворотних зв'язків. Цей недолік обмежує кількість зворотних зв'язків у регістрі зсуву, яке майже перевищує α=2, тобто. поліном регістру є триномом виду $xn + xu + 1$. Другий недолік самосинхронізуються скремблер пов'язаний з можливістю появи на його вході так званих "критичних ситуацій", коли вихідна послідовність набуває періодичного характеру з періодом, меншим за довжину ПВП.

Недоліки, властиві самосинхронізуючим скремблер-дескремблера, практично відсутні при адитивному скремблюванні (рис. 2.5).

Однак у цьому випадку потрібна попередня ідентична установка станів регістрів скремблера та дескремблера.

У скремблер з початковою установкою, як і в самосинхронізуючому скремблер, проводиться підсумовування вхідного сигналу і ПВП, але результуючий сигнал не надходить на вхід регістру.

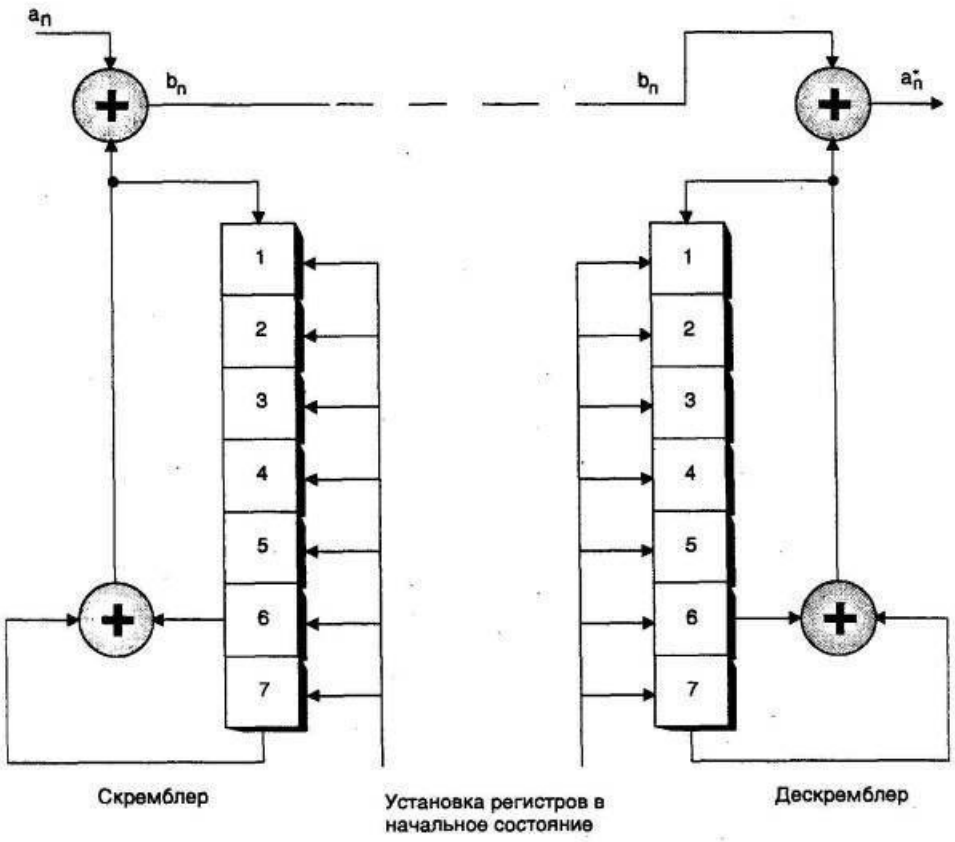

Рис. 2.5 - Схема скремблювання з початковою установкою

У дескремблері скремблированная послідовність також проходить через регістр зсуву, тому розмноження помилок немає.

Підсумовані в скремблер послідовності незалежні, тому критичних ситуацій не настає. Відсутність ефекту розмноження помилок і необхідність спеціального захисту від небажаних ситуацій роблять спосіб адитивного скремблювання кращим та економічно ефективнішим, якщо не враховувати витрат на вирішення завдання взаємної синхронізації пари скремблер-дескремблер.

Скремблери активно застосовуються для захисту телефонних переговорів. При скремблюванні можливе перетворення мовного сигналу за трьома параметрами: амплітуді, частоті і часу. Але в системах рухомого радіозв'язку практичне застосування знайшли в основному частотні і часові перетворення сигналу, а також їх комбінації.

Можливі перешкоди в радіоканалі істотно ускладнюють точне відновлення амплітуди мовного сигналу, в зв'язку з чим амплітудні перетворення при скремблюванні практично не застосовуються.

Розглянемо вплив скремблювання на енергетичний спектр бінарного сигналу. На рис. 2.6 а зображений приклад енергетичного спектра для періодичного сигналу з періодом Т, що містить 6 двійкових елементів з тривалістю Т0.

Після скремблювання ПВП з М=2n-1 елементами спектр суттєво "збагачується" (рис. 2.6, б). У прикладі число складових спектра збільшилося в М разів, одночасно рівень кожної складової зменшується в таку кількість разів.

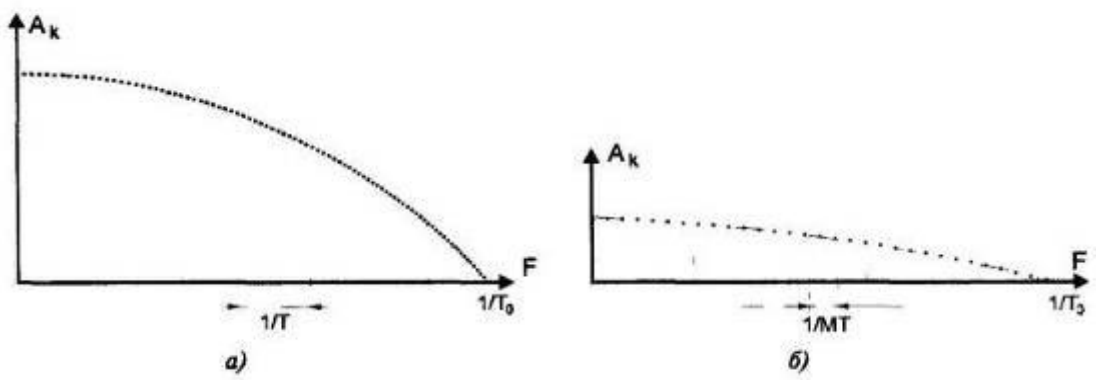

Рис. 2.6 — Спектр сигналу до (а) та після (б) скремблювання

Приведені скремблер і дескремблер широко використовуються в обладнанні зв'язку, включаючи апаратуру систем SHDSL і ADSL.

Використаємо MATLAB для моделювання процесу скремблювання та дескремблуванн, як показано нижче:

```
x = randi(2,1,1000)-1;% Початкова ПВБП

%--------------------------------------%
%%%  ------------ Скремблер ------------ %%%
%--------------------------------------%
%scrambler = randi(2,1,8)-1;% Початковий стан регістру  зсуву скремблера
scrambler = [0,1,1,0,1,1,1,1];
```

```
descrambler = scrambler;
y_scrambler = zeros(1,1000);
for i = 1 : 1000
  z(1) = bitxor(scrambler(1),scrambler(5));% Модуль2Сумматор (АБО)
  z(2) = bitxor(z(1),scrambler(6));
  z(3) = bitxor(z(2),scrambler(7));
  y_scrambler(i) = bitxor(z(3),x(i));
  for j = 1 : 7          % Shift регистр
     scrambler(j) = scrambler(j+1);
  end
  scrambler(8) = y_scrambler(i);
end
%---------------------------------------%
%%%  ------------ Дескремблер ------------ %%%
%---------------------------------------%
y_descrambler = zeros(1,1000);
for i = 1 : 1000
  z(1) = bitxor(descrambler(1),descrambler(5));% Модуль2Сумматор (АБО)
  z(2) = bitxor(z(1),descrambler(6));
  z(3) = bitxor(z(2),descrambler(7));
  y_descrambler(i) = bitxor(z(3),y_scrambler(i));
  for j = 1 : 7        % Shift регистр
     descrambler(j) = descrambler(j+1);
  end
  descrambler(8) = y_scrambler(i);
end
```

Результати скремблювання та дескремблювання порівнюються таким чином, ви можете бачити, що вихідні дані повністю узгоджуються з даними після дескремблювання:

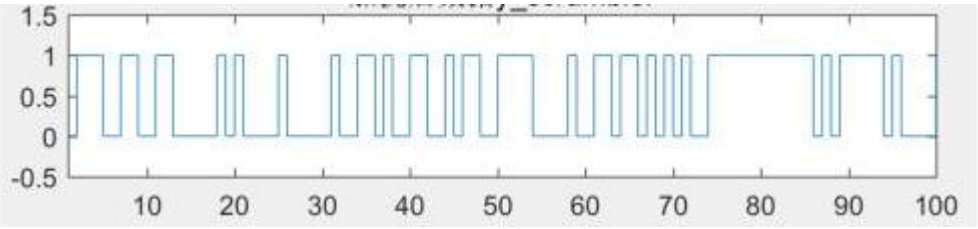

Рис. 2.7 — Скремблер у середовиші Matlab

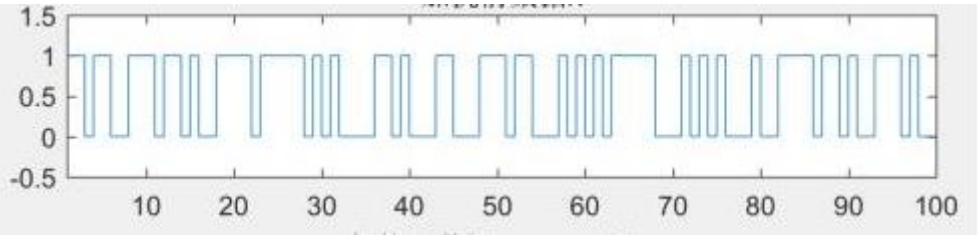

Рис. 2.8 — Дескремблер у середовиші Matlab

2.3 Реалізація автоматного дескремблювання

Дескремблер є такий пристрій, який призначений для відновлення вихідних структур цифрових каналів зв'язку, перетворених спочатку скремблером. Це функціональний блок, який дозволяє швидко відновлювати вихідний вид сигналу передавача. Дескремблер завжди працює, здійснює свою роботу разом зі скремблером, який зазвичай монтується в передавачах. Дескремблер дозволяє виключити псевдовипадковість, яка могла бути внесена в цифрові потоки передачі. При дескремблюванні відбувається повторне скремблювання потоку, причому використовується ідентичний генератор, який дозволяє ініціювати сигнали скремблера.

Багатоканальний дескремблер часто використовується для телекомунікаційних та кабельних операторів, а також для монтажу мереж мовлення. Цей пристрій допомагає розблокувати закритий цифровий сервіс.

За наявності чотирьох слотів дексремблер може дескремблювати мінімум чотири канали, які підтримують багато провідних систем умовного доступу. Для реалізації роботи первісна фаза будь-якого дескремблера встановлюється відповідно до фази скремблера.

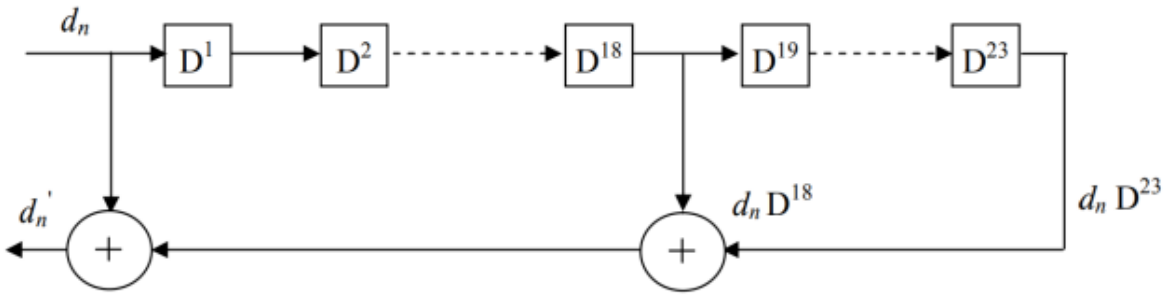

Рис. 2.9 — Дескремблер

Зауважимо, що скремблер є рекурсивним пристроєм, в той час як дескремблер - нерекурсивним (не містить зворотний зв'язок). приведена пара скремблера і дескремблера характеризується породжуючим поліномом G (D):

$$G(D) = D^{23} + D^{18} + 1 \quad (2.1)$$

Коефіцієнти полінома (2.1) вказують на розташування відводів, де здійснюється операція підсумовування по модулю 2. Породжуючий поліном скремблера зазвичай вибирається таким чином, щоб забезпечити на виході псевдовипадкову послідовність максимальної довжини, коли на вхід скремблера надходять поспіль нулі або одиниці. Іншими словами, послідовність максимальної довжини характеризує періодичність генерованої послідовності при незмінному сигналі на вході скремблера.

Якщо коефіцієнти полінома обрані правильно, то зазвичай, чим довший скремблер, тим довші послідовності максимальної довжини він виробляє.

При цьому довжина послідовності максимальної довжини скремблера дорівнює $2^n - 1$, де n — порядок породжуючого полінома скремблера.

Скремблер і дескремблер, зображені на рисунках 2.2 і 2.9, є самосинхронізуючими: почавши працювати в довільному стані (тобто при довільних початкових сигналах в комірках скремблера/дескремблера), після певного проміжку часу дескремблер починає видавати правильно передані двійкові символи. Крім того, помилка біта в каналі не буде приводити до

значного збільшення кількості помилок (розмноження помилок) на виході дескремблера.

Цією властивістю дескремблер володіє завдяки відсутності в ньому зворотного зв'язку. Однак дескремблер збільшує число помилок. Одна однобітова помилка на вході дескремблера призводить до кількості однобітових помилок, рівному числу відводів дескремблера. У показаному на рис. 2.9 прикладі одна однобітова помилка на вході виробляє три однобітових помилки на виході дескремблера. Цей недолік компенсується тими перевагами, які забезпечує скремблювання, і тому воно широко застосовується в сучасній апаратурі зв'язку. У різних напрямках передачі використовуються різні породжуючі поліноми скремблювання.

В даному розділі визначили поняття скремблювання та дескремлювання. Здійснили опис математичного апарату лінійних автоматів та розглянули різні схеми скремблювання. Розв'язання системи рівнянь (10) необхідне як ЛПС типу Фібоначчі, і типу Галуа. Єдиним винятком є ЛПС типу Фібоначчі, у якої послідовність X поступає лише з виходу останнього ЕП. В цьому разі немає необхідності вирішувати систему рівній (10), оскільки останні r біт послідовноності X безпосередньо є останнім станом S(n). Тому такий скремблер має мінімальний криптозахист.

РСЛОС є найбільш популярним схемотехнічним вузлом у завданнях скремблювання та поточного шифрування. І хоча вже багато десятиліть ведеться теоретичне дослідження їх властивостей, як і раніше з'являються нові можливості. Давно відомо, що джерела нових знань часто з'являються на стиках різних галузей науки, особливо близьких по суті. Для криптографії такий близькою галуззю є перешкодостійке кодування. Є численні приклади застосування ня алгебраїчної теорії кодування для Індивідуальних шифросистем [15]. У цій роботі передається ще один варіант такого плідного взаємодії. Якщо застосувати в задачах шифрування теорію ЛПС та автоматні уявлення циклічних кодів, тоді можна отримати багато нових перспективних

напрямів для подальших досліджень. Одним з них є використання в криптографії темпоральних (тимчасових) моделей.

Основна мета скремблювання полягає в підвищенні надійності синхронізації пристроїв на стороні передавача і приймача за допомогою утримання статистичних властивостей, що передаються даних. В результаті скремблювання на стороні приємника змінюється вид інформаційної після довальності I , тобто. відбувається шифрування відкритого тексту. За допомогою дескремблера на стороні приймача послідовність I відновлюється, тобто. дешифрується. Таким чином, ми маємо справу з різновидом потокового шифрування. Завдяки високої швидкості перетворень таке шифрування найбільш придатне для мобільного та інших видів зв'язку. Тому актуальним є поєднання операцій скремблювання та захисту інформації.

Кодування із зміною сигналу всердині такту (RZ код та Манчестерський код)

Два основних недоліки кодування NRZ – міжсигнальну інтерференцію та відсутність самосинхронізації — усуває спосіб кодування із обов'язковою зміною сигналу всередині такту. Зокрема таку властивість мають код RZ (із поверненням до 0) та так званий «манчестерський код» із зміною фази сигналу. Для сигналів AMI (Alternate Mark Invertion) значення «1» відображаються активними сигналами, для яких чергуються полярнсті, в той час як «0» задаються паузами. При цьому забезпечуються усунення межсігнальной інтерференції і частково самосинхронізація. Можлива втрата сінронізаціі для довгої послідовності «0» усувається за рахунок "вставок" активних сигналів, які порушують правило чергування полярностей (в цьому випадку приймач не розпізнає такі вставки як такі, що несуть інформацію). AMI-сигнали (точніше - їх вдосконалені модифікації) широко застосовуються в цифровій телефонії, тобто - при передачі на великі відстані.

Типові схеми збиткового логічного кодування. В практиці широко використовуються схеми логічного кодування із введенням збитковості. Тут групи бітів вихідного потоку (в сфері звязку їх традиційно називають

«символами») перетворюються у відповідні блоки більшої довжини. При цьому вирішується задача усунення незручних для передачі бітових послідовностей, а разом з цим реалізуються додаткові можливості, які надає збитковість — зокрема використання додаткових службових кодів, а також часткове виявлення помилок передачі.

Різноманітні пристрої у яких застосовуються зсувні реєстрори. Буферні накопичувачі конвеєрні системи лічильники за модулем N та кінцеві автомати можуть мати значну велику продуктивність при використанні сучасних компонентів, що працюють у діапазоні частот. як приклад можна вказати кристал 10G022 працюючий як послідовний або як паралельний зсувний регістр. Виконаний на основі арсеніду-галію технології і що володіє максимальною затримкою порядку 950 ПС цей кристал забезпечує 3-4 кратне підвищення продуктивності в порівнянні з аналогічними пристроями при вихідній споживаній потужності.

Програма працює діалоговому режимі і отримує два пробних з'єднання, дає наступну інформацію полегшують вибір з'єднань ідентифікує цикл, стан вказує чи код кодом в максимальній довжині, формує список всіх небажаних станів, генерує цикл стану для кожного з небажаних станів і застерігає від зависання.

3 ПРОГРАМНО-АПАРАТНА РЕАЛІЗАЦІЯ СКРЕМБЛЕРІВ

3.1 Програмна реалізація скремблерів

Як приклад розглянемо скремблер, який використовується в супутниковому зв’язку [3]. Реалізація скремблера виконана мовою С++

```
// Функция для скремблирования одного байта информации:
unsigned char SCR(unsigned char byte, bool begin)
// begin - признак скремблирования и дескремблирования
// с начальным значением регистра
{ // Параметры скремблера:
 unsigned char genpoly[2];// порождающий полином (номера
 // ненулевых элементов)
 unsigned int initseq; // инициализирующая последовательность
 static int reg;
 unsigned char i,j,genb,inb,outb;
 unsigned char outbyte;
 initseq=0xFFFFE;
 genpoly[0]=2; genpoly[1]=19;
 begin=true;
 if(begin)
 { reg=initseq;
 begin=false;
 }
 outbyte=0;
 for(i=0;i < 8;i++)
{ genb=0;
 for(j=0;j < 2;j++)
 genb^=(reg>>genpoly[j])&1;
 inb=(byte>>i)&1;
```

```
 outb=!inb^genb;
 outbyte|=outb<<i;
 reg=(reg<<1)|outb;
 }
 return outbyte;
}
// Функция для дескремблирования одного байта информации:
char deSCR(char byte, bool begin)
{ static int reg;
 char i,j,genb,inb,outb;
 char outbyte;
 if(begin)
 { reg=initseq;
 begin=false;
 }
 outbyte=0;
 for(i=0;i < 8;i++)
 { genb=0;
 for(j=0;j < 2;j++)
 genb^=(reg>>genpoly[j])&1;
 inb=(byte>>i)&1;
 outb=!inb^genb;
 outbyte|=outb<<i;
 reg=(reg<<1)|inb;
 }
 return outbyte;
}
```

У наведеному скремблері не використовується випадкова послідовність.

При подачі на вхід скремблера періодичної послідовності 10001000 10001000 10001000, що містить «1» в три рази менше, ніж «0», ми отримуємо

на виході неперіодичну послідовність 00010011 11001000 11110110 з рівною кількістю «0» і «1». Подача на вхід послідовності такої ж довжини лише з «1», призводить до вихідної послідовності 00011100 11000111 100010001. Збій 8-го біта при дескремблюванні призводить до наступної послідовності: 11111011 11111111 11101111, тобто збої розмножуються.

Розглянутий скремблер, широко використовуваний в супутниковому зв'язку, в наведеній класифікації доведеться віднести до класу таких, що самосинхронізуються, незважаючи на не використання ПВП. Тепер розглянемо один з скремблерів, реалізований у Matlab. Викликається він функцією wlanScramble(). Як видно з імені функції, використовується він в локальних бездротових мережах (WLAN — Wireless Local Area Network). Він відповідає стандарту IEEE 802.11-2012, розділ 18.3.5.5 та стандарту IEEE 802.11ad-2012, розділу 21.3.9.

Поля заголовка і даних, які слідують за полем ініціалізації скремблера (включаючи біти заповнення даних), дані скремблюються шляхом операції XOR (виключаюче «або») кожного біта з періодичною послідовністю довжиною 127, згенерованої поліномом $S(x) = x^7 + x^4 + 1$.

Схема роботи скремблера показана на рисунку 3.1.

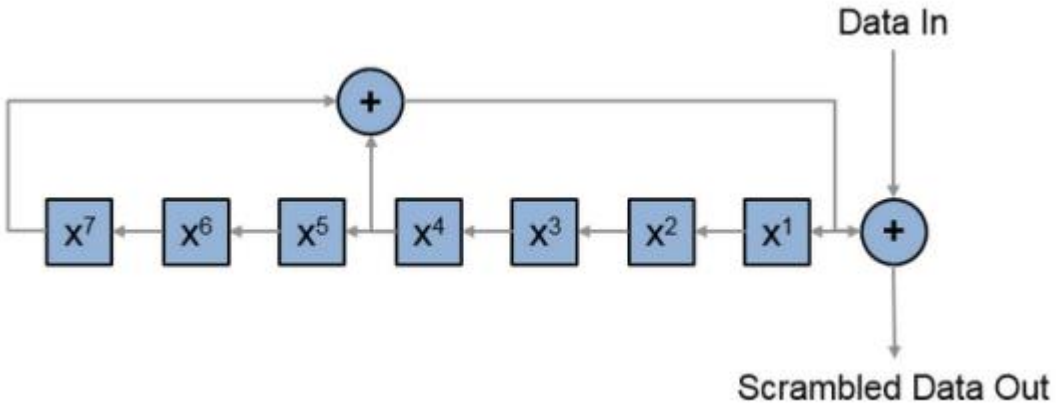

Рис. 3.1 — Логічна схема скремблера для локальних бездротових мереж

Одним з чудових властивостей скремблера є еквівалентність повторного скремблювання дескремблюванню.

Скремблер по першій послідовності видає масив 1100100 10010001 00100001 з частотою появи «1» всього 0.375, і скремблеру потрібно 7 байтів вхідної послідовності для досягнення однакової частоти появи «0» і «1».

Скремблювання лише «1» призводить до послідовності 10010011 11100110 01010110, спотворення 8-го біта перед дескремблюванням призводить до спотворення тільки 8-го ж біта вихідної послідовності. Безумовно, скремблер відноситься до класу адитивних.

Також, на сьогоднішній днь з’явилось чимало програмного забезпечення саме на мобільні пристрої для шифрування сигналу.

3.2 Апаратна реалізація скремблерів

Також для захисту можна використовувати скремблери, які добре зарекомендували себе при захисті звичайних телефонних мереж. Як приклад можна привести GUARD GSM. Даний пристрій (як і аналоги) з'єднується зі стільниковим телефоном по провідній гарнітурі й має невеликі розміри.

Скремблер GUARD GSM має тридцять два режими скремблювання. Принцип роботи даного скремблера заснований на первісному руйнуванні й часової перестановки звуку на передавальній стороні з його наступним відновленням на стороні, що ухвалює. Цей процес двосторонній. Часова перестановка відрізків мовного сигналу й відновлення їх послідовності на прийманні займають деякий інтервал часу. Тому обов'язковою властивістю такої апаратури є невелика затримка сигналу на прийомній стороні. Початок розмови, як правило, починається у відкритому режимі й далі по обопільній команді пристрою перемикаються в режим скремблювання.

При веденні переговорів прилад виконує одночасно дві функції скремблювання й дескремблювання. Тобто вимовлена одним з абонентів мова шифрується з його боку, а другий скремблер, що перебуває в другого абонента розшифровує дану мову. І теж саме відбувається у зворотному напрямку, коли починає говорити другий абонент.

Технічні характеристики:

— розбірливість мови не менш 95%;
— тип з'єднання повний дуплекс;
— затримка сигналу в лінії не більш 100 мс;
— рівень захищеності лінійного сигналу часовий;
— використання в мережах стандарту gsm 900/1800;
— тип підключення до стільникового телефону провідна гарнітура 7.

Також розглянем опристрій FSM-U1-це нова розмова з кодуванням пристрою для мобільного телефону-смартфона. Скремблер має потужний новий алгоритм "закрити" розмову, використовуючи "кілька динамічних фаз обробки" технології. Використання FSM-U1, перехоплення на вашому телефоні стає абсолютно неможливим, незалежно від методів перехоплення. Будь-які методи маються на увазі, в тому числі "оператор" контроль, пасивний перехоплення в області телефону, активного перехоплення шляхом перемикання телефону на "помилкові" бази і т. д. режим кодування.

Досить низька вартість скремблер дозволяє створити "мережу" серед постійних партнерів або всередині корпоративної "Топ" для проведення повністю "закритих" переговорів в рамках цієї мережі.

Скремблер реалізується у вигляді гарнітури та підключається до відповідного роз`єму смартфонів. При підключенні до скремблеру розмова ведеться через нього або навушників. FSM-U1 має вбудований динамік і мікрофон.

Пристрій живиться від вбудованої батареї Li-Pol 3.7 В потужністю 290 маг. Ресурс батарей-до 2,5 годин розмови в режимі скремблювання. Час поповнення становить 2 години, з USB (комп`ютер, Мережа або роз`єм у автомобілі).

Ще один мобільний скремблер Avantalk забезпечує захист інформації, що передається мобільним телефоном. Скремблери активно застосовуються для захисту телефонних переговорів, не дозволяючи системам радіомоніторингу мобільного зв'язку здійснювати «прослуховування» за ключовими словами та характерними змінами інтонації голосу.

При використанні скремблера Avantalk підслуховування розмови, яка ведеться вашим телефоном, стає повністю неможливим, незалежно від методики перехоплення. Маються на увазі будь-які методи, включаючи такі, як контроль оператора, пасивний перехоплення в зоні телефону, активне перехоплення з перемиканням телефону на помилкову базу і т.д. Всі ці способи прослуховування будуть марними, якщо ви та ваш співрозмовник увімкнули режим кодування. Потрібно враховувати, щоб абонент на іншому боці мав аналогічний прилад. Коди шифрування інформації в обох приладах мають співпадати.

Технічні характеристики:

— максимальна дальність зв'язку між блоком ms та телефоном до 3 метрів;

— мінімальна відстань між блоком ms та мобільним телефоном від 0,5 метра;

— максимальний час заряду li-ion акумулятора до 10 годин;

— час роботи блоку ms із повністю зарядженим акумулятором до 8 годин.

Досить невисока вартість скремблера дозволяє створити мережу серед постійних партнерів або всередині корпоративної верхівки для ведення повністю закритих переговорів у межах цієї мережі.

Скремблер Avantalk реалізований у вигляді Bluetooth-гарнітури та підключається до відповідного смартфона за допомогою Bluetooth. При підключеному скремблер розмова ведеться через вбудований мікрофон. Коли ви додзвонилися до Вашого співрозмовника, один із вас включає режим кодування. Протягом кількох секунд Ваші пристрої обмінюватимуться первинними даними та встановлюватимуть зв'язок. Після встановлення зв'язку загориться відповідний світлодіод, що підтверджує входження в «захищений режим». Після цього Ви можете спокійно розмовляти на таємні теми.

Голос співрозмовника у режимі скремблювання дещо спотворюється. Це нормально, оскільки сигнал проходить багаторазову обробку і потім

передається відносно низькоякісним GSM-каналом. Створюваний дискомфорт не можна порівняти з важливістю забезпечення конфіденційності. Для покращення розуміння говоріть повільно та розбірливо, а також використовуйте навушники.

Бездротовий скремблер «Guard Bluetooth» — це надійний пристрій для захисту інформації під час переговорів по мобільному телефону. Скремблер шифрує мова методом частотної інверсії, після чого сигнал відправляється каналом стільникового зв'язку співрозмовнику. Другий абонент з аналогічним приладом отримує зашифроване мовлення, яке дешифрується його скремблером. За такого принципу спілкування, навіть якщо канал зв'язку буде перехоплено або зловмиснику вдасться отримати записи у провайдера, зрозуміти суть розмови не вдасться, оскільки відсоток розбірливості не перевищує від 3 до 5%.

Для підключення скремблер використовується Bluetooth канал, що звільняє від необхідності використовувати дроти та кабелі, даючи можливість користуватися пристроєм у будь-якому місці.

Особливості:

— при несанкціонованому підключенні до телефону або каналу зв'язку, третій особі вдасться розібрати не більше 3 - 5% мовного потоку

— можливість вибору одного з чотирьох режимів шифрування, залежно від умов, за яких здійснюється розмова.

— підключення скрімблера до телефону через Bluetooth.

— метод частотної інверсії забезпечує високий рівень надійності шифрування.

— наявність роз'єму для підключення навушників jack 3,5'.

— як джерело живлення використовується змінна батарея типу «Крона» 9В.

ВИСНОВКИ

Отож, можна зробити висновок, що виходячи зі сказаного вище, актуальність використання ПВБП присутня для таких сфер використання як діагностування електронних схем, шифрування, можна зробити висновок що проблеми їх генерації є актуальними на сьогоднішній день. А саме,синтез псевдовипадкових тестових послідовностей є важливим у сфері ймовірнісного тестування. В нинішній час в новій техніці тестування цифрових схем найбільш часто використовується цифрове скремблювання.

Бакалаврський дипломний проект присвячений аналізе застосування моделей цифрових скремблерів та побудови лінійних автоматів на їх основі.

У теоретичній частині роботи проведено огляд процесу цифрового скремлювання. Дано короткий опис задач скремблювання, та характеристика процесу скремлювання..

Другий розділ присвячений реалізації скремблювання та дескремлювання. Розглянуто різні види скремблерів, наведено їх класифікацію та реалізацію двох видів скремблювання.

У третьому розділі детально розглянуті програмні продукти для скремблювання сигналу. Наведено приклади апаратів для скремлювання .

ПЕРЕЛІК ДЕЖЕРЕЛ ПОСИЛАННЯ

1. Скремблер — [Електронний ресурс]. URL: https://ru.wikipedia.org/wiki/Скремблер

2. Telecommunications Industry Association Standard. IP over Satellite (IPOS). Revision of TIA-1008-A. — USA, May 2006. — pages 247.

3. Іхсанов Ш. М. Методичні вказівки для вивчення теорії та виконання лабораторних робіт з дисципліни «Адаптивна обробка сигналів». — НУК, кафедра теоретичної електротехніки та електронних систем, 2017. — 69 с.

4. Klein A. Attacks on the RC4 stream cipher. / A. Klein. Designs, Codes and Cryptography — 286 c

5. Oversby L. 21 Scrambler/ L. Oversby — M.: Ardis Publishing , 2002. — C. 78. — 156 c.

6. M. Liskov. Tweakable Block Ciphers. Advances in Cryptology – CRYPTO 2002 Proceedings/ M. Liskov, R. Rivest, D. Wagner. Springer-Verlag, 2002. – pp. 31-46.

7. Алгоритм SQ1-R – Режим доступу: http://crypto.pp.ua/2011/02/sq1-r/.

8. Бродин В. Б. Системы на микроконтролерах и БИС программируемой логики / В. Б. Бродин, А. В. Калинин. – М.: Издательство Эком, 2002. – 400 с.

9. Использование интерфейса SPI в мікросхемах – Режим доступа: http://chipspace.ru/stm32-spi/.

10. Асосков А. В. Поточные шифры. / А. В. Асосков, Иванов, А. А. Мирский, А. В. Рузин, А. В. Сланин, А. Н. Тютвин. — КУДИЦ, 2003. — 336с.

11. Потокові шифри. Результати зарубіжної відкритої криптології. Режим доступу до статті: http://www.ssl.stu.neva.ru/psw/crypto.html.

ДОДАТОК А

Технічне завдання

Міністерство освіти і науки України

Вінницький національний технічний університет

Факультет інформаційних технологій та комп’ютерної інженерії

Кафедра обчислювальної техніки

ЗАТВЕРДЖУЮ

Завідувач кафедри ОТ

проф., д.т.н.. Азаров О.Д..

" " 2022 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання бакалаврської дипломної роботи

“Цифрові скремблери на основі лінійних автоматів ”

08-23.БДР.029.00.000 ТЗ

Науковий керівник: доцент к.т.н.

_____ Семеренко В. П.

Студент групи 2КІ-18б

_____ Салата О. Л.

м. Вінниця – 2022

1 Підстава для використання бакалаврської кваліфікаційної роботи (БДР)

1.1 Актуальність обраної теми є розвитком систем зв’язку з якої витікає проблема захисту інформації від різних ризиків, а також проблема діагностування цифрової апаратури.

1.2 Наказ про затвердження теми бакалаврської дипломної роботи.

2 Мета і призначення БДР

2.1 Мета проекту — є всебічний аналіз застосування моделей цифрових скремблерів та побудови лінійних автоматів на їх основі.

2.2 Призначення розробки — виконання програмної та апаратної реалізації скремблерів.

3 Вихідні дані для виконання БДР

3.1 Проведення математичного аналізу.

3.2 Розгляд принципів роботи скремблерів.

3.2 Розробка програмної реалізаціх скремблерів.

4 Вимоги до виконання БДР

Головна вимога — проаналізувати скремблювання та дескремблювання.

5 Етапи БДР та очікувані результати

Етапи роботи та очікувані результати приведено в Таблиці А.1.

6 Матеріали, що подаються до захисту БДР

До захисту подаються: пояснювальна записка БДР, ілюстративні матеріали, протокол попереднього захисту БДР на кафедрі, відгук наукового керівника, анотації до БДР українською та іноземною мовами, довідка про відповідність оформлення БДР діючим вимогам.

Таблиця А.1 — Етапи БДР

№ з/п	Назва етапів виконання комплексної бакалаврської роботи	Строк виконання етапів роботи	Примітка
1	Постановка задачі роботи	09.03.22	Розділ 1
2	Аналіз предметної області	10.03-18.03.22	Розділ 1
3	Аналіз характеристик скремблювання	21.03-31.03.22	Розділ 1
4	Аналіз завадостійкості кодування в МЗ	05.04-13.04.22	Розділ 2
5	Огляд математичних апаратів лінійних автоматів	14.04-22.04.22	Розділ 2
6	Програмно-апаратна реалізація скремблерів	25.04-.06.05.22	Розділ 3
7	Програмна реалізація скремблерів	09.05-13.05.22	Розділ 3
8	Апаратна реалізація скремблерів	17.05-22.05.22	Розділ 3
9	Підготовка матеріалів та опис розробки інформаційної системи	23.05-26.05.22	Пояснювальна записка
10	Аналіз виконання роботи, висновки, додатки	27.05-31.05.22	Пояснювальна записка
11	Перевірка якості виконання бакалаврського проекту та усунення недоліків	02.06 -.17.06.22	Пояснювальна записка

7 Порядок контролю виконання та захисту БДР

Виконання етапів графічної та розрахункової документації БДР контролюється науковим керівником згідно зі встановленими термінами. Захист БДР відбувається на засіданні Екзаменаційної комісії, затвердженої наказом ректора.

8 Вимоги до оформлювання та порядок виконання БДР

При оформлюванні БДР використовуються:

— ДСТУ 3008 : 2015 «Звіти в сфері науки і техніки. Структура та правила оформлювання»;

— ДСТУ 8302 : 2015 «Бібліографічні посилання. Загальні положення та правила складання»;

— ГОСТ 2.104-2006 «Єдина система конструкторської документації. Основні написи»;

— документами на які посилаються у вище вказаних.

ДОДАТОК Б

Лістинг програми

```
// Функция для скремблирования одного байта информации:
unsigned char SCR(unsigned char byte, bool begin)
// begin - признак скремблирования и дескремблирования
// с начальным значением регистра
{ // Параметры скремблера:
 unsigned char genpoly[2];// порождающий полином (номера
 // ненулевых элементов)
 unsigned int initseq; // инициализирующая последовательность
 static int reg;
 unsigned char i,j,genb,inb,outb;
 unsigned char outbyte;
 initseq=0xFFFFE;
 genpoly[0]=2; genpoly[1]=19;
 begin=true;
 if(begin)
 { reg=initseq;
 begin=false;
 }
 outbyte=0;
 for(i=0;i < 8;i++)
{ genb=0;
 for(j=0;j < 2;j++)
 genb^=(reg>>genpoly[j])&1;
 inb=(byte>>i)&1;
 outb=!inb^genb;
 outbyte|=outb<<i;
 reg=(reg<<1)|outb;
```

```
 }
 return outbyte;
}
// Функция для дескремблирования одного байта информации:
char deSCR(char byte, bool begin)
{ static int reg;
 char i,j,genb,inb,outb;
 char outbyte;
 if(begin)
 { reg=initseq;
 begin=false;
 }
 outbyte=0;
 for(i=0;i < 8;i++)
 { genb=0;
 for(j=0;j < 2;j++)
 genb^=(reg>>genpoly[j])&1;
 inb=(byte>>i)&1;
 outb=!inb^genb;
 outbyte|=outb<<i;
 reg=(reg<<1)|inb;
 }
 return outbyte;
}
```

ДОДАТОК В

ПРОТОКОЛ ПЕРЕВРКИ ДИПЛОМНОЇ РОБОТИ НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: цифрові скремблери на основі лінійних автоматів

Тип роботи: бакалаврська дипломна робота

Підрозділ кафедра обчислювальної техніки

Показники звіту подібності Unicheck

Оригінальність 91,3% Схожість 8,7%

Аналіз звіту подібності (відмітити потрібне):

- ✓ Запозичення, виявлення у роботі, оформлені коректно і не містять ознак плагіату.
- □ Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.
- □ Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа, відповідальна за перевірку _____ Захарченко С.М.

Ознайомлені з повним звітом подібності, який був згенерований системою Unicheck що до роботи.

Автор роботи _____ Салата О.Л.

Керівник роботи _____ Семеренко В.П.