Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА

## Пояснювальна записка

рівень вищої освіти другий (магістерський)

Використання систем безпеки у GSM каналах

(тема)

Виконав:
студент 6 курсу, групи: ІМІм-22-1

Заєць М. Ю.
(прізвище, ініціали)

Спеціальність: 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)

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

Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник: доцент кафедри ІМІ Скорик Ю. В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри

(підпис) (прізвище, ініціали)

2024 р.

Не містить відомостей заборонених до відкритого публікування.

Студент _____ /М.Ю. Заєць/

Керівник _____ /Ю.В. Скорик/

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інформаційно-мережної інженерії
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації та радіотехніки
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри _____
(підпис)
«____» _____2023р.

# ЗАВДАННЯ

## НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Зайцю Максиму Юрійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: *Використання систем безпеки в GSM каналах затверджена наказом по університету від «23» жовтня 2023року № 1233.*
2. Термін подання студентом роботи до екзаменаційної комісії 18.01.2024.
3. Вихідні дані до роботи: *вимоги стандарту Технологія GSM; кластерна структура; структура GSM: SIM, BTS, BSC, MSC, OMC, EIR, VLR, HLR, AUC, Abis, Um, ISDN, NSS, BSS, MSS, IMEI, RAND, DCN; механізми безпеки: алгоритми A3, A8, A5/(1,2,3), COMP128, структура LFSR; код та структура "метелика" COMP-128-1; Шифрування тафіку: пакет 114 біт, COUNT, TDMA, FN, регістри R1, R2, R3; атака на алгоритми: лінійний вираз, бінарні заміни, початковий внутрішній стан регістрів, тактування регістрів.*
4. Перелік питань, що потрібно опрацювати в роботі:
*1. Огляд технології GSM*
*2. Принципи безпеки GSM*
*3. Аналіз безпеки в GSM*

5. Перелік табличного та графічного матеріалу із зазначенням порівнянь, плакатів, комп'ютерних ілюстрацій: *демонстраційний матеріал у вигляді ppt-презентації; (Архітектура та структура GSM; Структура алгоритмів COMP-128, A3, A5, A8; Код та структура метелика в COMP-128-1, Шифрування даних, циклічна та нециклічна зміна частоти; Висновки).*

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів роботи | Термін виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Ознайомлення із завданням. Уточнення ТЗ* | *23.10.23* | *виконано* |
| 2 | *Підбір літератури за темою роботи* | *24.10-31.10.23* | *виконано* |
| 3 | *Виконання розділу 1* | *01.11-1.12.23* | *виконано* |
| 4 | *Виконання розділу 2* | *02.12-20.12.23* | *виконано* |
| 5 | *Виконання розділу 3* | *21.12-10.01.24* | *виконано* |
| 6 | *Оформлення пояснювальної записки* | *11.01-14.01.24* | *виконано* |
| 7 | *Оформлення презентаційного матеріалу* | *15.01-17.01.24* | *виконано* |

Дата видачі завдання *23 жовтня 2023р.*

Студент _____ Заєць М.Ю.

(підпис)

Керівник роботи _____ доц. Скорик Ю. В.

(підпис) (посада, прізвище)

# РЕФЕРАТ

Пояснювальна записка: 61с., 17 рис., 3 табл., 25 джерел.

Об'єкт роботи – канали безпеки GSM мережі.

Мета роботи – аналіз алгоритмів шифрування, аутентифікації та генерації ключів; знаходження можливих вразливостей.

Описано процес створення та переваги мережі GSM. Розглянуто архітектуру системи, включаючи мобільні, базові станції та мережеву підсистему, а також розкрито принципи роботи різних підсистем.

Розібрано алгоритм A5, який поділяється на різні версії, такі як A5/0, A5/1 та A5/2, розкрито принципи їхньої роботи. Особлива увага приділена атакам на криптографічний алгоритм COMP128 та ризикам, пов'язаним з фізичним доступом до SIM-карт.

Детально проаналізовано атаку на мережу GSM. Розглянуті методи виявлення ключа шифрування та зменшення витрат для отримання ключа. Подано аналіз двох атак, які забезпечують компроміс між робочим часом і пам'яттю проти A5/1, а також розглянуто кореляційні атаки, використовуючи статистичні залежності між послідовностями ключових потоків та регістрами зсуву. Робота дозволяє зрозуміти вразливості мережі GSM та ризики, пов'язані з її шифруванням та безпекою.

GSM МЕРЕЖА, АНАЛІЗ БЕЗПЕКИ, СТРУКТУРА МЕТЕЛИКА, АЛГОРИТМИ БЕЗПЕКИ, ШИФРУВАННЯ КАНАЛІВ, КОРЕЛЯЦІЙНІ АТАКИ, ВИЗНАЧЕННЯ ЗНАЧЕНЬ БІТІВ КЛЮЧОВОГО ПОТОКУ.

# ABSTRACT

Explanatory note: 61 p., 17 figures, 3 tables, 25 references.

The object of the work is the security channels of the GSM network.

The aim of the study is to analyse encryption, authentication and key generation algorithms and identify possible vulnerabilities.

The process of creation and advantages of GSM network are described. The system architecture including mobile, base station and network subsystems is reviewed and the principles of operation of various subsystems are disclosed.

The A5 algorithm, which is subdivided into different versions such as A5/0, A5/1 and A5/2, is analysed and the principles of their operation are disclosed. Special attention is paid to attacks on the COMP128 cryptographic algorithm and the risks associated with physical access to SIM cards.

The attack on GSM network is analysed in detail. Methods for discovering the encryption key and reducing the cost of obtaining it are considered. Two attacks that provide a trade-off between runtime and memory versus A5/1 are analysed, and correlation attacks using statistical dependencies between key stream sequences and shift registers are considered. The work provides insight into the vulnerabilities of the GSM network and the risks associated with its encryption and security.

GSM NETWORK, SECURITY ANALYSIS, BUTTERFLY STRUCTURE, SECURITY ALGORITHMS, CHANNEL ENCRYPTION, CORRELATION ATTACKS, DETERMINATION OF KEY STREAM BIT VALUES.

# ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ

GSM – Global System for Mobile

CEPT – Conference of European Post and Telecommunications

SMS – Short Message Service

GPRS – General Packet Radio Service

ISDN – Integrated Services Digital Network

BTS – Base Transceiver Station

BSC – Base Station Controller

MSC – Mobile Switching Center

HLR – Home Location Register

VLR – Visited Location Register

AuC – Authentication Centre

TMSI – Temporary Mobile Subscriber Identity

IMSI – International Mobile Subscriber Identity

LAI – Location Area Identity

EIR – Equipment Identity Register

PIN – Personal Identification Number

BSS – Base Station Subsystem

NSS – Network Subsystem

PSTN – Public Switched Telephone Network

LAN – Local Area Network

DCN – Data Communications Network

SRES – Signed Response

LFSR – Linear Feedback Shift Register

# Вступ

GSM - найпоширеніша у світі система мобільного зв'язку. Згідно з нещодавнім прес-релізом Асоціації GSM, 55 відсотків населення світу, або близько 4,3 мільярда людей, мають смартфони. За їхніми даними, існує 4,6 мільярда користувачів мобільного інтернету, 4 мільярди з яких отримують доступ до послуг через свої смартфони [1].

Для GSM, як і для багатьох інших широко використовуваних систем, безпека має першорядне значення. Однак багато цінних аспектів GSM виявилися вразливими до атак: Анонімність користувачів GSM скомпрометована, і зловмисники можуть спостерігати час, швидкість, тривалість, джерело і пункт призначення. Можна навіть відстежувати переміщення абонентів. Автентифікація є важливим фактором у системах бездротового зв'язку, оскільки природа середовища - бездротовий зв'язок - робить його доступним для всіх, а не лише для законних суб'єктів. Навіть механізми автентифікації вразливі до атак.

Найбільш очевидною загрозою для систем зв'язку є прослуховування: GSM-розмови захищені певними версіями алгоритму A5. Ці алгоритми мають деякі вражаючі атаки криптоаналізу, які можуть зламати шифрування і дозволити прослуховування в реальному часі. Однак більшість з цих алгоритмів важко використовувати на практиці, оскільки вони вимагають значних обчислювальних потужностей. Той факт, що GSM-дзвінки важко перехоплювати за допомогою атак криптоаналізу, не означає, що вони належним чином захищені. Прогалини в протоколах, що використовуються в GSM, означають, що будь-яка неавторизована особа, яка має доступ до достатнього обладнання, може підслуховувати дзвінки в режимі реального часу. Враховуючи ці загрози і вразливості, виникає питання, чи забезпечує GSM належний рівень безпеки для користувачів, які передають конфіденційну інформацію. До таких користувачів можуть належати військові організації та керівники великих компаній. Слід зазначити, що поточна модель безпеки GSM не забезпечує належного захисту для таких організацій.

# 1 ОГЛЯД ТЕХНОЛОГІЇ GSM

## 1.1 Особливості GSM

Глобальна система мобільного зв'язку (GSM) - найпоширеніша у світі система мобільного зв'язку; назва GSM походить від назви Конференції європейських поштових і телекомунікаційних адміністрацій (CEPT), створеної в 1982 році з метою розробки загальноєвропейської системи мобільного зв'язку для заміни багатьох інших несумісних систем, що вже існували. Однак, коли послуги GSM були запущені в 1991 році, абревіатура GSM була змінена на Глобальну систему мобільного зв'язку (Global System for Mobile Communications), розроблену компанією Group Special Mobile.

GSM є набагато кращою системою, ніж стара аналогова система; основні особливості GSM можна підсумувати наступним чином:

— Міжнародний роумінг, єдиний абонентський номер по всьому світу;

— Вища якість голосу, краща, ніж у сучасних аналогових технологій мобільного зв'язку;

— Високий рівень безпеки, інформація користувача надійно захищена;

— Універсальні та недорогі мобільні телефони;

— Цифрова зручність, вдвічі більше часу для розмов на одному заряді;

— Нові послуги, очікування виклику, переадресація, служба коротких повідомлень (SMS), GSM;

— Пакетні радіопослуги (GPRS);

— Цифрова інтероперабельність, легка взаємодія з існуючими цифровими мережами, такими як ISDN [3].

## 1.2 Архітектура GSM

Мережа GSM поділяється на три частини. Мобільні станції зв'язуються з абонентами, підсистема базової станції контролює радіозв'язок з

мобільними станціями, а мережева підсистема, важливою частиною якої є мобільний комутаційний центр, перемикає дзвінки між мобільними станціями та іншими користувачами фіксованої або мобільної мережі, а також керує мобільними послугами, такими як аутентифікація. Мобільні та базові станції зв'язуються через радіоканали. Підсистему базової станції та мережеву підсистему також називають фіксованою мережею.

Мобільний зв'язок означає, що існує багато різних систем і пристроїв зв'язку, включаючи антени і базові станції. Якщо потужність антени базової станції висока, вона покриває велику площу. І навпаки, якщо потужність антени низька, це означає, що покривається лише невелика територія. Однак є й інші параметри, які впливають на збіжність. Наприклад, для хорошого зв'язку в перевантажених районах необхідно зменшити конвергенцію і збільшити пропускну здатність каналу.

Багато сусідніх стільників утворюють кластери. Кластер може складатися з різної кількості стільників, кожен з яких використовує свою частоту, щоб уникнути інтерференції. Такі кластерні структури повторюються в різних зонах зв'язку.

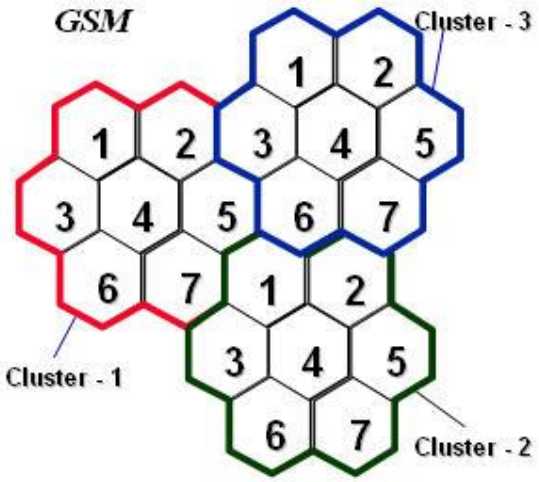


Рисунок 1.1 – Кластерна структура GSM

Як видно з рис. 1.1, різні стільники в кластері знаходяться далеко один від одного, тому вони не взаємодіють один з одним і можуть використовувати одну і ту ж частоту.

На рис. 1.2 показано кожен пристрій у системі GSM. Розглянемо кожен з них більш детально [4, 5].

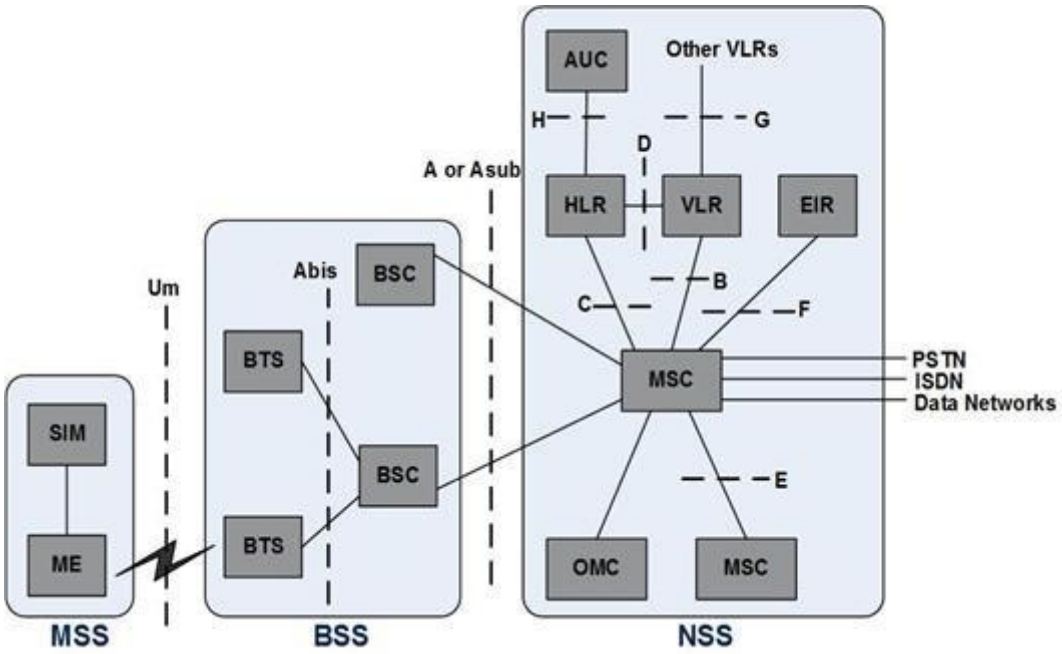


Рисунок 1.2 – Структура GSM

SIM-карти (модулі ідентифікацій абонента). Це залежні від оператора смарт-картки, що містять алгоритми A3/8, IMSI та Ki.

Мобільне обладнання (МО) – незалежний від оператора пристрій зв'язку. Містить алгоритм A5. Без SIM-карти не працює. Він ніколи не бачить алгоритми A3/8 та Ki

Базова станція (BTS) - базова станція, що належить до PLMN, яка надає послуги абоненту. BTS утворюють мережу радіоточок у межах певної географічної зони покриття. Базові станції підключені до контролера базової станції (BSC).

Контролер базової станції (BSC). Це вузол, який керує кількома BTS, координує хендовери і виконує координацію некомутаційних дій БС. Зв'язок від BSC до BTS зазвичай здійснюється за допомогою мікрохвильового каналу "точка-точка". BSC також підключені до мобільних центрів комутації (MSC) за допомогою фіксованих або мікрохвильових ліній зв'язку.

Мобільний комутаційний центр (MSC). Це вузол, який контролює ряд BSC; це центральний пристрій, який виконує багато функцій системи GSM. Він виконує комутацію, аутентифікацію та реєстрацію, а також з'єднує вузли між собою. Він підключений до телефонної мережі загального користування.

Домашній реєстр місцезнаходження (HLR). Використовується для реєстрації останнього відомого місцезнаходження всіх мобільних телефонів,

що належать до домашньої зони оператора. Цей реєстр містить всю адміністративну інформацію про кожного користувача, зареєстрованого в мережі GSM, а також поточне місцезнаходження мобільного телефону.

Реєстр відвіданих місцезнаходжень (VLR). Використовується для запису інформації про те, коли всі MS перебувають у "відвіданій" зоні. Він відстежує мобільні телефони, які знаходяться за межами домашньої мережі, дозволяючи мережі знати, де вони знаходяться.

Центр автентифікації (AuC) використовується HLR для генерації випадкового пошуку (RAND) і зберігання інформації про секретний ключ (Ki), пов'язаної з кожною MS. AuC може бути інтегрований з іншими мережевими функціями, такими як HLR. База даних AUC включає міжнародний ідентифікатор мобільного абонента (IMSI), тимчасовий ідентифікатор мобільного абонента (TMSI), ідентифікатор зони розташування (LAI) і ключ автентифікації (Ki).

Ідентифікаційний реєстр обладнання (EIR) EIR - це база даних, яка відстежує телефони в мережі за допомогою IMEI, і існує лише один EIR на мережу. Він складається з трьох списків: білого, сірого та чорного. Чорний список - це список IMEI, які мережа відмовляється обслуговувати з певних причин. Ці причини включають в себе те, що IMEI був зареєстрований як викрадений або клонований, телефон несправний або не має технічної можливості працювати в мережі. Сірий список - це список IMEI, які слід відстежувати на предмет підозрілої поведінки. Сюди можуть входити телефони, які поводяться дивно або не працюють належним чином у мережі. Білий список - це порожній список. Це означає, що якщо IMEI не знаходиться ні в чорному, ні в сірому списку, він вважається безпечним і потрапляє до "білого списку".

## 1.3 Підсистеми та принципи роботи

Структура GSM складається з підсистем: підсистеми базової станції, підсистеми мережі та підсистеми управління мережею. Крім того, є три інтерфейси: UM, Abis (між BTS і BSC) і A (між BSC і MSC) [2].

Мобільні станції. Всі мобільні телефони стандарту GSM обладнані модулем ідентифікації абонента (SIM) SIM-карта забезпечує унікальну

ідентифікацію мобільного телефону за допомогою міжнародного стандарту ідентифікації мобільних абонентів (IMSI) SIM-карта не дає мобільному телефону працювати, це як ключ. Вона може зберігати особисті телефонні номери та текстові повідомлення, а також інформацію, пов'язану з безпекою, таку як алгоритм автентифікації A3, алгоритм генерації ключів шифрування A8, ключ автентифікації (Ki) та IMSI. Мобільні станції зберігають алгоритм шифрування A5; SIM-карти можуть бути захищені персональним ідентифікаційним номером (PIN), обраним абонентом; PIN зберігається на картці, і якщо його ввести неправильно тричі, картка блокується.

Підсистема базової станції (BSS). Її завданням є з'єднання користувачів мобільного зв'язку з іншими користувачами фіксованого або мобільного зв'язку. Базова приймально-передавальна станція (BTS) безпосередньо контактує з мобільним телефоном через повітряний інтерфейс і може вважатися вдосконаленим радіомодемом. Контролер базової станції (BSC) відповідає за управління кількома BTS. Він відстежує кожен дзвінок, вирішує, коли перевести дзвінок з однієї BTS на іншу, і управляє радіочастотами, виділеними для дзвінків в BTS [3].

Мережева підсистема (NSS). Це повноцінна АТС, здатна маршрутизувати дзвінки з фіксованої мережі на іншу мобільну станцію через BSC і BTS. Мобільний комутаційний центр (MSC) з'єднує стільникову мережу з телефонною мережею загального користування (PSTN).

MSC також відповідає за координацію налаштування дзвінків до і від користувачів GSM. Реєстр домашнього місцезнаходження (HLR) зберігає інформацію про всіх абонентів, що належать до зони обслуговування MSC. HLR зберігає постійні дані, такі як IMSI, послуги, на які підписаний користувач, номери мережі загального користування, Ki та інші тимчасові дані. HLR повинен надавати всю необхідну інформацію до MSC, коли надходить виклик з ТфОП. Реєстр місцезнаходження абонента (VLR) містить відповідну інформацію для всіх мобільних телефонів, що обслуговуються в MSC; постійні дані, що зберігаються в VLR, також зберігаються в HLR. Крім того, зберігається тимчасовий ідентифікатор мобільного абонента (TMSI). Якщо виклик надходить з мобільної станції, VLR повинен підтримувати MSC під час встановлення виклику та аутентифікації. реєстрація ідентифікації обладнання (EIR) EIR підтримує білі, сірі та чорні списки. Користувачам,

внесеним до білого списку, дозволяється користуватися мережею, тоді як користувачам, внесеним до чорного списку, доступ до мережі заборонено. Сірий список складається з несправного обладнання, яке може спричинити проблеми в мережі, але все ще може працювати в мережі. IMEI вказує на серійний номер мобільної станції, виробника, схвалення типу та країну-виробника. Центр автентифікації (AuC) - це захищена база даних, що містить CI, алгоритми автентифікації A3, алгоритми шифрування A5 та алгоритми генерації ключів шифрування A8. Він відповідає за генерацію наборів випадкових чисел (RAND), підписаних відповідей (SRES) і ключів шифрування (KC), а згенеровані набори зберігаються в HLR і VLR [3].

Підсистема управління мережею (NMS). На додаток до підсистеми комутації мережі (NSS) і підсистеми базових станцій (BSS), це третя підсистема мережі GSM. Робоча станція оператора з'єднана з базою даних і сервером зв'язку через локальну мережу (LAN). Сервер бази даних зберігає управлінську інформацію про мережу. Сервер зв'язку відповідає за зв'язок між NMS і так званими "мережевими елементами" в мережі GSM.

Цей зв'язок відбувається через мережу передачі даних (DCN), яка підключена до NMS через маршрутизатор; DCN зазвичай реалізується за допомогою мережі з комутацією пакетів.

Функції NMS можна розділити на три категорії: управління несправностями, управління конфігурацією та управління продуктивністю [6].

# 2 ПРИНЦИПИ БЕЗПЕКИ GSM

## 2.1 Механізми безпеки

GSM має низку систем захисту для безпечного зв'язку. Вони включають багато різних типів алгоритмів і різних типів пристроїв.

Основні аспекти безпеки GSM можна звести до чотирьох принципів:

— Аутентифікація дозволяє мобільним пристроям доводити, що вони мають доступ до певного облікового запису в оператора;

— Всі сигнали і дані користувача (наприклад, текстові повідомлення і голос) повинні бути захищені від прослуховування за допомогою шифрування;

— Для гарантування безпеки, IMSI рідко використовується для GSM-зв'язку, а TMSI (Тимчасовий ідентифікатор мобільного абонента) - для забезпечення більш безпечного зв'язку та уникнення розкриття особи користувача. Це означає, що той, хто перехоплює зв'язок, не повинен знати, чи перебуває конкретний мобільний користувач у даній місцевості, чи ні;

— Використання SIM-карт як модуля безпеки: Навіть якщо SIM-карту викраде ворог, він зможе зчитати PIN-код.

## 2.2 Алгоритми A3 та A8

Алгоритми A3 і A8 є симетричними алгоритмами, в яких для шифрування і розшифрування використовується один і той же ключ. Обидва алгоритми є односторонніми функціями: вихід можна знайти, якщо відомий вхід, але майже неможливо знайти вхід, якщо відомий вихід. Алгоритми A3 і A8 зберігаються і реалізуються на SIM-карті.

Сам мобільний телефон не пов'язаний з конкретною мережею, коли SIM-карта вставляється в мобільний телефон, вибирається відповідний мережевий обліковий запис. Таким чином, SIM-карта містить всі дані, необхідні для доступу до певного облікового запису: IMSI, алгоритми Ki, A3 і A8 [9].

IMSI (International Mobile Subscriber Identity): це унікальний номер для всіх абонентів у всьому світі. Він містить інформацію про домашню мережу

абонента та країну видачі. Цю інформацію можна зчитати з SIM-картки, якщо вона доступна на місці (зазвичай захищена простим PIN-кодом); IMSI - це десяткове число до 15 цифр, перші п'ять або шість з яких ідентифікують мережу і країну.

Кореневий ключ шифрування. Це випадково згенероване 128-бітне число, яке присвоюється конкретному абоненту і використовується для генерації всіх ключів і дзвінків, що використовуються в системі GSM; Ki є дуже захищеним і відомий лише SIM-картці та Центру аутентифікації мережі (AuC). Сам мобільний телефон не знає Ki, він лише надсилає на SIM-карту інформацію, необхідну для аутентифікації та генерації ключів шифрування.

Аутентифікація та генерація ключів відбувається всередині SIM-карти, що можливо завдяки тому, що SIM-карта є інтелектуальним пристроєм з мікропроцесором.

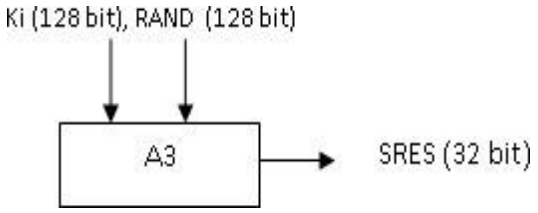


Рисунок 2.1 – Алгоритм A3

Алгоритм A3 автентифікує користувачів, коли вони мають привілеї на доступ до системи. Для автентифікації абонентів мережа використовує метод "запит-відповідь".

У цьому алгоритмі 128-бітне випадкове число (RAND) надсилається через повітряний інтерфейс на мобільну станцію; RAND надсилається на SIM-карту і разом з KI передається алгоритму аутентифікації A3.

Підписана відповідь (SRES), результат роботи алгоритму A3, надсилається з мобільної станції в мережу через повітряний інтерфейс. У мережі AuC порівнює значення SRES зі значенням SRES, отриманим від мобільної станції. Якщо обидва значення SRES збігаються, автентифікація є успішною і абонент приєднується до мережі. На практиці AuC не зберігає копію SRES, а запитує її у HLR або VLR, коли це необхідно [3].

На рис. 2.2 показано послідовність запитів між мобільною станцією і мережею оператора в алгоритмі A3. Цю схему можна представити наступним чином:

1. Здійснюється спроба встановити з'єднання між телефоном і мережею.

2. Телефон надсилає свої облікові дані. Всі потенційні повідомлення, що використовуються на початку з'єднання, містять поле ідентифікації. Якщо можливо, уникайте надсилання IMSI у вигляді простого тексту (щоб слухач не знав, що конкретний абонент намагається встановити з'єднання). Замість цього використовуйте TMSI (тимчасовий ідентифікатор мобільного абонента). Це пояснюється нижче.

3. Мережа надсилає повідомлення AUTOMATION REQUEST, що містить RAND.

4. Телефон отримує RAND і надсилає його на SIM-карту за допомогою команди RUN GSM ALGORITHM.

5. SIM-карта виконує алгоритм A3 і надсилає SRES назад на телефон.

6. Телефон надсилає SRES до мережі у повідомленні AUTHENTICATION RESPONSE (відповідь на перевірку автентичності).

7. Мережа порівнює SRES з власним SRES. Якщо вони збігаються, операція може бути продовжена. В іншому випадку мережа вирішує, чи повторити процедуру автентифікації або повернути повідомлення AUTOMATICATION REJECT, якщо використовувався TMSI [9].

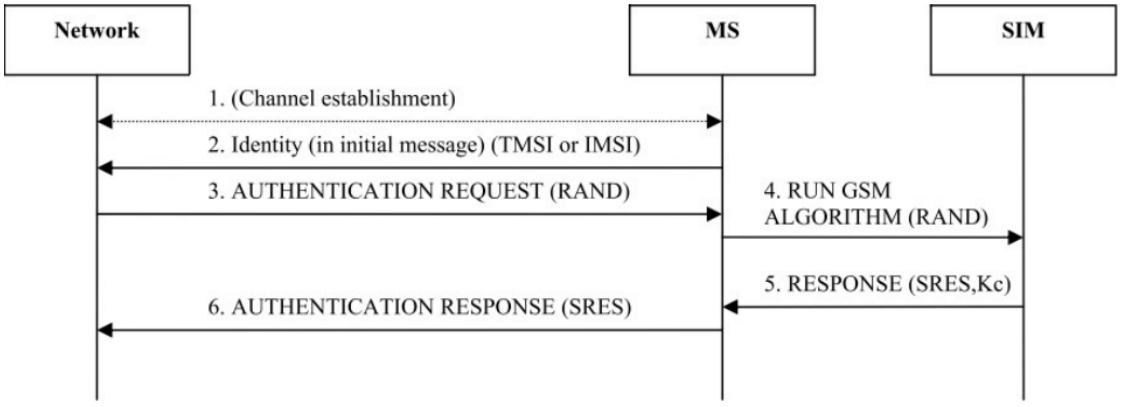


Рисунок 2.2 – Алгоритм запиту A3

Алгоритм A8 в GSM використовує криптографічні ключі для захисту як даних користувача, так і сигналів на вразливих повітряних інтерфейсах. Після авторизації користувача дані RAND (отримані з мережі) і Ki (отримані з SIM-карти) передаються алгоритму генерації криптографічних ключів A8, який генерує ключ шифрування (Kc). Алгоритм A8 зберігається на SIM-карті; Kc, згенерований алгоритмом A8, потім використовується з шифруванням A5 Алгоритм A5 реалізований в апаратному забезпеченні мобільного телефону, оскільки дані повинні шифруватися і розшифровуватися бездротовим способом.

Алгоритм A8 генерує 64-бітний ключ шифрування Kc, використовуючи RAND і Ki в якості вхідних даних, який зберігається на SIM-карті і зчитується мобільним телефоном. Мережа також генерує Kc і надсилає його на базову станцію (BTS), яка обробляє з'єднання. На рис. 2.3 показано, як працює алгоритм A8.

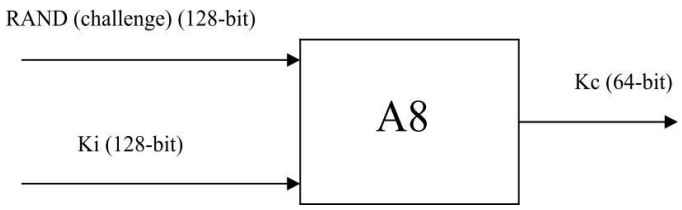


Рисунок 2.3 – Алгоритм A8

## 2.3 COMP128

COMP128 - це хеш-функція, яка реалізує алгоритми A3 і A8 стандарту GSM.

Algorithm Expert Group була створена в 1987 році і займалася розробкою алгоритмів шифрування GSM. Першим був COMP128 для аутентифікації та отримання ключа шифрування (A3/8), а другим - алгоритм A5. GSM дозволяє кожному оператору використовувати свій власний алгоритм A3/8 без перемикання між мережами, включаючи роумінг, і всі системи це підтримують. Однак більшість операторів не мають достатнього досвіду для розробки власного алгоритму A3/8 і використовують алгоритм COMP128 як приклад: COMP128 приймає RAND і Ki на вході і видає 128 біт на виході [12].

Перші 32 біти з 128 біт формують відповідь SRES, а останні 54 біти на виході COMP128 формують ключ сеансу Kc. Довжина ключа на цьому етапі становить 54 біти, а не 64 біти.

До ключа, згенерованого алгоритмом COMP128, додаються десять нульових бітів. Таким чином, 64-бітний ключ обнуляється, включаючи останні 10 біт. Це зменшує розмір ключа з 64 біт до 54 біт. Це робиться у всіх реалізаціях A8, включаючи ті, що не використовують COMP128 для генерації ключів, і, схоже, є навмисною особливістю реалізації A8 [13].

## 2.4 Алгоритм A5

A5 - це потоковий шифр, який може бути дуже ефективно реалізований на апаратному рівні. Існує декілька реалізацій цього алгоритму, найпоширенішими з яких є A5/0, A5/1 та A5/2 (A5/3 використовується в системах 3G). Причиною різних реалізацій є експортні обмеження на технології шифрування; A5/1 є найсильнішою версією і широко використовується в Західній Європі та США, в той час як A5/2 широко використовується в Азії. Країни, що перебувають під санкціями ООН, і деякі країни третього світу використовують A5/0, який не містить шифрування [14].

Як потоковий шифр, A5 працює побітно (а не поблочно, як DES або AES). Тому, якщо в зашифрованому тексті є помилка, то відповідний біт у відкритому тексті буде неправильним.

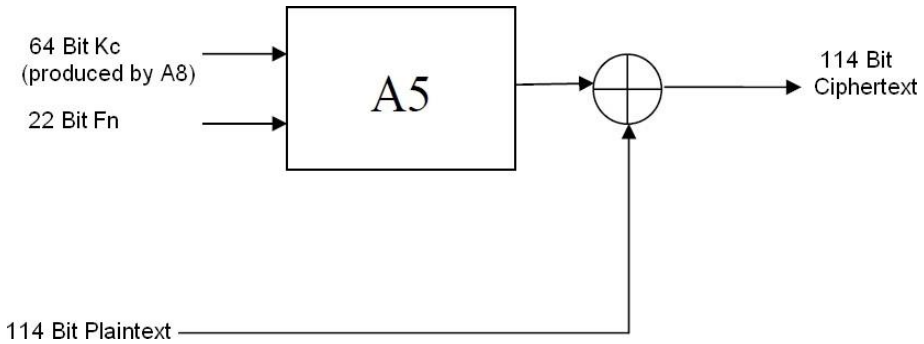


Рисунок 2.4 – Структура A5

Жоден з алгоритмів не опублікований Асоціацією GSM. Всі вони були відкриті за допомогою методів зворотного інжинірингу. Алгоритм A5/1 використовує структуру, показану на рис. 2.4 [9].

Kc - це ключ, отриманий алгоритмом A8; Plaintext - це дані, що передаються; Fn - це біти кадру, отримані в результаті операції LFSR (лінійний регістр зсуву зі зворотним зв'язком).

Як видно з рис. 2.4, у структурі LFSR є спеціальні біти (гілки) та певна кількість бітів. Ці спеціальні гілки виконують операцію XOR, зсуваючи всі біти на один біт вліво і поміщаючи результат в перший біт.

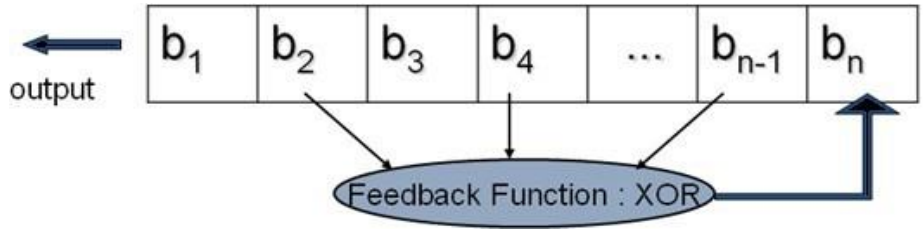


Рисунок 2.5 – Структура LFSR

В алгоритмі A5/1 структура LFSR використовує три біти регістра. Ці біти показані на рис. 2.5 [14].

A5/1 складається з трьох коротких лінійних регістрів зсуву зі зворотним зв'язком (LFSR) по 19, 22 і 23 біти, позначених R1, R2 і R3 відповідно. Крайній правий біт кожного регістра встановлено в нуль; вивід R1 знаходиться в бітових позиціях 13, 16, 17 і 18, вивід R2 - в бітових позиціях 20 і 21, а вивід R3 - в бітових позиціях 7, 20, 21 і 22. Коли регістр синхронізується, гілка виконує операцію XOR, і результат зберігається в крайньому правому біті зсунутого вліво регістра; три регістри синхронізуються в режимі Stop/Go згідно з наступним правилом більшості кожен регістр має "тактовий" ключ (R1 має біт 8, R2 має біт 10, R3 має біт 10) і для кожного такту обчислюється мажоритарна функція голосування тактового ключа, і тільки регістри, що відповідають мажоритарним бітам тактового ключа, фактично синхронізуються. Зауважте, що на кожному кроці тактуються два або три регістри, причому кожен регістр рухається з імовірністю 3/4 і зупиняється з імовірністю 1/4.

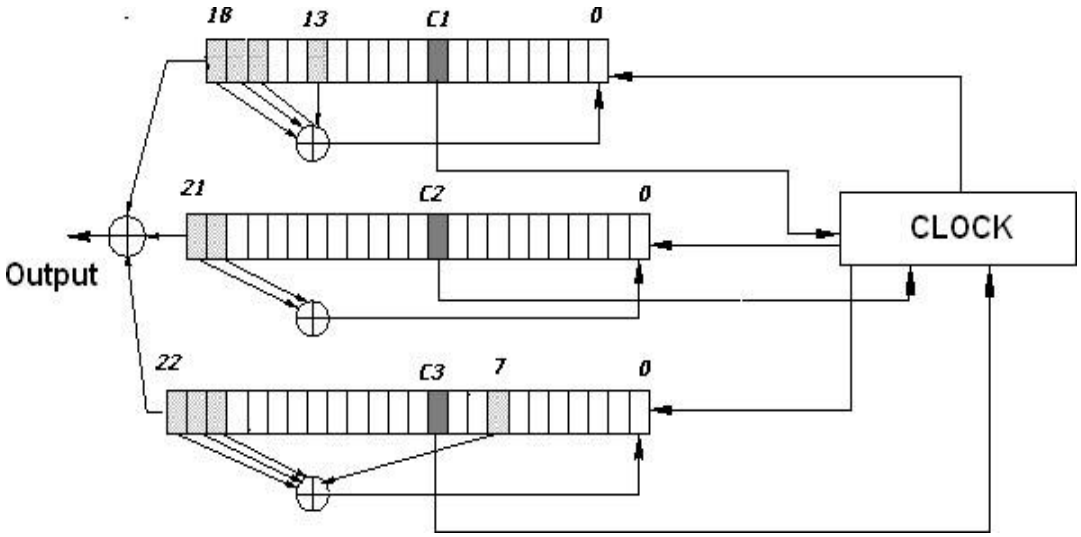


Рисунок 2.6 – Структура LFSR в алгоритмі A5/1

Процес генерації псевдовипадкових бітів з сеансового ключа Kc та лічильника кадрів Fn виконується у кілька кроків:

1. Всі три регістри скидаються, а потім тактуються протягом 64 циклів (ігноруючи управління Stop/Go тактового генератора). Протягом цього часу кожен біт Kc (від молодшого біта до старшого) додається паралельно до LSB трьох регістрів за допомогою операції XOR.

2. Три регістри синхронізуються протягом наступних 22 циклів (ігноруючи керування зупинкою/запуском тактування). Протягом цього часу послідовні Fn бітів (від LSB до MSB) знову паралельно перевіряються на XOR.

3. Fn бітів знову паралельно виконується XOR у молодших бітах цих трьох регістрів. В кінці цього кроку вміст трьох регістрів називається початковим станом кадру.

4. Три регістри синхронізуються з тактовим генератором Stop/Go протягом наступних 100 тактів, але вихідні дані не генеруються.

5. Три регістри синхронізуються з годинником Stop/Go протягом наступних 228 тактів, генеруючи 228 вихідних бітів.

6. Сформовано 228 вихідних бітів. У кожному такті генерується один вихідний біт як XOR - MSB трьох регістрів. З цих 228 біт 114 біт використовуються для зв'язку MS-BTS, а решта 114 біт використовуються для зв'язку BTS-MS [15].

## 2.5 Атаки на алгоритм аутентифікації

Багато операторів GSM використовують проектні специфікації, замість того, щоб розробляти власні алгоритми автентифікації (A3) та генерації сеансових ключів (A8). Складність у створенні нових алгоритмів полягає в тому, що абоненти, які придбали SIM-картки до запровадження нових алгоритмів, змушені використовувати старі SIM-картки зі старими алгоритмами. Іншою причиною зміни/перегляду алгоритму є вартість зміни програмного забезпечення бази даних тощо. З іншого боку, новіші та безпечніші версії алгоритму COMP128 можуть використовуватися для нових SIM-карт, що видаються новим абонентам.

Оскільки специфікація GSM для SIM-карт є загальнодоступною, все, що потрібно для копіювання SIM-карти - це 128-бітний секретний ключ Ki та IMSI, закодовані на SIM-карті.

Скопіювавши Ki та IMSI на чисту SIM-карту (яку можна легко придбати в Інтернеті), зловмисник може видавати себе за законного абонента мережі та здійснювати дзвінки на рахунок абонента. Зловмисник також може використовувати отриманий ключ Ki для розшифровки всіх вхідних і вихідних дзвінків до абонента і від нього замість сплати абонентської плати.

Якщо зловмисник має фізичний доступ до SIM-карти, він може виконати різні атаки для її клонування. Деякі з цих атак використовують потоки криптографічних алгоритмів, присутніх на смарт-карті, а інші експлуатують вразливості в самій смарт-карті.

Найпоширенішою атакою на SIM-картки є атака на сам криптографічний алгоритм (COMP128). Це атака, яка використовує потік хеш-функції для отримання секретного ключа Ki. Кожного разу, коли зловмисник запитує SIM-карту, вона генерує серію спеціальних викликів; SIM-карта застосовує функцію COMP128 до секретного ключа та вибраних викликів і повертає відповідь; SIM-карта застосовує функцію COMP128 до секретного ключа та вибраних викликів і повертає відповідь. Зловмисник може визначити Ki, проаналізувавши відповідь. Таким чином, в результаті цієї атаки зловмисник отримує доступ до секретного ключа Ki мобільного пристрою. Крім фізичного доступу до цільової SIM-карти, для проведення атаки потрібен готовий зчитувач смарт-карт і комп'ютер, який керує

процесом. Атака вимагає приблизно 150 000 запитів до SIM-карти, а оскільки середній зчитувач SIM-карт може робити 6,25 запитів в секунду, то вся атака займає приблизно 8 годин; цей час можна значно скоротити, розігнавши SIM-карту або використовуючи більш високочастотний генератор в зчитувачі SIM-карт. Однак це збільшує ризик пошкодження оригінальної SIM-карти.

Зловмисники також можуть використовувати підроблені базові станції для організації атаки з повітря. На додаток до цього обладнання зловмиснику потрібно знати IMSI або TMSI цілі. Для цього зловмисник повинен знати IMSI або TMSI.

Скомпрометована MS негайно змушена транслювати запит на оновлення місцезнаходження, який потім виконується. Як тільки призначення каналу завершено, зловмисник починає процес аутентифікації. Як тільки зловмисник отримує пару виклику та відповіді, він негайно починає нову процедуру автентифікації. Цей процес триває до тих пір, поки зловмисник не отримає необхідну кількість пар для початку процедури клонування.

Кількість кадрів, якими обмінюються мережа і MS під час процесу автентифікації, становить близько 66 кадрів, а тривалість кадру TDMA - 4610 мс, тому тривалість всієї сигнальної послідовності становить 0,30459 секунди. Можна розрахувати час, необхідний для отримання необхідної для атаки кількості пар запитів-відповідей. Відомо, що для криптографічної атаки потрібно приблизно 150 000 пар запитів-відповідей. Це означає, що атака тривала приблизно 45 689 секунд, або приблизно 13 годин. Це означає, що зловмисник мав можливість спілкуватися з MS протягом часу, необхідного для збору інформації. Це пов'язано з тим, що люди використовують мобільні телефони для здійснення та прийому дзвінків, і такий потік дзвінків призводить до того, що MS розряджається і викликає підозру у жертви. Щоб вирішити ці проблеми, атаки можна розбити на частини. Замість 13-годинної атаки зловмисник може запитувати у MS 30 хвилин щодня. Таким чином, батарея ніколи не розряджається, а ризик викликати підозру у власника або законної мережі зменшується.

Функція захисту від повітряного клонування обмежує кількість аутентифікацій SIM-карти до 150 000. Якщо цей ліміт перевищено, SIM-карта блокується. Недоліком цього рішення є необхідність виготовлення та

розповсюдження нових SIM-карт серед абонентів, що є витратним як для абонента, так і для оператора.

## 2.6 Атаки на конфіденційність GSM

Як зазначалося вище, конфіденційність телефонних дзвінків у мережах GSM захищається за допомогою потокового шифру A5. Існує два основних варіанти цього алгоритму: A5/1 - "сильна" версія з обмеженнями, що використовується країнами CEPT, і A5/2 - "слабка" версія без обмежень [21].

Атаки поділяються на три групи: атаки грубої сили, атаки з використанням криптоаналізу та атаки без криптоаналізу.

Атаки грубої сили - це атаки, в яких секретність GSM захищається секретом Kc, де Kc становить 64 біти, але останні 10 бітів дорівнюють нулю. Це зменшує ключовий простір з 2^64 до 2^54. A5/2 був розроблений у співпраці з АНБ і може бути розшифрований в реальному часі з операційним коефіцієнтом близько 2^16. Однак, a5/1 є більш потужним з двох варіантів і вразливий до атак, які можна зламати з робочим коефіцієнтом 2^40.

В мікросхемі Pentium 4 майже 60 мільйонів транзисторів, і для реалізації одного набору LFSR (A5/1) потрібно близько 2000 транзисторів. Це означає, що на одному кристалі можна реалізувати 30 000 паралельних реалізацій A5/1: На прикладі мікросхеми з тактовою частотою 3,2 ГГц кожен A5/1 генерує один вихідний біт, а це означає, що в секунду в одній реалізації A5/1 може використовуватися близько 10 мільйонів перемикачів. Таким чином, ключовий простір розміром 2^54 займе близько 18 годин, якщо використовувати всі паралельні програми на чіпі. Якщо атака буде в середньому успішною після перебору половини ключового простору, то ключі будуть знайдені приблизно за 9 годин. Подальша оптимізація шляхом відмови від даного ключа після першого помилкового біта в ключовому потоці і розподілення обчислень на декілька чіпів може скоротити час обчислень на декілька порядків. У найгіршому випадку це означає час обчислень у години/хвилини, що далеко від атаки в реальному часі. Слід мати на увазі, що складність атаки ще більше збільшується через характер відкритого тексту, який ускладнює визначення моменту знаходження ключа [22, 23].

Таким чином, успішну атаку грубої сили в реальному часі дуже складно реалізувати, але цілком можливо знайти ключ протягом декількох годин. Організація з достатніми ресурсами (обчислювальними потужностями), ймовірно, може значно скоротити час обробки.

Атаки грубої сили не можуть бути використані як атака в реальному часі проти алгоритму A5, але вони можуть бути легко використані для пошуку "офлайн" ключів, що використовуються в конкретних розмовах. Зловмисник перехоплює і записує розмову, яка його цікавить, а потім розшифровує її.

Існують різні атаки криптоаналізу проти алгоритмів, які захищають різні аспекти GSM. Алгоритм, який використовується багатьма операторами для аутентифікації абонентів (COMP128), був зламаний через недолік в дизайні хеш-функції. В результаті зловмисники отримали можливість клонувати підписки, отримуючи фізичний або бездротовий доступ до SIM-карти жертви. Найпоширеніша атака вимагає фізичного доступу до SIM-карти для клонування, що займає близько восьми годин. Процес можна прискорити, але при цьому існує ризик пошкодження SIM-карти; найефективнішим способом клонування смарт-карти GSM є атака розбиття на розділи, запропонована командою IBM. У цій атаці цільова SIM-карта викликається до восьми разів, тому клонування може бути здійснене за лічені хвилини або секунди. Однак обладнання, необхідне для проведення цієї атаки (спеціально розроблений зчитувач смарт-карт і програмне забезпечення), наразі доступне лише в лабораторіях; нові версії COMP128 вже розроблені і розгорнуті. Однак, наскільки ці більш потужні версії були прийняті операторами, невідомо. Можна припустити, що багато операторів все ще використовують старіші алгоритми через витрати, пов'язані з модернізацією. Що відомо точно, так це те, що користувачі, які мали COMP128 на своїх SIM-картах, коли вони приєдналися до мережі, все ще використовують COMP128. Існують різні криптоаналітичні пропозиції щодо того, як атакувати криптографічні алгоритми, що використовуються для захисту конфіденційності, і як зламати ці алгоритми в реальному часі. Більшість атак вимагають від зловмисника знання частини ключової послідовності. Можна отримати невелику частину відкритого коду, оскільки, крім канального кодування, яке застосовується до даних перед шифруванням,

зловмисник зазвичай знає структуру і зміст сигнальних повідомлень (особливо якщо зловмисник емулює мережу жертви і може запитувати інформацію у жертви). Зловмисник може попросити абонента-жертву надіслати певне сигнальне повідомлення (зміст якого відомий або майже відомий) після початку шифрування. У цьому випадку, окрім відомих частин відкритого тексту, зловмисник може отримати доступ до зашифрованого тексту і отримати частину ключового потоку, що використовується в процесі шифрування. Однак, для деяких з цих атак важко отримати таку кількість відомого відкритого тексту, яку вимагають деякі з них. Атака, яка вимагає найменшої кількості відомого відкритого тексту - це атака A5/2. Ця атака вимагає від зловмисника знання відкритого тексту двох кадрів з інтервалом близько шести секунд і знаходження ключа сеансу приблизно за 10 мілісекунд. Атака A5/2 була використана в одній зі стелс-атак, оскільки вимога відомого відкритого тексту може бути виконана вищезгаданим методом; варто зазначити, що для злому A5/2 потрібно лише кілька годин, що свідчить про слабкість цього алгоритму.

Атаки без шифрування. Добре відомо, що більшість мобільних телефонів стандарту GSM можуть зв'язуватися з багатьма різними базовими станціями і мережами. Це відбувається тому, що всі виробники дотримуються специфікацій і стандартів GSM. Ці специфікації розробляються Європейським інститутом телекомунікаційних стандартів (ETSI). Ви можете знайти специфікації взаємодії мереж і мобільних пристроїв, а також отримати детальну інформацію про протоколи зв'язку і механізми, що використовуються, коли мобільний пристрій потребує авторизації в мережі.

Для різних алгоритмів шифрування A5/1, A5/2 і A5/3 використовується один і той самий ключ Kc. Це означає, що злам одного з цих трьох алгоритмів і отримання сеансового ключа поставить під загрозу конфіденційність розмови, навіть якщо згодом буде використана більш безпечна версія цього алгоритму.

Базовим станціям не потрібно автентифікувати себе щодо MS, з яким вони спілкуються. Крім того, повідомлення не автентифікуються і їх цілісність не захищається.

## 2.7 DoS атаки

DoS-атаки можуть здійснюватися шляхом фізичного втручання або за допомогою логічних засобів.

Фізичні атаки є найпростішими. Зловмисник фізично втручається в передачу користувацького або сигнального трафіку через будь-який системний інтерфейс, дротовий або бездротовий. Прикладом фізичного втручання в дротовий інтерфейс є перерізання кабелів. Зловмисник може, наприклад, перерізати кабелі, що йдуть від базової станції. Прикладом фізичного втручання в радіоінтерфейс є глушіння. Для цього достатньо мати пристрій, який створює перешкоди радіосигналам GSM. Пристрій розміщується в зоні, де він створює перешкоди для руху, і GSM-обладнання, що знаходиться в зоні дії пристрою, перестане функціонувати належним чином. Стрибки частоти роблять глушіння складнішим, ніж зазвичай [25].

Зловмисник може використовувати логічні засоби для проведення DoS-атаки, як показано в наступному прикладі:

— Зловмисник надсилає в мережу фальшивий запит на скасування реєстрації (IMSI-detach). Мережа знімає абонента з реєстрації в зоні відвідування і дає вказівку HLR зробити те ж саме. Після цього користувач стає недоступним для інших абонентів. Для зняття з реєстрації зловмиснику потрібні модифіковані MS та IMSI користувача.

— Зловмисник створює запит на оновлення місцезнаходження в іншій зоні, ніж та, де абонент перебуває в роумінгу. Мережа реєструє абонента в новому регіоні, і пейджингове повідомлення надсилається цільовому користувачеві в цьому новому регіоні. Користувач більше не доступний для зв'язку з мобільним терміналом.

— Зловмисник з підробленою базовою станцією передає базовий канал з більш високим рівнем сигналу, який фіксує абонента в регіоні на радіоканал підробленої базової станції, роблячи його недосяжним для мережі, що обслуговує [24].

## 2.8 Слабкість GSM

Як згадувалося, мережа не аутентифікує телефон. Це найсерйозніша вразливість GSM, яка дозволяє проводити атаки типу "зловмисник

посередині". Ця слабкість була відома розробникам, коли створювався GSM, але очікувалося, що створення фальшивих BTS буде дуже дорогим і важко зробити такі атаки економічно ефективними. Однак двадцять років потому ситуація кардинально змінилася. Сьогодні зловмисники можуть дешево купувати BTS, оскільки існують компанії, які виробляють BTS короткого радіусу дії. Існує також проект OpenBT, який має на меті створити Unix-додаток з відкритим вихідним кодом для представлення повітряного інтерфейсу GSM.

Пізніше була виявлена поглиблена атака, вона полягає в тому, що мережа вибирає алгоритм шифрування на основі списку підтримуваних алгоритмів, з якими мобільний пристрій обмінюється повідомленнями, які називаються class marks. Повідомлення class marks не шифруються, тому для створення A5/2 можна використовувати фальшиву BTS. Фальшиве повідомлення class mark, що містить лише алгоритм, передає мову жертви на справжню BTS; перевага надається A5/0, але очікується, що легальні мережі GSM відмовлятимуть в обслуговуванні БС, які підтримують лише A5/0. Зловмисник може підслухати розмову, розшифрувавши слабший шифр A5/2. Крім того, через відсутність поділу ключів (протокол узгодження ключів не залежить від використовуваного алгоритму шифрування) зловмисник може підмінити з'єднання BTS, використовуючи A5/2 на БС, і підключитися до мережі жертви, використовуючи A5/1.

Іншою серйозною вразливістю GSM є нездатність належним чином аутентифікувати ідентифікатор абонента або відправника. Це означає, що номер абонента або номер відправника SMS може бути підроблений.

Підробка ідентифікатора абонента не є специфічною проблемою GSM, вона також стосується інших типів телефонії. Найпоширенішим методом підробки ідентифікатора абонента є використання PRI-ліній або VoIP. Основним інтерфейсом є інтерфейс доступу до мережі ISDN. Він був розроблений для середніх і великих підприємств з цифровими АТС і забезпечує доступ до телефонної мережі загального користування Лінії PRI складаються з каналів B і D, де B - основний канал для передачі даних і голосу, а D - для управління і сигнальної інформації Лінії PRI передають голос по каналу B, а ідентифікатор абонента - по каналу D, що робить їх вразливими для підміни. Іншими словами, ідентифікатор абонента на каналі

D є додатковою інформацією до передачі голосу на каналі B. Встановлення його на підроблене значення не порушує трафік голосового каналу. Цей факт часто використовується бізнесом для відображення основного телефонного номера на всіх вихідних дзвінках; PRI-лінії були недоступні приватним особам через їхню високу вартість, і спуфінг використовувався переважно бізнесом. Однак ситуація змінилася з широким розповсюдженням технології VoIP; підробка була легкою, оскільки голос передавався в IP-пакетах, а створення фальшивого ідентифікатора абонента не впливало на IP-маршрутизацію.

Декілька років тому, хакер знайшов вразливість у VoIP-провайдері Vonage, яка дозволила йому створити фальшивий ідентифікатор абонента. Його метод був дуже простим. Зловмисник міг попросити Vonage переадресувати номер телефону в їхню мережу, але замість свого номера він міг вказати дійсний номер. У той же час інші ентузіасти телефонії виявили, що Asterisk, програмне забезпечення для АТС з відкритим вихідним кодом, дозволяє користувачам вільно встановлювати ідентифікатор абонента в додатку і переадресовувати фальшивий ідентифікатор абонента провайдерам VoIP-телефонії. Однак справжній вибух шахрайства відбувся пізніше. Тоді один шахрай створив сайт підробки ідентифікаторів абонентів. Це привернуло увагу впливових ЗМІ по всьому світу і спричинило появу низки подібних сервісів. Протягом наступних кількох місяців з'явилося багато подібних сайтів. Більшість з них незабаром зникли. Незважаючи на зменшення кількості операторів, цей ринок продовжує зростати і становить реальну загрозу не лише для окремих осіб, але й для систем, які використовують ідентифікатор абонента для автентифікації користувачів. Наприклад, у 2006 році компанія SpoofCard оголосила, що закрила рахунки понад 50 клієнтів, у тому числі Періс Хілтон, за те, що вони нібито прослуховували їхні скриньки голосової пошти.

Підробка відправника SMS схожа на підробку ідентифікатора абонента. Шахраям потрібно знайти SMSC, який не перевіряє ідентифікатор відправника при відправленні SMS, і використовувати його для відправлення SMS абонентам іншого SMSC. Багато операторів можуть здійснити цю атаку, оскільки вони не перевіряють ідентифікатор відправника, коли SMS надходить з іншої мережі. Наприклад, підміна можлива на більшості

європейських операторів, але не в США чи Канаді. Ця атака набула популярності кілька років тому з появою онлайн-шлюзів для відправлення SMS. Провайдери масових SMS-розсилок часто дозволяли своїм клієнтам використовувати що завгодно як ідентифікатор відправника, якщо вони сплачували регулярну плату. Хорошим прикладом такого провайдера був Clickatell, один з найбільших провайдерів масових SMS у світі, і будь-який клієнт Clickatell міг встановити ідентифікатор відправника на будь-який номер телефону або короткий текст за допомогою невеликого додатку під назвою SmsDumper. Сьогодні, однак, більшість операторів масових текстових повідомлень відчувають потребу контролювати свої послуги і обмежують своїх клієнтів у зміні ідентифікаторів відправників за власним бажанням. Наприклад, Clickatell перевіряє нові ідентифікатори відправників перед їх використанням. Поважні провайдери масових SMS-розсилок не дозволяють підробку SMS, але є деякі провайдери, які спеціалізуються на цьому.

Ще одним слабким місцем безпеки GSM є шифрування. Дані в мережах GSM шифруються тільки на рівні повітряного інтерфейсу, під час розробки GSM вважалося, що шифрування не є необхідним, оскільки наземна частина мережі GSM використовує фіксовані, захищені лінії зв'язку. Сьогодні ситуація змінилася. Оператори з'єднують різні частини мережі за допомогою мікрохвильових каналів зв'язку "точка-точка", виділених ліній, а іноді навіть Інтернету. Ще одним недоліком є те, що працівники операторів мають доступ до даних абонентів.

Загальновідомо, що оператори можуть прослуховувати розмови абонентів, реагуючи на скарги споживачів. Наприклад, коли абонент повідомляє про тріщину в лінії, співробітники можуть прослуховувати розмову абонента лише кілька хвилин, щоб перевірити обґрунтованість скарги. Це вказує на більш серйозну загрозу доступу до інформації, яка не повинна бути доступною.

Ще одним слабким місцем, яким можуть скористатися зловмисники, є вразливість механізму безпеки IMSI. Як згадувалося вище, мережі використовують TMSI для захисту IMSI, але якщо мережа якимось чином втрачає певний TMSI, їй доводиться запитувати IMSI абонента по повітрю. Оскільки мережа не знає особи користувача, вона не може зашифрувати

з'єднання, і IMSI надсилається у відкритому вигляді. Таким чином, зловмисник може перевірити, чи знаходиться певний користувач (IMSI) поблизу. Зловмисник робить це, імітуючи легітимний BTS. Телефон абонента встановлює радіозв'язок, зловмисник може надіслати абоненту повідомлення з проханням про ідентифікацію, і телефон відповідає IMSI.

Нарешті, щоб перехопити GSM-зв'язок, зловмиснику потрібно розірвати стрибкоподібну зміну частоти. Для цього зловмиснику потрібно вивчити послідовність обміну стрибкоподібними змінами. Основна проблема зі стрибкоподібними послідовностями полягає в тому, що параметри стрибкоподібної послідовності для певної BTS зазвичай дуже статичні, і типові параметри стрибкоподібної послідовності для цієї BTS можна швидко вивчити. Таким чином, перестрибування не підвищує безпеку, а лише додає рівень складності для зловмисника.

# 3 АНАЛІЗ БЕЗПЕКИ В МЕРЕЖІ GSM

## 3.1 Аутентифікація абонента

У мережах GSM абоненти ідентифікуються за допомогою SIM-карт, які містять всі необхідні для доступу дані; на SIM-карті зберігаються дві найважливіші частини інформації:

— IMSI, номер, який легко зчитується з SIM-карти;

— Ki номер.

Дозвіл MS на доступ до наземної рухомої мережі загального користування (PLMN) здійснюється за допомогою механізму виклику-відповіді, як показано нижче:

1. Телефон підключається до мережі;
2. Телефон ідентифікується;
3. Мережа генерує 128-бітове випадкове число, відоме як RAND, і надсилає його на MS. БС шифрує RAND за допомогою Ki та алгоритму аутентифікації A3, реалізованого в SIM-картці:

$$A3_{Ki}(RAND) = SRES \tag{3.1}$$

4. Обчислене 32-бітне значення SRES надсилається назад;
5. Мережа виконує ту саму операцію, щоб отримати XRES (очікувану реакцію) і порівняти її з SRES:

$$A3_{Ki}(RAND) = XRES; \tag{3.2}$$

$$SRES = XRES \text{ або } SRES \neq XRES;$$

6. Якщо обидва значення рівні, телефон підтвердив знання Ki, таким чином, є автентифікованим;
7. MS та мережа обчислюють ключ сеансу шифрування Kc за алгоритмом A8:

$$Kc = A8_{Ki}(RAND); \tag{3.3}$$

8. Мережа обирає алгоритм шифрування відповідно до списку підтримуваних алгоритмів, про який повідомляє мобільний телефон, і шифрування активується. Kc використовується як сеансовий ключ шифрування [7].

Оскільки шифрування активується після авторизації, щоб запобігти несанкціонованому відстеженню мережі, користувач уникає використання IMSI, натомість він використовує тимчасовий ідентифікатор мобільного абонента (TMSI). TMSI генерується, коли користувач вперше підключається до нової мережі наступним чином:

— MS використовує свій IMSI для ідентифікації в мережі;

— Мережа активує шифрування і надсилає новий TMSI на MS.

Щоб забезпечити ще більшу безпеку, TMSI часто змінюється.

Більшість мобільних операторів використовують алгоритми A3 і A8 фактично як один алгоритм, а саме COMP128 (версія 1, 2 або 3).

COMP128-1 використовує 16-байтовий ключ Ki і 16-байтовий RAND, щоб вивести 12-байтовий хеш наступним чином:

$$\begin{aligned} \text{COMP128}(\,\text{Ki}||\text{RAND}\,) &= \text{hash};\\ \text{SRES} &= \text{hash}[0\ldots3];\\ \text{Kc} &= \text{hash}[4\ldots11]. \end{aligned} \tag{3.4}$$

Точніше, алгоритм спочатку завантажує Ki та RAND у 32-байтовий вектор X. Ki зберігається в X[0,15], а RAND - в X[16,31]. Потім виконується стиснення X. Стиснення складається з перебору 5 таблиць $T_0$, $T_1$, $T_2$, $T_3$, $T_4$ та структури-метелика $B_{A3}$. Кожна $T_j$ містить лише (8-j)-бітові значення, таким чином, результатом стиснення є 32 4-бітові значення, які далі переставляються за допомогою перестановки $P_{A3}$ та копіюються у X[16..31]. Потім Ki завантажується в X[0..15] і починається нова ітерація. Отримані 128 біт після восьми ітерацій додатково стискаються до 12 байт за допомогою функції перестановки/вибору $F_{A3}$, яка формує вихід алгоритму. Код та структура стиснення в алгоритмі COMP128-1 показано на рис. 3.1 та 3.2 [8].

```
for j=0 to 4 do{
    for k=0 to 2j-1 do{
        for l=0 to 2(4-j)-1 do{
        m = l + k-2(5-j);
        n = m + 2(4-j);
        y = (X[m] + 2X[n]) mod 2(9-j);
        z = (2X[m] + X[n]) mod 2(9-j);
        X[m] = Tj[y];
        X[n] = Tj[z];
            }
        }
    }
```

Рисунок 3.1 – Код стиснення в COMP128-1

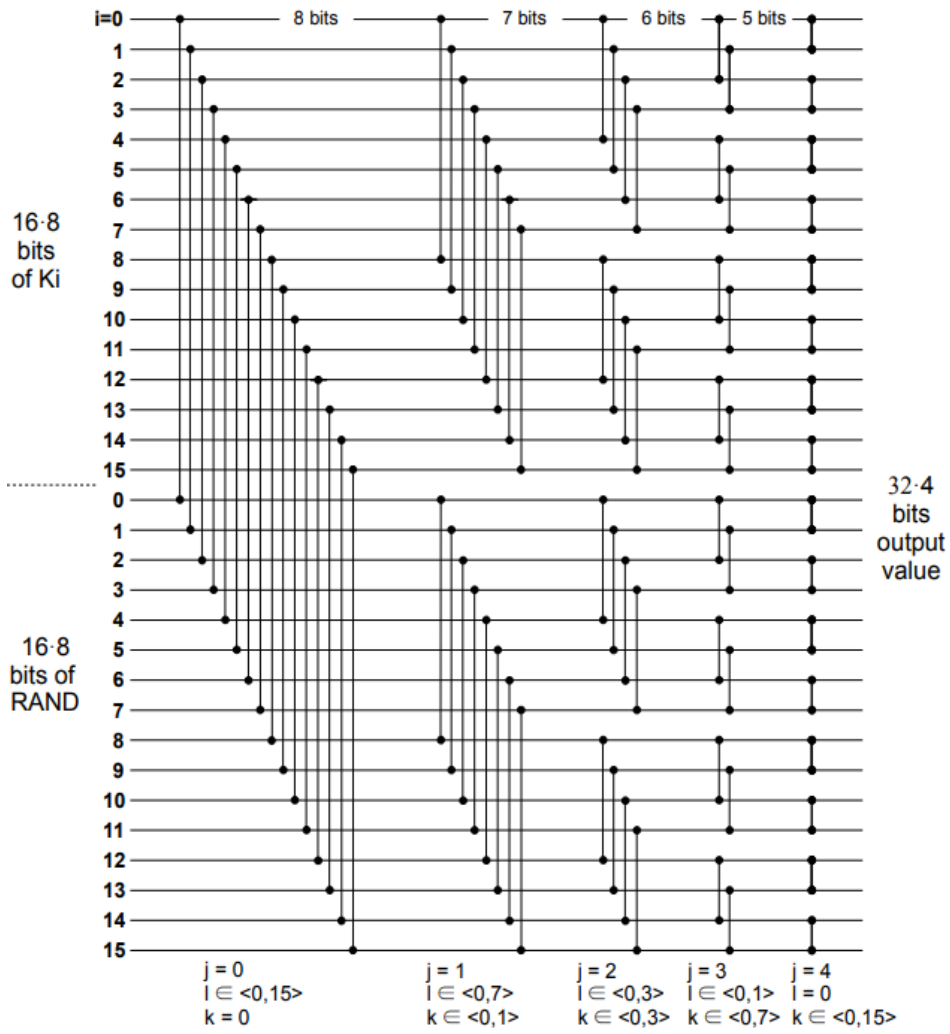


Рисунок 3.2 – Структура “метелика” в COMP128-1

У кожному шарі є 16 операцій об'єднання, кожна з яких перетворює пару входів у пару виходів:

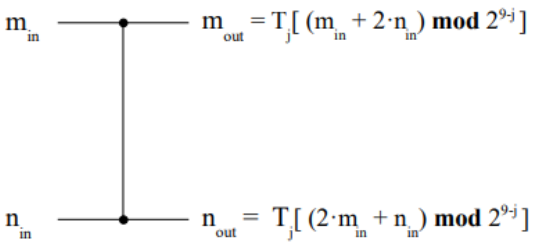


Рисунок 3.3 – Поєднання операцій у структурі “метелик”

## 3.2 Шифрування трафіку

Шифрування всього радіоканалу виконується MS, оскільки це вимагає значних обчислювальних потужностей і не може бути виконано 8-бітною SIM-карткою. Оскільки комп'ютер не знає Ki, він не може бути використаний як ключ шифрування. Замість цього, БС і мережа домовляються про новий ключ шифрування Kc.

GSM-передача організована у вигляді послідовності пакетів. Один пакет містить 114 біт і надсилається кожні 4,516 мс. Шифрування відбувається шляхом генерації потоку бітів (шифрованого блоку), який об'єднується з відкритим текстом для отримання зашифрованого тексту. Дані розшифровуються на іншому кінці шляхом XOR-обробки отриманих даних з ідентичним шифрованим блоком [11].

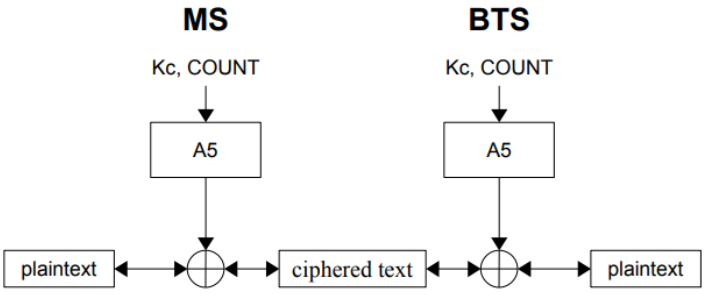


Рисунок 3.4 – Шифрування та дешифрування даних в GSM

Цей метод має один серйозний недолік. Два однакових відкритих тексти дають однакове шифрування. Ця, здавалося б, несуттєва особливість широко досліджується в криптоаналізі, наприклад, Енігма була зламана, в тому числі, через цю особливість. Щоб запобігти цьому, алгоритм також "засівається" COUNT, кількість яких базується на номері кадру TDMA:

$$\begin{aligned} T1 &= FN / 1326 \\ T2 &= FN \bmod 26 \\ T3 &= FN \bmod 51 \\ COUNT &= T1||T3||T2 \\ A5(Ki||COUNT) &= cipher\_block \end{aligned} \tag{3.5}$$

Де FN - номер кадру TDMA. У GSM множинний доступ з часовим розділенням каналів - це метод, який дозволяє обслуговувати один і той самий фізичний канал до восьми різних телефонів. Це досягається шляхом виділення фізичного каналу різним телефонам за допомогою циклічного процесу, де кожен телефон передає дані в часовому інтервалі, який триває 0,02 с.

A5/1 і A5/2 - це потокові шифри, які використовують регістри зсуву з лінійним зворотним зв'язком (LFSR). Регістр зсуву - це апаратний регістр, який може одночасно зсунути всі свої біти на одну позицію і заповнити "порожній" біт заданим значенням, отриманим за допомогою деяких функцій лінійного зворотного зв'язку (найчастіше XOR). Позиції бітів, які "беруть участь" у функції зворотного зв'язку, називаються послідовністю перемикань. Потокові шифри A5 створюються шляхом об'єднання виходів декількох LFSR. A5/1 використовує три LFSR довжиною 19, 22 і 23 біти (всього 64 біти). На рис. 3.5 показані послідовності перемикань та інші деталі A5/1 [10].

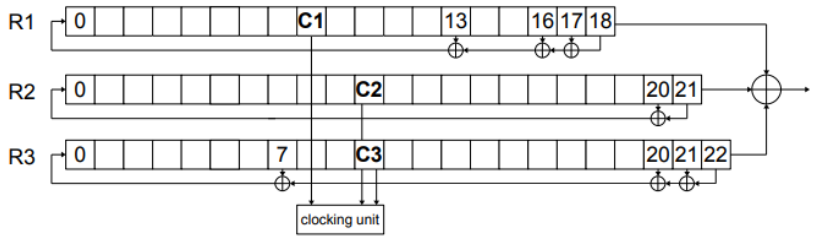


Рисунок 3.5 – Внутрішня структура A5/1

Регістри R1, R2 і R3 синхронізуються в режимі stop/go за наступним правилом: кожен регістр має один синхронізуючий відвід (C1, C2, C3); на кожному такті обчислюється мажоритарна функція синхронізуючих відводів

і синхронізуються тільки ті регістри, синхронізуючі відводи яких збігаються з мажоритарним бітом. Перед кожним використанням A5/1 ініціюється наступним чином:

1. $R1 = R2 = R3 = 0$
2. Для i = 0 to 63 do

$$\begin{aligned} R1[0] &= R1[0] + Kc[i] \\ R2[0] &= R2[0] + Kc[i] \\ R3[0] &= R3[0] + Kc[i] \end{aligned} \tag{3.6}$$

Тактуються всі три регістри, ігноруючи керування тактовою частотою stop/go

3. Для i = 0 to 21 do

$$\begin{aligned} R1[0] &= R1[0] + COUNT[i] \\ R2[0] &= R2[0] + COUNT[i] \\ R3[0] &= R3[0] + COUNT[i] \end{aligned} \tag{3.7}$$

Тактуються всі три регістри, ігноруючи керування тактовою частотою stop/go

4. Для i = 0 to 99 do

Тактується шифр за допомогою його звичайного управління тактовим генератором [16].

Після ініціалізації обчислюється 228 біт вихідного потоку. 114 біт використовуються для шифрування даних з мережі на мобільний телефон, а інші 114 біт використовуються для шифрування даних з телефону в мережу.

A5/2 дуже схожий на свого "старшого брата". Він також використовує три регістри на 19, 22 і 23 біти для формування вихідних даних, але його механізм зупинки/вимикання відрізняється. Замість тактових відводів він має додатковий регістр R4, який використовується лише для керування тактовою частотою R1, R2 і R3. На рис. 3.6 показано структура A5/2.

Керування синхронізацією A5/2 можна описати наступним чином:

$$\begin{aligned} &m = Majority(R4[3], R4[7], R4[10]) \\ &\text{if } R4[10] = m \text{ then clock the R1} \\ &\text{if } R4[3] = m \text{ then clock the R2} \\ &\text{if } R4[7] = m \text{ then clock the R3} \end{aligned} \tag{3.8}$$

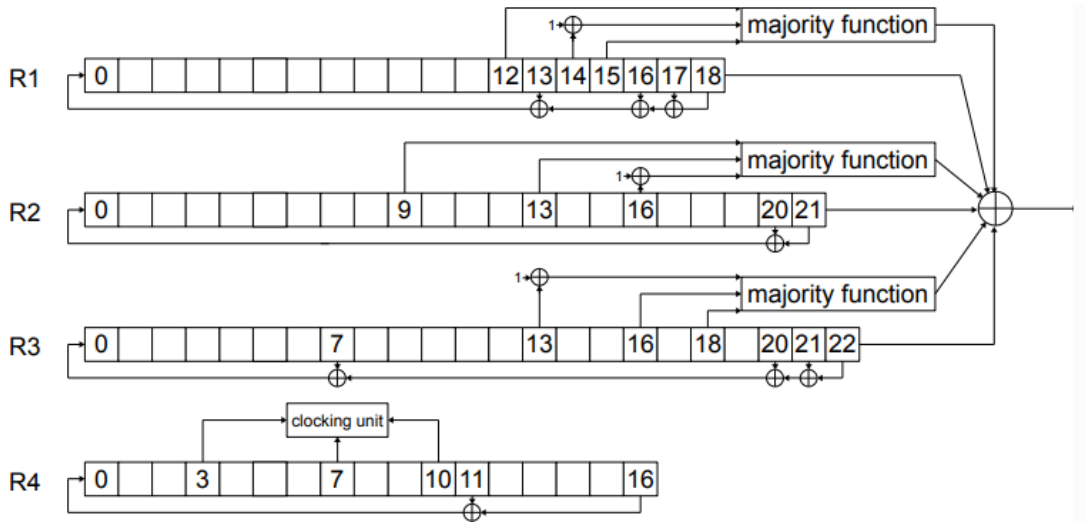


Рисунок 3.6 – Внутрішня будова формату A5/2

Ініціалізація A5/2 подібна до ініціалізації A5/1 і виглядає наступним чином:

1. $R1 = R2 = R3 = R4 = 0$
2. For i = 0 to 63 do

$$\begin{aligned} R1[0] &= R1[0] + Kc[i] \\ R2[0] &= R2[0] + Kc[i] \\ R3[0] &= R3[0] + Kc[i] \\ R4[0] &= R4[0] + Kc[i] \end{aligned} \tag{3.9}$$

Тактуються всі три регістри, ігноруючи керування тактовою частотою stop/go

3. For i = 0 to 21 do

$$\begin{aligned} R1[0] &= R1[0] + COUNT[i] \\ R2[0] &= R2[0] + COUNT[i] \\ R3[0] &= R3[0] + COUNT[i] \\ R4[0] &= R4[0] + COUNT[i] \end{aligned} \tag{3.10}$$

Тактуються всі три регістри, ігноруючи керування тактовою частотою stop/go

4. $R1[15] = R2[16] = R3[18] = R4[10] = 1$
5. For i = 0 to 98 do

Тактується шифр за допомогою його звичайного управління тактовим генератором і відкидання вихідних даних

A5/1 і A5/2 схожі, а A5/3, навпаки, має зовсім іншу конструкцію. Він має розмір блоку 64 біти і розмір ключа 128 біт [17].

Окрім криптографії, як ще один рівень безпеки використовується стрибкоподібна зміна частоти. Вона визначається двома параметрами - зміщенням індексу мобільного розподілу (MAIO), яке приймає значення від нуля до кількості частот у списку мінус один, і номером послідовності стрибкоподібних змін (HSN), який приймає значення від 0 до 63. Існує 2 режими перемикання - циклічне перемикання і нециклічне перемикання. Якщо HSN дорівнює 0, використовується циклічний стрибок, коли мобільна станція просто переходить через набір частот.

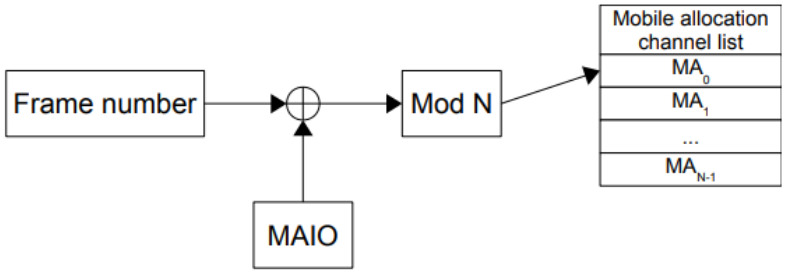


Рисунок 3.7 –Циклічна зміна частоти в GSM

У нециклічному стрибку номер кадру і HSN використовуються для запуску більш складного алгоритму стрибка, що показано на рисунку 3.8.

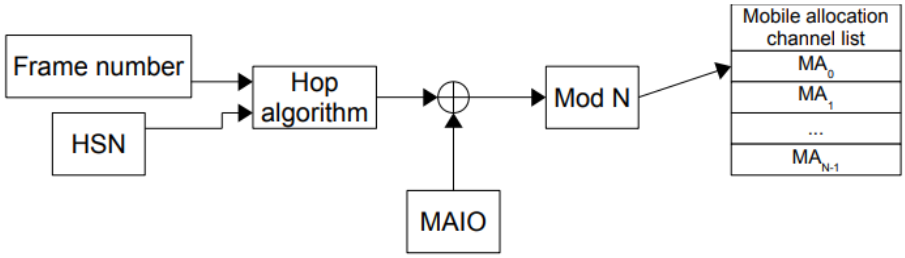


Рисунок 3.8 – Нециклічна стрибкоподібна зміна частоти в GSM

Зазвичай, канали трафіку в одній комірці мають однаковий HSN і різні MAIO. Після призначення каналу трафіку мобільний телефон і мережа обчислюють частоту для кожного пакета відповідно до вищевказаної інформації, наданої під час призначення, і відповідно до номера кадру TDMA [20].

## 3.3 Слабкість алгоритмів A3/A8

A3 і A8 покладалися на модель захисту через невідомість, але специфікації алгоритмів частково просочилися, і відсутні фрагменти були заповнені шляхом реінжинірингу працюючої SIM-карти. Виявилося, що і A3, і A8 насправді були одним алгоритмом, а саме COMP128-1. Як ми раніше вже з'ясували, хоча Ki є 64-бітним числом, його 10 останніх бітів завжди дорівнюють нулю. Після реконструкції COMP128-1 був проведений його аналіз, і пізніше запропонували атаку на алгоритм, яка дозволяє зловмиснику витягти секретний ключ (Ki) з SIM-карти. Це був дуже серйозний пролом у безпеці GSM. Оскільки весь GSM-трафік шифрується лише за допомогою Ki та незашифрованого RAND.

Для вилучення Ki атака використовує парадокс дня народження. У теорії ймовірностей парадокс дня народження стосується ймовірності того, що у множині випадково вибраних людей якась пара з них матиме однаковий день народження. Питання полягає в тому, скільки людей потрібно, щоб ймовірність перевищила 50%? Багато хто думає про 366/2 = 183 або щось подібне, але правильна відповідь: лише 23. Це тому, що в групі з 23 осіб є: 0,5*22*23 = 253 пари, так що ймовірність згаданої подвійності набагато вища (50,7%). У криптографії математика, що лежить в основі парадоксу дня народження, використовується для оцінки ймовірності того, що для заданої хеш-функції f ми знайдемо пару $x_1 \neq x_2$ таку, що $f(x_1) = f(x_2)$. Така пара називається колізією.

Було виявлено, що зіткнення в COMP128-1 можуть бути використані для вилучення Ki з SIM. Як згадувалося раніше, COMP128-1 використовує структуру "метелик" $B_{A3}$. Атака ґрунтується на тому, що зіткнення можуть відбуватися на другому шарі першого раунду, що видно на рис. 3.9.

Як видно з діаграми, Ki можна атакувати по частинах, оскільки для заданого i на другому рівні (j=1) 4 * 7 = 28 біт вихідних даних залежать лише від пари байт ($Ki_i$, $Ki_{i+8}$) з ключа та пари ($RAND_i$, $RAND_{i+8}$) з виклику. Зловмисник перебирає значення ($RAND_i$, $RAND_{i+8}$), зберігаючи інші байти RAND-запиту незмінними, поки не відбудеться колізія у 96 бітному виході функції COMP128-1. Оскільки 28 біт на виході мало в порівнянні з 2 входами[16] і через вищезгаданий парадокс дня народження, це з великою ймовірністю може статися. Маючи таку колізію, зловмисник тепер має дві

пари ($RAND_i$ [1], $RAND_{i+8}$ [1]), ($RAND_i$ [2], $RAND_{i+8}$[2]), які дають однаковий вихід, майже напевно через колізію на другому рівні. Тепер зловмисник може перебирати значення ($Ki_i$, $Ki_{i+8}$) на своєму комп'ютері, шукаючи ключові байти, які також призведуть до колізії для тих самих значень$_i$ ($RAND_{i+8}$[1], $RAND^{1})_i$, ($RAND_{i+8}$[2], $RAND^{2}$). Повторюючи цей процес 8 разів, можна витягти всі 16 байт Ki. Очікувана кількість запитів до того, як ця атака буде успішною, становить близько 150 000. Але кількість запитів можна зменшити. Після того, як другий рівень буде атаковано, атака може бути проведена на наступних рівнях, і весь процес може бути скорочений до 20 000 запитів.

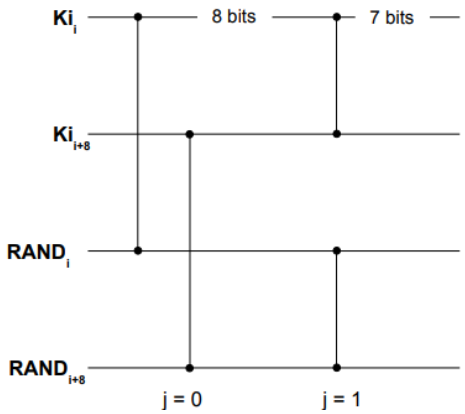


Рисунок 3.9 – Зіткнення в COMP128-1

SIM-карту можна підмінити двома способами. Якщо зловмисник має фізичний доступ до SIM-картки, він може просто використати зчитувач смарт-карт. При швидкості 6,25 викликів на секунду це займе близько 1 години. Цей час можна скоротити, наприклад, розігнавши зчитувач. Другий метод - це повітряна атака. У цьому сценарії зловмисник імітує легітимну GSM-мережу і використовує процедуру автентифікації багато разів для отримання Ki. В ідеальних умовах йому знадобиться 235 мс для відправлення запиту на аутентифікацію і 235 мс для отримання відповіді (в той же час він може відправити наступний запит), таким чином, очікуваний час відновлення Ki становитиме близько 85 хвилин.

З часом було запропоновано ще одну атаку, але побічного каналу на COMP128-1. У криптографії атака побічного каналу - це будь-яка атака, заснована на інформації, отриманій з фізичної реалізації криптосистеми, а не на грубій силі або теоретичних слабкостях алгоритмів. Було виявлено що

миттєве споживання енергії та електромагнітне випромінювання корелює з проблемою в декількох реалізаціях COMP128-1. Аномалія, ймовірно, викликана тим, що COMP128-1 вимагає деяких 9-бітних операцій, в той час як SIM-карти є 8-бітними чіпами. Як видно зі специфікації COMP128-1, при j=0:

$$\begin{aligned} X[m] &= T0\,[y]\,, y = (X[m] + 2 - X[n]) \bmod 29 \\ X[n] &= T0\,[z]\,, z = (2 - X[m] + X[n]) \bmod 29 \end{aligned} \tag{3.11}$$

Як видно, таблиця $T_0$ повинна мати 9-бітовий індекс. Оскільки на 8-бітній архітектурі адресації неможливо безпосередньо звертатися до такої таблиці, дуже ймовірно, що програмісти розбивають $T_0$ на дві таблиці, $T_{00}$ і $T_{01}$, розміром 256 елементів кожна. Крім того, найпростіший спосіб розділити її - зберігати перші 256 елементів $T_0$ у $T_{00}$, а останні 256 елементів - у $T_{01}$. Ця гіпотеза пояснює спостережувану аномалію. Пошук випадкового елемента $T_{00}$ призведе до дещо іншого сигналу потужності, ніж пошук випадкового елемента $T_{01}$ . Більше того, існувало 32 регіони SIM-карти, де спостерігалися ці аномалії. Це пов'язано з тим, що перший рівень стиснення в COMP128-1 вимагає двох пошуків в таблиці $T_0$ з індексами y і z для кожного з 16 байт вхідних даних. Ці спостереження дозволяють користувачам провести дуже ефективну атаку на COMP128-1. Зверну увагу, що у першому шарі (j=0):

$$\begin{aligned} m &= i \\ n &= m + 16 \\ X[m] &= Ki[i] \\ X[n] &= RAND\,[i] \\ y &= (Ki[i] + 2 - RAND[i]) \bmod 512 \\ z &= (2 - Ki[i] + RAND[i]) \bmod 512 \end{aligned} \tag{3.12}$$

Наступний приклад буде використаний для пояснення того, як обчислити Ki. Припустимо, що у зловмисника є SIM-карта з невідомим Ki. Він помітив, що всі запити в таблиці $T_0[y]$ потрапляють в $T_{01}$ з RAND[0] в діапазоні [27,...,154]. Перехід, коли RAND[0] переходить від 26 до 27, має

бути спричинений тим, що значення у перетинає 256. Аналогічно, перехід при переході RAND[0] від 154 до 155 повинен бути викликаний перетином значення у через 512. З цього випливає, що Ki[0] може бути тільки 202 або 203. Далі така ж класифікація виконується з z. Зловмисник помітив, що всі запити в таблиці $T_0[z]$ потрапляють в $T_{00}$ з RAND[0] в діапазоні [0...105]. Оскільки Ki[0] дорівнює або 202, або 203, то перехід при зміні RAND[0] від 105 до 106 відбувається лише для Ki[0]=203, а отже зловмисник отримує перший байт ключа. Для отримання всього ключа зловмисник виконує аналогічний аналіз для решти значень i.

Для усунення відомих недоліків COMP128-1 були розроблені дві нові версії COMP128, а саме COMP128-2 і COMP128-3 [18].

## 3.4 Атаки на A5/1 та A5/2

Коли алгоритми A5/1 та A5/2 почали аналізувати криптологи, стало очевидно, що обидва не забезпечують належного рівня безпеки. Крім того, такі факти, як те, що 10 останніх бітів Ki завжди дорівнюють нулю, вказують на те, що це не випадковість.

Більшість атак, які будуть описані далі, є атаками з відомим відкритим кодом, тобто, щоб розшифрувати ключ шифрування, зловмисник повинен знати не тільки зашифровані кадри, але й їхній відкритий текстовий вміст. Це припущення може виглядати нереалістичним, але було знайдено методологію, як витягти певну кількість відкритого тексту із зашифрованих GSM-кадрів. Наприклад, кожен канал трафіку між телефоном і мережею супроводжується повільнішим каналом управління, а саме повільним асоційованим каналом управління (SACCH). Мережа використовує цей канал для надсилання деяких системних повідомлень на мобільний телефон, а також для управління потужністю і часом поточної розмови. Вміст SACCH можна певним чином передбачити, спостерігаючи за поведінкою телефону жертви. Крім того, певний вміст SACCH передається циклічно. Такими повідомленнями можуть бути отримані, наприклад, шляхом підслуховування початку дзвінка, коли передача даних не зашифрована, або з телефону зловмисника.

A5/2 було проаналізовано одразу після зворотного інжинірингу за допомогою лінійного криптоаналізу.

Лінійний криптоаналіз полягає в побудові систем лінійних рівнянь, які апроксимують дію шифру.

У класичній алгебрі лінійний вираз зі змінними $x_1$ , ... , $x_n$ має вигляд:

$$y = a_1 x_1 + a_2 x_2 + ... + a_n x_n \qquad (3.13)$$

де $a_1$ - дійсні числові константи. Навпаки, в лінійному криптоаналізі всі змінні є бінарними і всі класичні алгебраїчні операції замінюються відповідними бінарними операціями, а саме, додавання замінюється операцією XOR, а множення представляється як операція AND.

Звичайні арифметичні правила для дійсних чисел застосовуються і тут, хоча вони можуть здатися дещо дивними.

Таблиця 3.1 – Бінарні заміни для алгебраїчних операцій

| Бінарне додавання, XOR | Бінарне множення, AND |
|---|---|
| 0 + 0 = 0<br>1 + 0 = 0 + 1 = 1<br>1 + 1 = 0 | 0 * 0 = 1 * 0 = 0 * 1 = 0<br>1 * 1 = 1 |

Пізніше, вищезгадану техніку було використано для атаки на A5/2. Атака базується на спостереженні, що R4[10] встановлюється в 1 після кожного налаштування ключа, отже, R4 має однакове значення після ініціалізації незалежно від того, чи біт COUNT[10] дорівнює 0 або 1. Нехай $f_i$ та $f_{i+\alpha}$ - відповідні значення COUNT для кадрів і та i+α. Якщо $f_i$ відрізняється від $f_{i+\alpha}$ лише у $f$[10] ($f_i + f_{i+\alpha} = 00000000000100000000000_b$), то $R4_i = R4_{i+\alpha}$. Через обрану перестановку між номером кадру TDMA та $f$, це відбувається для будь-яких двох кадрів, які знаходяться на відстані рівно 1326 кадрів TDMA один від одного (α = 1326). Нехай $Z_i$ і $Z_{i+\alpha}$ є значеннями ключового потоку для вищезгаданих кадрів, також було помічено, що $Z_i + Z_{i+\alpha}$ є лінійним в $R1_i$, $R2_i$ і $R3_i$. Тому для заданих $Z_i + Z_{i+\alpha}$ початковий внутрішній стан $R1_i$, $R2_i$ і $R3_i$ можна відновити, розв'язавши лінійну систему рівнянь. Оскільки початковий внутрішній стан $R1_i$, $R2_i$ і $R3_i$ становить 61 біт

(три біти R1, R2 і R3 встановлені в 1), то для розв'язання цих рівнянь потрібно лише 61 біт $Z_i + Z_{i+\alpha}$. Оскільки R4 невідоме, зловмиснику потрібно вгадати всі можливі $2^{16}$ значення R4, і для кожного значення розв'язати отримане лінійне рівняння, доки не буде знайдено послідовний розв'язок [19].

Потім атаку було вдосконалено. В це раз атака вимагає ключового потоку з будь-яких чотирьох кадрів. Був описаний спосіб записати кожен вихідний біт - навіть якщо він знаходиться на різних кадрах - у вигляді квадратичного члена від $R1_1$, $R2_1$ і $R3_1$ першого кадру. Маючи вихідні біти чотирьох кадрів, вони побудували систему квадратичних рівнянь для кожного з $2^{16}$ можливих значень $R4_1$ і розв'язували її, поки не знайшли узгоджений розв'язок. Таким чином, вони змогли відновити початкове значення $R1_1$, $R2_1$, і $R3_1$, а також, змінивши налаштування ключів, і сеансовий ключ. Для побудови атаки на шифрований текст використаєм той факт, що в каналі SACCH застосовується корекція помилок перед шифруванням. Виправлення помилок можна змоделювати як множення відкритого тексту повідомлення (позначеного P) на постійну матрицю (позначену G), і XOR з постійним вектором (позначеним g), M = (G * P) + g. Тепер, нехай H - матриця перевірки на парність, тобто H * (M + g) = 0 і C - зашифроване повідомлення, C = M + Z. І в результаті виходить рівняння:

$$H(C + g) = H(M + Z + g) = H(M + g) + H * Z = 0 + H * Z = H * Z \quad (3.14)$$

Оскільки H, C і g відомі, вони можуть перетворити описану раніше атаку на відкритий текст в атаку тільки на зашифрований текст.

Перша атака на A5/1 була здійснена коли A5/1 ще не була повністю відома. Основна ідея полягала в тому, щоб вгадати повний вміст регістрів R1 і R2 і приблизно половину регістра R3. Таким чином визначається тактова частота всіх трьох регістрів, а друга половина R3 може бути отримана з 64 біт ключового потоку. Потім було припущено, що A5/1 повинен бути схильний до двох типів атак, а саме: атаки типу "розділяй і володарюй" та атаки типу "компроміс між часом і пам'яттю". Алгоритм "розділяй і володарюй" працює шляхом розбиття проблеми на дві або більше підпроблем, які стають досить простими для вирішення. Така

поведінка може бути використана для розбиття LFSR. Якщо структура генератора відома, а секретний ключ - це початкові стани LFSR, то для генератора ключового потоку, що складається з n LFSR, загальна кількість ключів, які потрібно перебрати, дорівнює:

$$\prod_{i=1}^{n}(2-1)\,, \tag{3.15}$$

де $L_i$ - довжина i-го LFSR.

Використання атаки "розділяй і володарюй", яка послідовно визначає окремі стани LFSR, зменшує загальну кількість ключів для перебору $\sum_{i=1}^{n}(2-1)$. Ключова ідея атаки полягає в тому, щоб вгадати нижню половину кожного регістра (ці біти визначають тактову частоту регістра в перші кілька тактів) і тактують шифр, поки не закінчаться вгадані біти. Кожен вихідний біт негайно дає лінійне рівняння в термінах бітів внутрішнього стану, що належать верхнім половинам трьох регістрів. Потім вгадування тактової послідовності продовжується, що знову призводить до інших лінійних рівнянь, які описують вихід мажоритарної функції. Коли таким чином отримано 64 лінійно незалежних рівняння, система розв'язується за допомогою методу Гауссового виключення. За приблизними розрахунками потрібно вгадати близько 20 бітів.

Другою атакою, була атака компромісу між часом і пам'яттю. Це практичний метод зменшення часу на пошук ключа. Цей тип атаки можна застосовувати, якщо шифр має невеликий розмір стану. Зазвичай, в атаках з використанням компромісу з пам'яттю часу зловмисник генерує певну кількість вихідних бітів з певних станів шифру, а потім зберігає ці стани шифру і відповідні їм вихідні біти попарно, у відсортованому списку. Потім він шукає збіг між отриманою послідовністю ключового потоку і збереженими вихідними послідовностями. Якщо це відбувається, отримується відповідний стан шифру і з цього стану можна відновити ключ.

Пізніше представлено ще дві атаки, але на компроміс між робочим часом і пам'яттю проти A5/1. Перша вимагала таблиці розміром 300 ГБ, дві хвилини потоку клавіш і близько однієї секунди часу обробки на середньому ПК, тоді як друга атака вимагала таблиці розміром 300 ГБ, дві секунди потоку клавіш і кілька хвилин часу обробки на середньому ПК.

Інший напрямок атак на A5/1 розпочався в момент ідеї кореляційних атак були застосовані до A5/1. Кореляційні атаки на генератори ключових потоків на основі LFSR базуються на статистичних залежностях між спостережуваними послідовностями ключових потоків та послідовностями зсувних регістрів. Для відновлення ключа A5/1 за допомогою кореляційної атаки зловмисник намагається дізнатися, як виглядали регістри R1, R2 і R3 безпосередньо перед ініціалізацією ключа. Для цього зловмисник пробує зашифрувати багато триплетів ($R1_1$, $R2_1$, $R3_1$)...($R1_n$, $R2_n$, $R3_n$), поки не знайде потрібний. Але оскільки він знає деяку статистичну залежність між регістрами R1, R2, R3 та ключовим потоком шифру, йому не потрібно пробувати всі можливі триплети, він може спробувати лише ті, які корелюють з заданим (перехопленим) ключовим потоком Z. Іншими словами, він використовує кореляцію для кожного триплету, щоб оцінити ймовірність того, що і-го триплет ($R1_i$, $R2_i$, $R3_i$) згенерує Z. Пробне шифрування виконується лише для триплетів з найвищою ймовірністю.

Потім було опубліковано кореляційну атаку, помічено що через лінійність налаштування ключа початкове внутрішнє значення R1, R2 і R3 на кадрі j задається величиною :

$$\begin{aligned} R1 &= S1 + F_1^j; \\ R2 &= S2 + F_2^j; \\ R3 &= S3 + F_3^j \end{aligned} \tag{3.16}$$

Де S1, S2 і S3 - початковий внутрішній стан регістрів R1, R2 і R3 після налаштування ключа за допомогою правильного ключа K, де номер кадру вибрано рівним нулю, тобто:

$$(S1, S2, S3) = \text{keysetup}(K, 0) \tag{3.17}$$

Аналогічно, нехай $F_1^j$, $F_2^j$, $F_3^j$ - початковий внутрішній стан регістрів R1, R2 і R3 після налаштування ключа з використанням усіх нулів як ключа, але з номером кадру j, тобто:

$$(Fj1, Fj2, Fj3) = keysetup(0, j) \quad (3.18)$$

Нехай $S_i$ ($l_i$) і $F_i$ ($l_i$) позначають вихідні біти регістрів $S_i$ і $F_i$ після того, як вони були тактовані $l_i$ разів з початкового стану до кінця циклу t. В результаті виходить рівняння:

$$S_1(l_1) + S_2(l_2) + S_3(l_3) = Z(t) + F_1^j(l_1) + F_2^j(l_2) + F_3^j(l_3) \quad (3.19)$$

Рівняння (3.19) виконується у двох випадках:

1. LFSR дійсно тактуються $l_1$, $l_2$, $l_3$ у момент часу t. Якщо це так, то вираз буде істинним з ймовірністю 1.
2. Якщо умова в 1 не виконується, вираз все одно буде істинним з ймовірністю ½ (тобто чисто випадково).

Отже, рівняння (3.19) виконується з певною ймовірністю:

$$p = \frac{1}{2} + \frac{1}{2}(\Pr\{(l_1, l_2, l_3)\ at\ time\ t\}) \quad (3.20)$$

де Pr {($l_1$, $l_2$, $l_3$) в момент часу t} - ймовірність того, що в момент часу t LFSR були відлічені точно $l_1$, $l_2$, $l_3$ разів, відповідно. Ймовірність того, що в момент часу t LFSR були запущені $l_1$, $l_2$, $l_3$ разів, в результаті маємо:

$$\Pr\{(l1, l2, l3\ at\ t\}) = \frac{\left(\frac{t}{t-l_1}\right)\left(\frac{t-(t-l_1)}{t-l_2}\right)\left(\frac{t-(t-l_1)-(t-l_2)}{t-l_3}\right)}{4^t} \quad (3.21)$$

Це означає, що співвідношення (3.19) є зміщеним (p > ½). Ймовірність p дає оцінку відповідної лінійної комбінації для одного кадру j.

Вищезгадане зміщення можна покращити. Припустимо, що в момент часу t LFSR мають тактові частоти $l_1$ , $l_2$ та $l_3$ разів, відповідно. Тоді ми також припускаємо, що в момент часу t + 1 третій LFSR не тактується. За цих двох припущень R3 вносить один і той самий біт у вихідні біти t і t +1. Таким чином, внесок R3 виключається з різниці цих двох вихідних бітів, і має місце наступне рівняння:

$$S'_1(l_1) + S'_2(l_2) + S'_3(l_3) = Z'(t) + F'^{j}_{1}(l_1) + F'^{j}_{2}(l_2) + F'^{j}_{3}(l_3) \qquad (3.22)$$

Коли S'(l) = S(l) +' S(l+1) і так далі. Припускаючи, що значення у відгалуженнях тактової частоти розподілені рівномірно, припущення про те, що в момент часу t +1 третій LFSR не є тактовим, виконується з ймовірністю 25% і зараз:

$$p = \frac{1}{2} + \frac{1}{2}\left(\frac{1}{4}\Pr\{(l_1, l_2) \text{at time } t\}\right) = \frac{1}{2} + \frac{1}{8}\Pr\{(l_1, l_2) \text{at time } t\} \qquad (3.23)$$

Коли:

$$\Pr\{(l_1, l_2) \text{at time } t\} = \frac{\left(\frac{t}{t-l_1}\right)\left(\frac{l_1}{t-l_2}\right)}{2^{3t-(l_1+l_2)}}; \qquad (3.24)$$

Також зауважу, що ¼ $\Pr\{(l_1, l_2 \text{ at time } t\} > \Pr\{(l_1, l_2, l_3) \text{ at time } t\}$, тому це дає нам більшу похибку при оцінці значення лінійних комбінацій $S_i(l_i)$. В таб. 3.1 наведено порівняння цих ймовірностей.

Таблиця 3.2 – Порівняння зміщень Екдаля, Йоханссона та Максимова, Йоханссона, Беббіджа

| $(l_1, l_2, l_3)$, t | $\Pr\{(l_1, l_2, l_3)$ в момент t$\}$ - $10^4$ | ¼$\Pr\{(l_1, l_2)$ в момент t$\}$ - $10^4$ |
|---|---|---|
| (76, 76, 76), 101 | 9.7434 | 22.1207 |
| (79, 79, 79), 105 | 9.2012 | 21.2840 |
| (80, 80, 80), 105 | 6.6388 | 19.3778 |
| (79, 80, 81), 106 | 8.3858 | 20.8899 |
| (82, 82, 82), 109 | 8.7076 | 20.5083 |

Зауважу, що зміщення кореляції можна ще більше покращити, перевіривши значення синхронізуючих відводів C1 та C2. Значення синхронізуючих відводів у момент часу t можна було легко знайти за формулами 3.25 та 3.26.

Після зроблених дій ми маємо два різних випадки. Перший випадок - це коли C1 ≠ C2. Завдяки тактованому механізму, R3 у цьому випадку завжди заведений. Однак у другому випадку, коли C1 = C2, ми отримуємо

двократне збільшення зсуву. У цьому випадку і R1, і R2 синхронізовані, а R3 синхронізується з імовірністю ½. Отже, коли C1=C2, рівняння (3.22) виконується з ймовірністю $\frac{1}{2}+\frac{1}{4}\mathrm{r}\{(l_1,l_2)at\ time\ t\}$ у порівнянні з ймовірністю $\frac{1}{2}+\frac{1}{8}\mathrm{r}\{(l_1,l_2)at\ time\ t\}$.

У таб. 3.3 представлено порівняння описаних атак.

$$C1 = S_1 (l_1 +10) + F_1^j (l_1 +10) \quad (3.25)$$

$$C2 = S_2 (l_2 +11) + F_2^j (l_2 +11) \quad (3.26)$$

Таблиця 3.3 – Порівняння кореляційних атак.

| Атака | Обов'язкові кадри потоку ключів | Середній час обчислення | Коефіцієнт успіху |
|---|---|---|---|
| Екдаль, Йоханссон | 70000 (322 s) | 5 хв | 76% |
| | 50000 (230 s) | 4 хв | 33% |
| | 30000 (138 s) | 3 хв | 3% |
| Максимов, Йоханссон, Беббедж. | 10000 (46 s) | 10 хв | 99.99% |
| | 5000 (23 s) | 10 хв | 85% |
| | 2000 (9.2 s) | 10 хв | 5% |
| Баркан, Біхам | 2000 (9.2 s) | 133 s | 91% |
| | 1500 (6.9 s) | 7.2 хв | 54% |

# Висновок

У першому розділі описується створення GSM та його переваги. Розглянуто архітектуру GSM, включаючи мобільні, базові станції та мережна підсистема. Детально описано різні підсистеми та принципи роботи GSM, включаючи підсистеми базової станції, мережі та управління мережею. Було розглянуто взаємодію мобільних станцій, базових станцій, контролера базової станції та мобільного комутаційного центру.

В другому розділі було розглянуто алгоритм A5, який використовується для шифрування та аутентифікації. Розглянуто різні версії цього алгоритму, такі як A5/0, A5/1 та A5/2, і пояснено причини їхнього застосування в різних регіонах. Також надано структуру та принцип роботи алгоритму A5/1, включаючи використання лінійних регістрів зсуву зі зворотнім зв'язком. Розглянуто проблеми безпеки, пов'язані з використанням старих алгоритмів та можливістю їх копіювання. Зазначено, що атака на криптографічний алгоритм COMP128 є однією з найпоширеніших, що дозволяє зловмисникам отримати секретний ключ Ki. Розглянуто ризики, які пов'язані з фізичним доступом до SIM-карт та можливістю використання підроблених базових станцій для атаки.

В третьому розділі докладно проаналізовано атаки. Розглянуті різноманітні методи, спрямовані на виявлення ключа шифрування, а також зменшення обчислювальних та пам'яттевих витрат для отримання ключа. Атака "розділяй і володарюй" базується на послідовному визначенні окремих станів LFSR, що дозволяє зменшити загальну кількість ключів для перебору. Її суть полягає в вгадуванні нижньої половини кожного регістра та тактуванні шифру до визначення всіх бітів. Отримані лінійні рівняння вирішуються методом Гаусса. Наступна атака компромітує між часом і пам'яттю, використовує генерацію вихідних бітів для певних станів шифру та їх подальше порівняння для визначення ключа. Додатково розглянуто дві атаки, які забезпечують компроміс між робочим часом і пам'яттю проти A5/1. Перша вимагає великої таблиці та невеликих часових витрат, тоді як друга вимагає меншої таблиці, але більше часу на обробку. Наприкінці, представлено кореляційні атаки, які використовують статистичні залежності між послідовностями ключових потоків та регістрами зсуву. Зокрема,

описано метод визначення значень бітів ключового потоку за допомогою кореляційного підходу. Аналіз різних атак дозволяє зрозуміти вразливості мережі GSM.

# ПЕРЕЛІК ПОСИЛАНЬ

1. The Mobile Economy 2023 / K. Okeleke et al. GSMAi Research & analysis. URL: https://data.gsmaintelligence.com/research/research/research-2023/the-mobile-economy-2023.

2. Sherman Y. GSM Security Overview (Part 1): Wireless Telephone History: курс лекцій. 2020. – 22 p.

3. Srinivas S. The GSM Standard (An overview of its security): extended abstract. 2001. – 9 p.

4. GSM Security: конспект лекцій. Helsinki: Helsinki University of Technology, 2003. – 17 p.

5. Pagliusi P. A contemporary foreword on GSM Security. London, 2002. – P. 32.

6. Man Young Rhee, Mobile Communication Systems and Security, Wiley. – 2009.

7. Pacharawit Topark-Ngarm, Panupat Poocharoen, GSM security Vulnerability, Oregon State University, islab.oregonstate.edu. – 2009.

8. Friedhelm Hillebrand, GSM and UMTS: the creation of global mobile communication, Wiley. – 2002.

9. Marc Briceno, Ian Goldberg, David Wagner, An implementation of the GSM A3A8 algorithm, www.gsm-security.net/papers/a3a8.shtml. – 1998.

10. Stuart Wray, COMP128: A Birthday Surprise, www.stuartwray.net. – 2003.

11. Vassilis Prevelakis, Diomidis Spinellis, The Athens Affair, IEEE Spectrum, July. – 2007.

12. John Leyden, SMS security risks highlighted by Friends Reunited hacking case, www.theregister.co.uk. – 2002.

13. Josyula R. Rao, Pankaj Rohatgi, Helmut Scherzer, Stephane Tinguely, Partitioning Attacks: Or How to Rapidly Clone Some GSM Cards, www.research.ibm.com. – 2002.

14. Reinhard Wobst, Cryptology Unlocked, Wiley. – 2007.

15. Ian Goldberg, David Wagner, Lucky Green, The (Real-Time) Cryptanalysis of A5/2, Lecture Notes in Computer Science 2729, Springer Berlin / Heidelberg. – 2003.

16. lad Barkan, Eli Biham, Nathan Keller, Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication, Technion - Computer Science Department - Technical Report CS-2006-07–2006, www.cs.technion.ac.il. – 2006.

17. Jovan Dj. Golić, Cryptanalysis of Alleged A5 Stream Cipher, Lecture Notes in Computer Science 1233, Springer Berlin / Heidelberg. – 1997.

18. K.Y. Lam, I. Shparlinski,H. Wang, C. Xing, Cryptography and Computational Number Theory, Birkhäuser. – 2001.

19. I.C. Göknar, L. Sevgi, Complex Computing-Networks, Springer-Verlag. – 2006.

20. Patrik Ekdahl, Thomas Johansson, Another attack on A5/1, IEEE Transactions on Information Theory 49. – 2003.

21. Alexander Maximov, Thomas Johansson, Steve Babbage, An Improved Correlation Attack on A5/1, Selected Areas in Cryptography 2004. – 2004.

22. Jörg Keller, Birgit Seitz, A Hardware-Based Attack on the A5/1 Stream Cipher, fernuni-hagen.de. – 2001.

23. Timo Gendrullis, Martin Novotný, Andy Rupp, A Real-World Attack Breaking A5/1 within Hours, Lecture Notes in Computer Science 5154, Springer Berlin / Heidelberg. – 2008.

24. Friedhelm Hillebrand, GSM and UMTS: the creation of global mobile communication, Wiley. – 2002.

25. J. Quirke, “Security in the GSM system,” p. 2–13, 01-May 2004.