ХАРЬКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

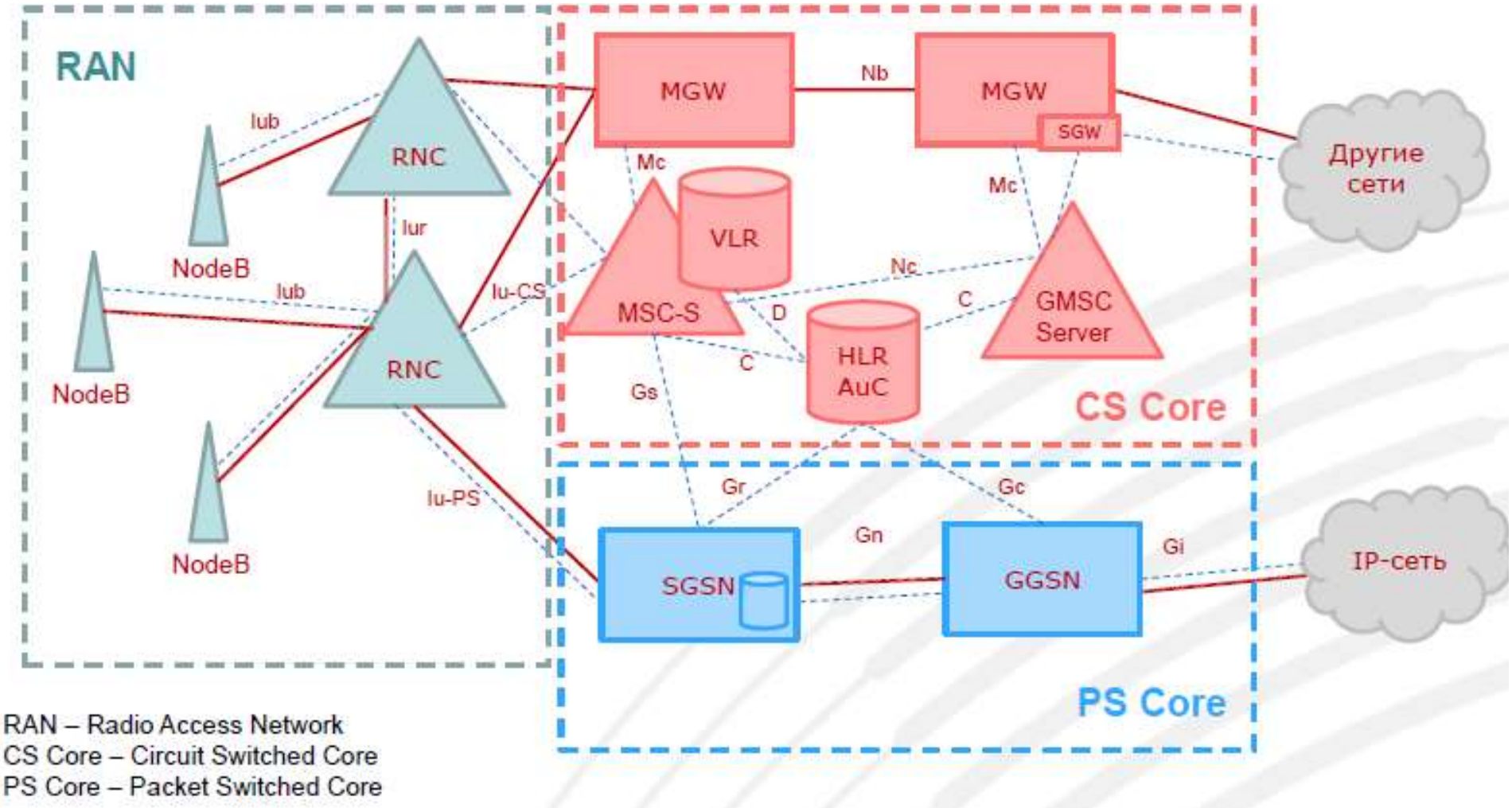
ТЕХНОЛОГІЯ МЕРЕЖ МОБІЛЬНОГО ЗВ'ЯЗКУ UMTS

ЛЕКЦІЯ 9

Доцент кафедри кібербезпеки та ІТ
к.т.н. Лимаренко Вячеслав Володимирович
к.т. 066-0708586 (Viber, Telegram)

Стандарт UMTS

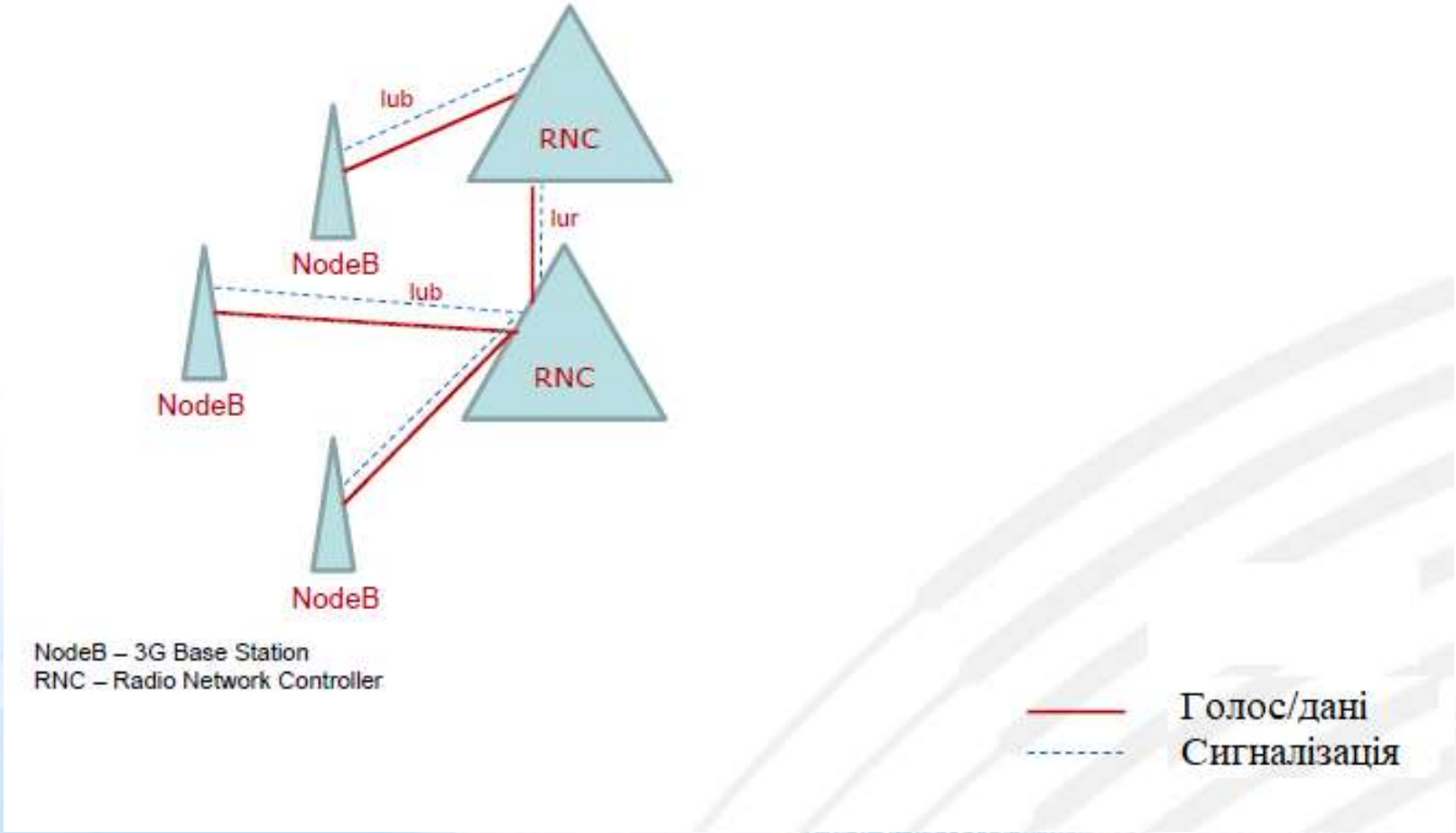
Стандарт UMTS – підсистеми



RAN – Radio Access Network
CS Core – Circuit Switched Core
PS Core – Packet Switched Core

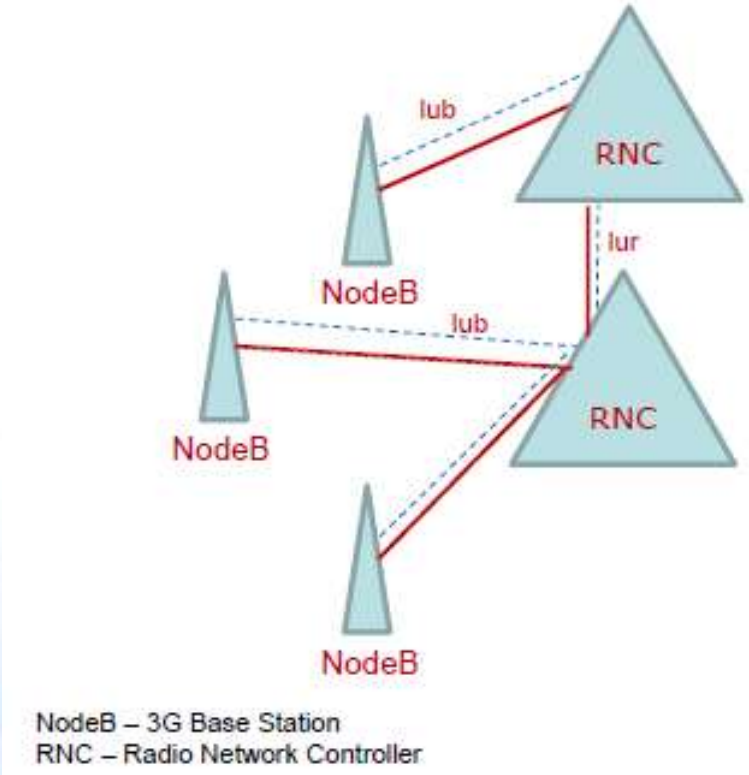
RAN - Підсистема Радіо Доступу
SC Core - Ядро з комутацією каналів
PS Core – Ядро з пакетною комутацією

Стандарт UMTS – Підсистема Радіо Доступу



Node - Базова станція 3G
RNC - Контролер радіомережі

Стандарт UMTS – Підсистема Радіо Доступу

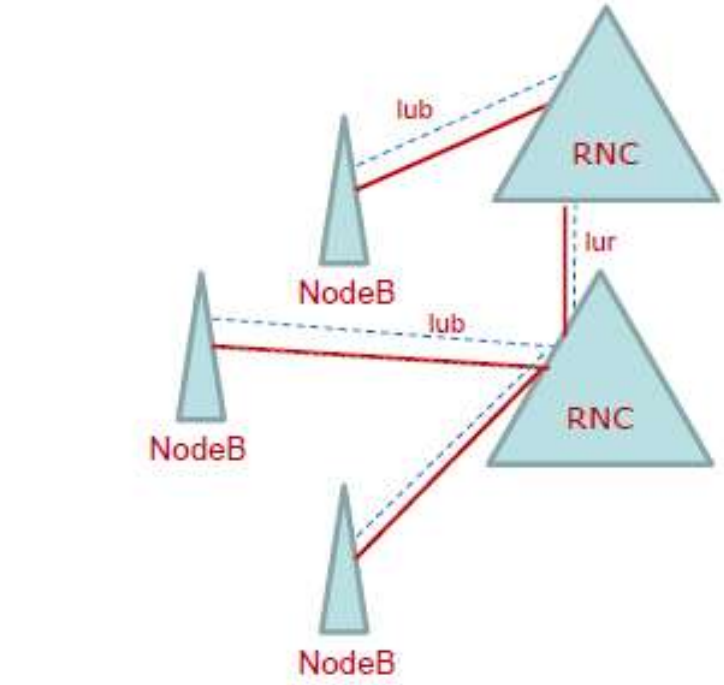


Призначення NodeB:

- Забезпечення радіо покриття.
- Створення з'єднання між мобільним апаратом і системою мобільного зв'язку.

Node - Базова станція 3G
RNC - Контролер радіомережі

Стандарт UMTS – Підсистема Радіо Доступу



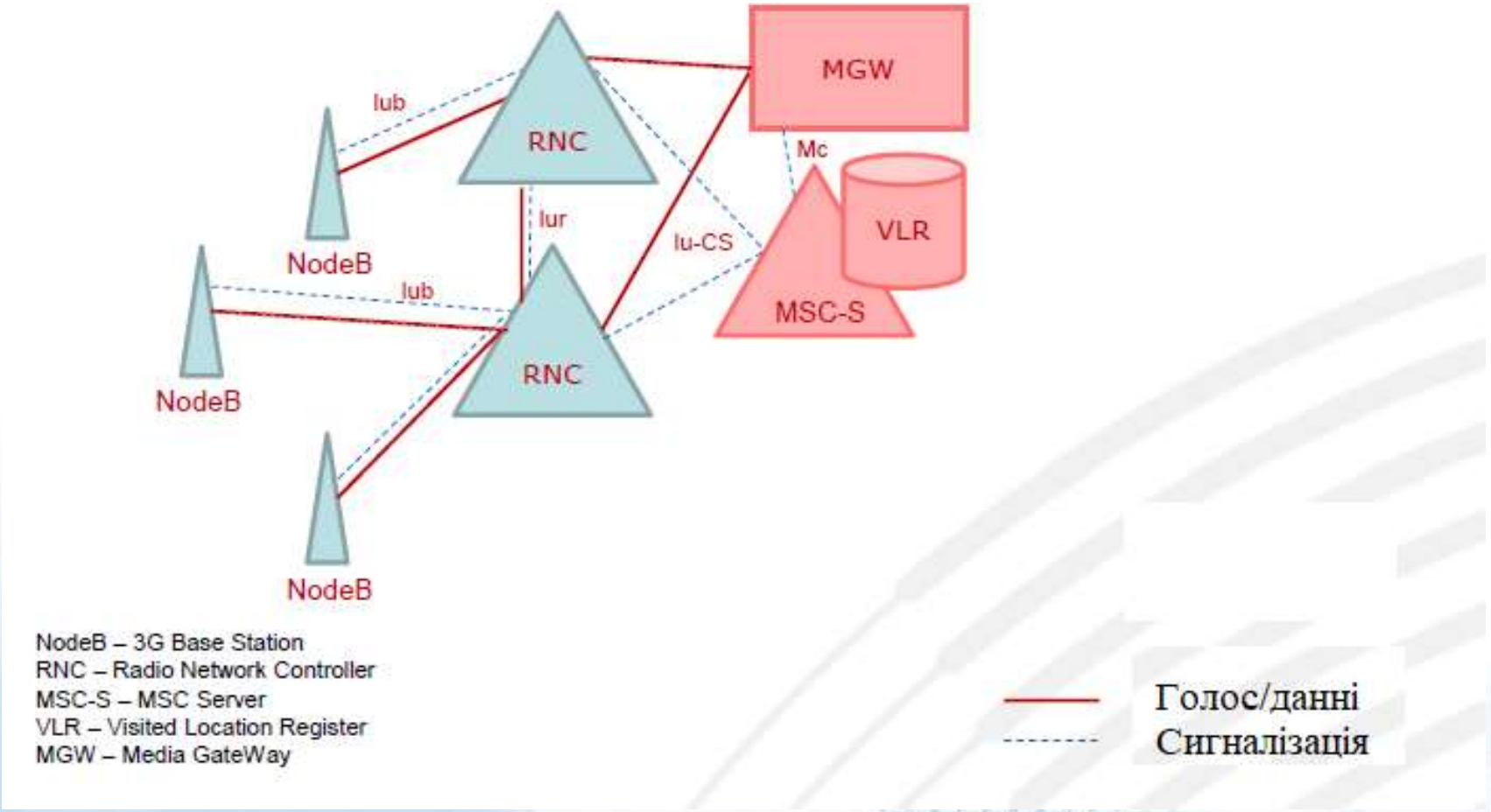
Призначення RNC:

- Управління радіоканалами.
- Керування транспортними каналами між NodeB і RNC.
- Керування транспортними каналами між RNC і Core Network.
- Управління безрозривною передачею з'єднання між NodeB під час розмови або інтернет-сесії.

Голос/дані
Сигналізація

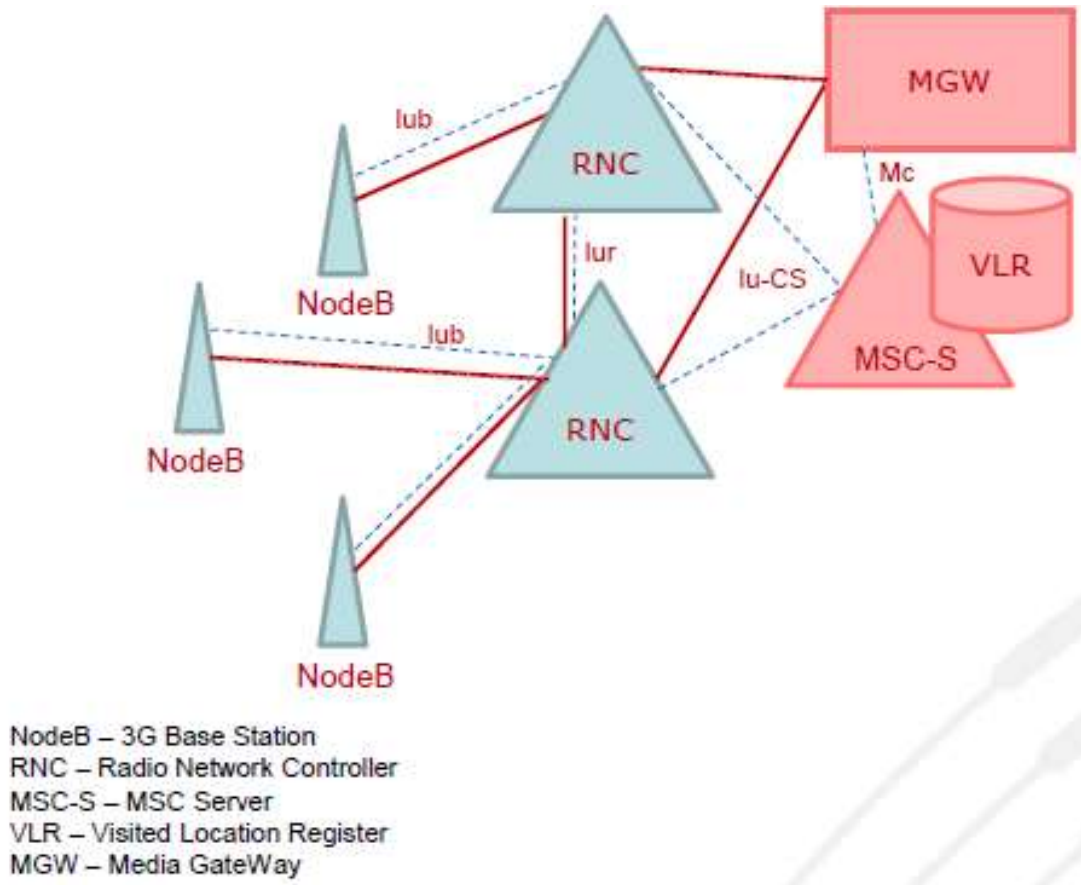
Node - Базова станція 3G
RNC- Контролер радіомережі

Стандарт UMTS – Розподілений Комутатор



Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць

Стандарт UMTS – Розподілений Комутатор

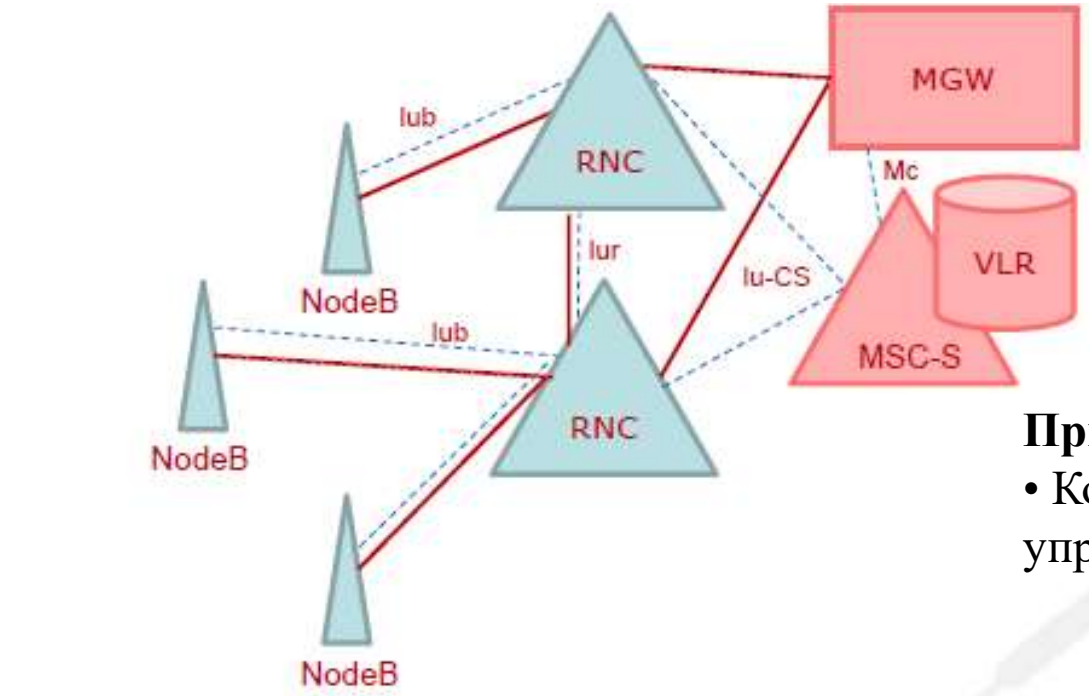


Призначення MSC-S:

- Обробка сигналізації, встановлення з'єднань.
- Управління медіа-шлюзом (MGW).
- Управління хендоверів між двома RNC, між комутаторами, між різними системами доступу.
- Перетворення керуючої інформації (сигналізації) між двома телекомунікаційними системами.

Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць

Стандарт UMTS – Розподілений Комутатор

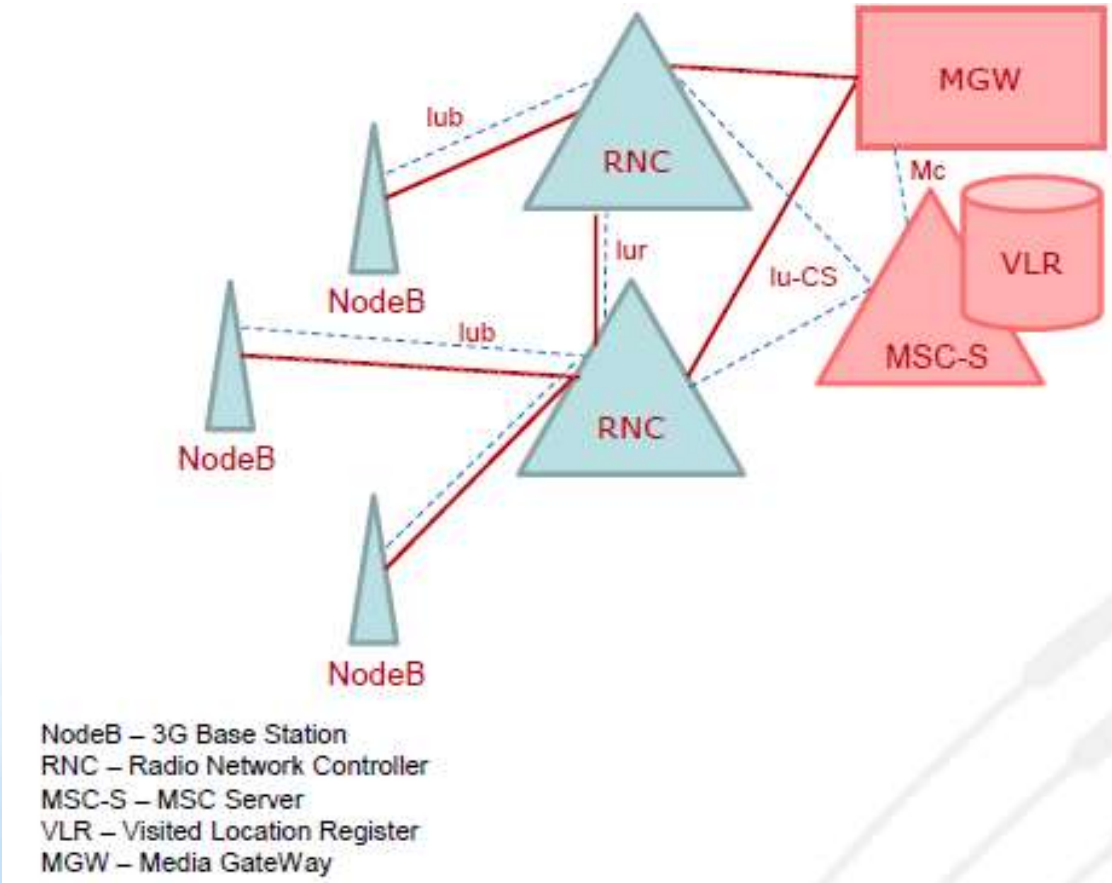


Призначення MGW:

• Комутація голосових каналів під управлінням MSC-S.

Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць

Стандарт UMTS – Розподілений Комутатор



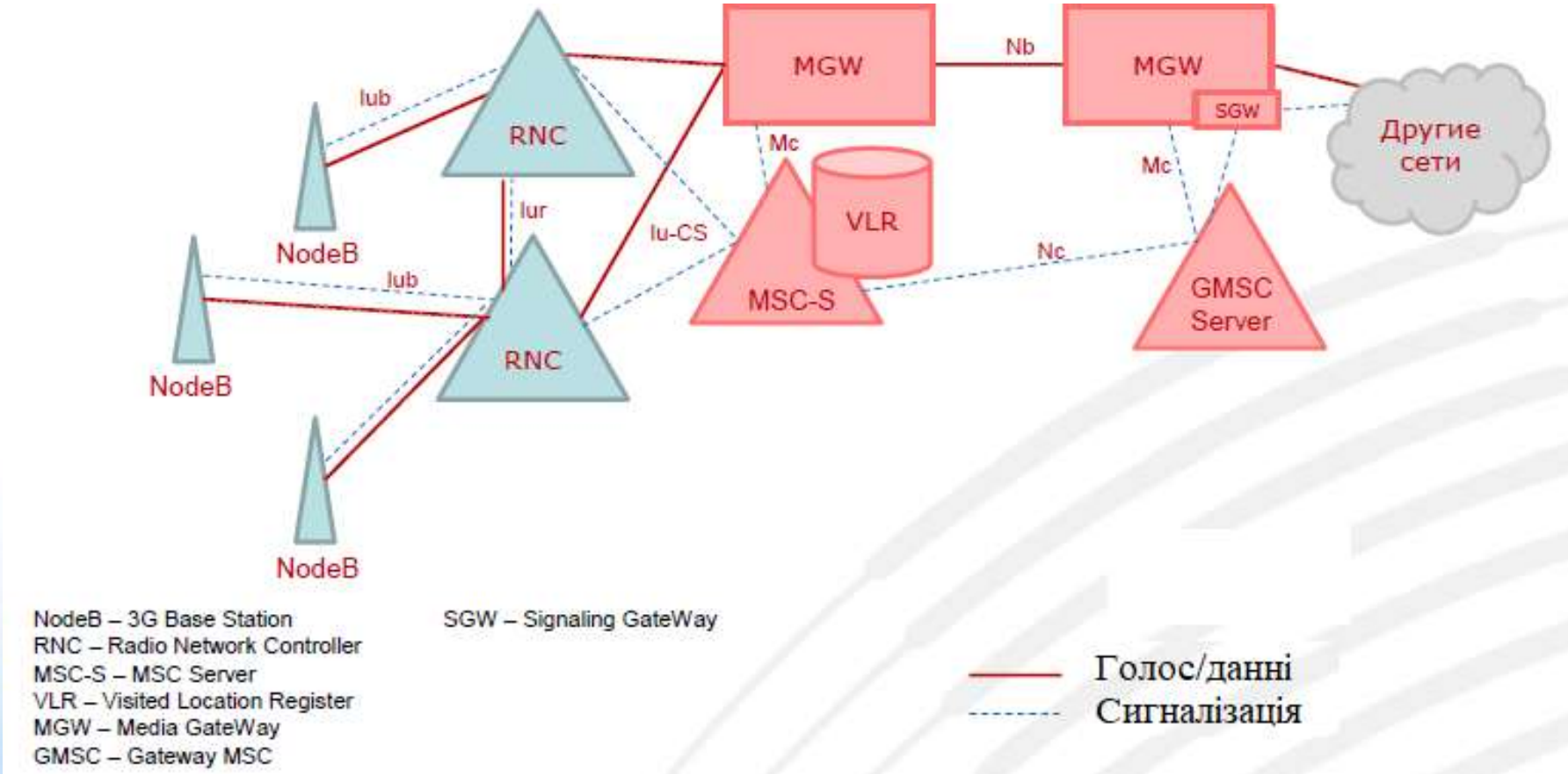
Призначення VLR:

• Зберігання інформації про активних абонентів, що знаходяться в зоні дії свого MSC-S (місце розташування, тимчасові ідентифікатори, дозволені послуги та ін.)

• Участь в аутентифікації абонентів.

Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць

Стандарт UMTS – Розподілений Комутатор

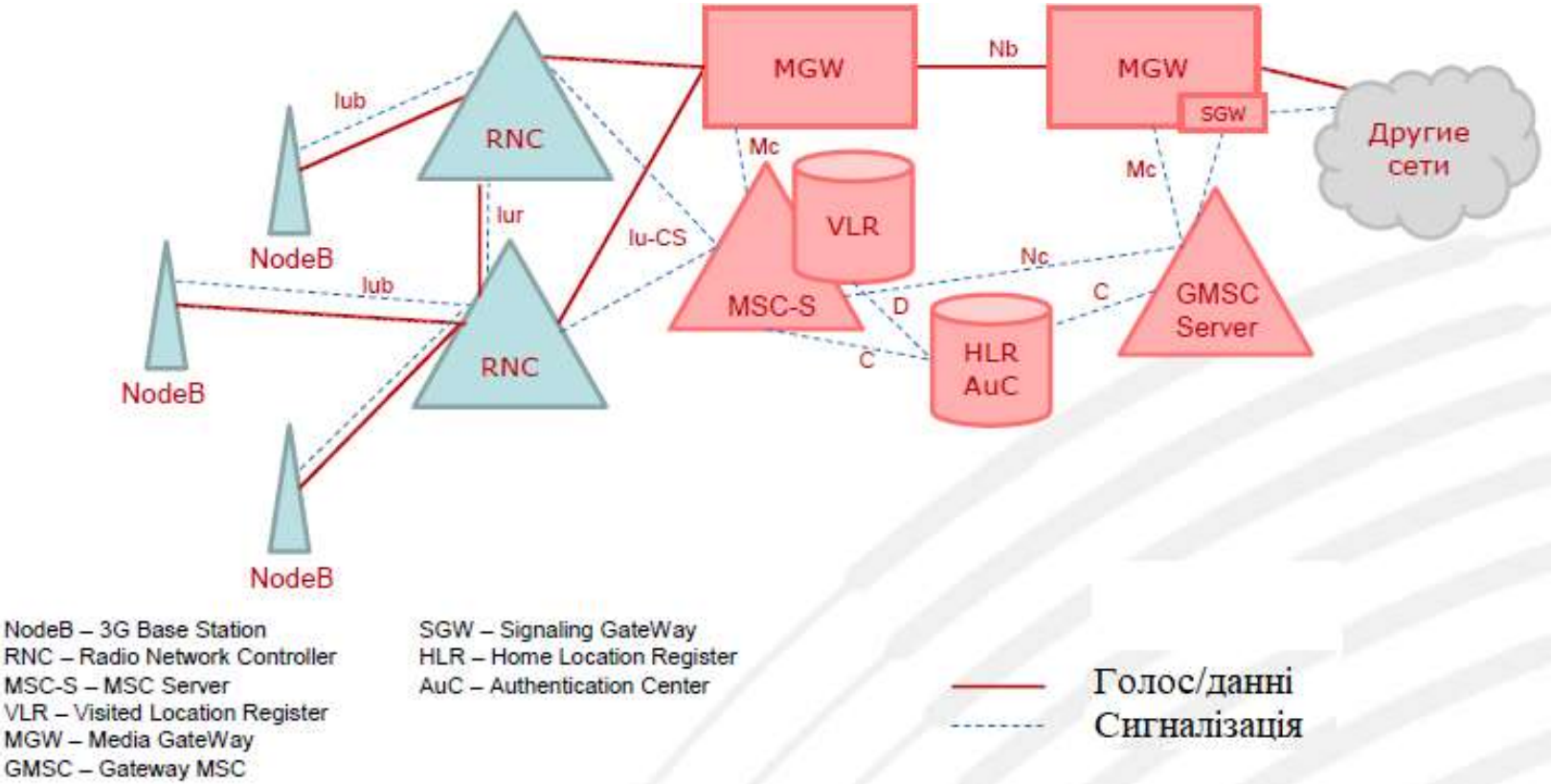


Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць

Призначення GMSC-Server:

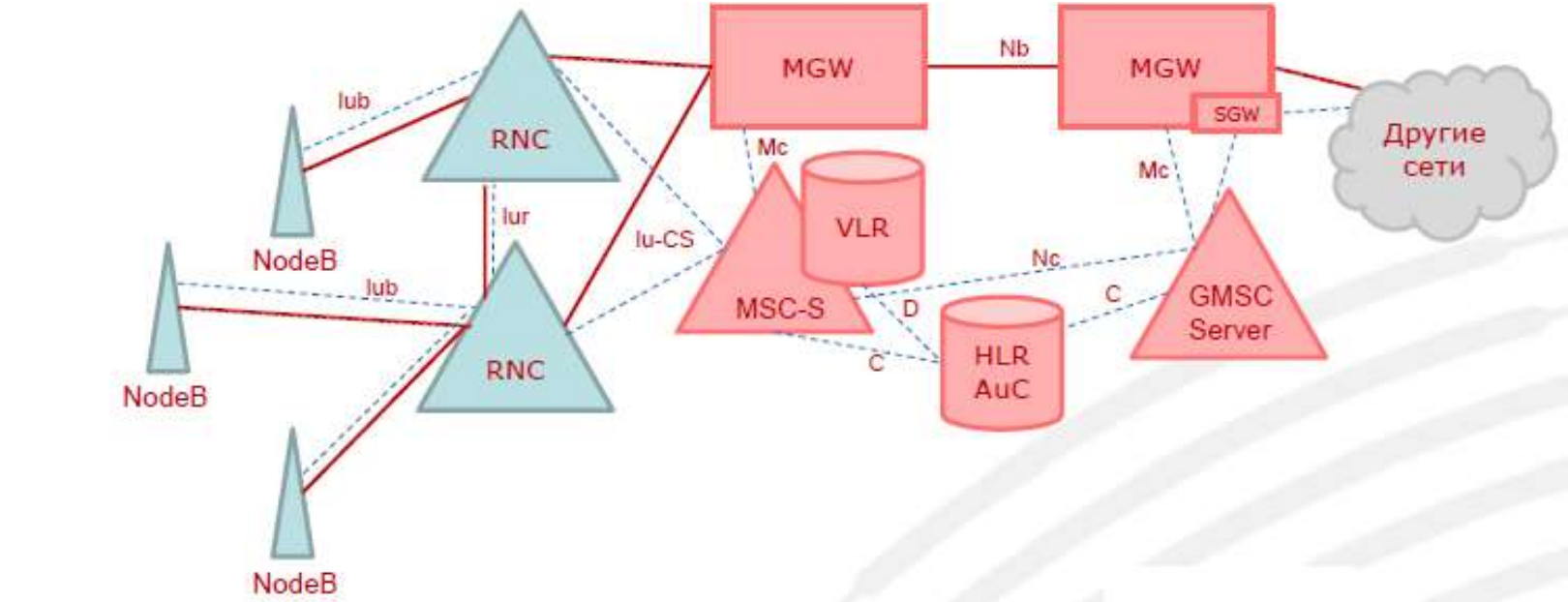
- Отримання від HLR інформації про поточний MSC-S/VLR абонента при вхідному виклику.
- Маршрутизація вхідних викликів на відповідний MSC-Server.
- Управління медіа-шлюзом (MGW).

Стандарт UMTS – Регістр Домашніх Абонентів і Центр Аутентифікації



Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць
HLR - Реєстр домашнього місцезнаходження
AuC - Центр аутентифікації

Стандарт UMTS – Регістр Домашніх Абонентів і Центр Аутентифікації

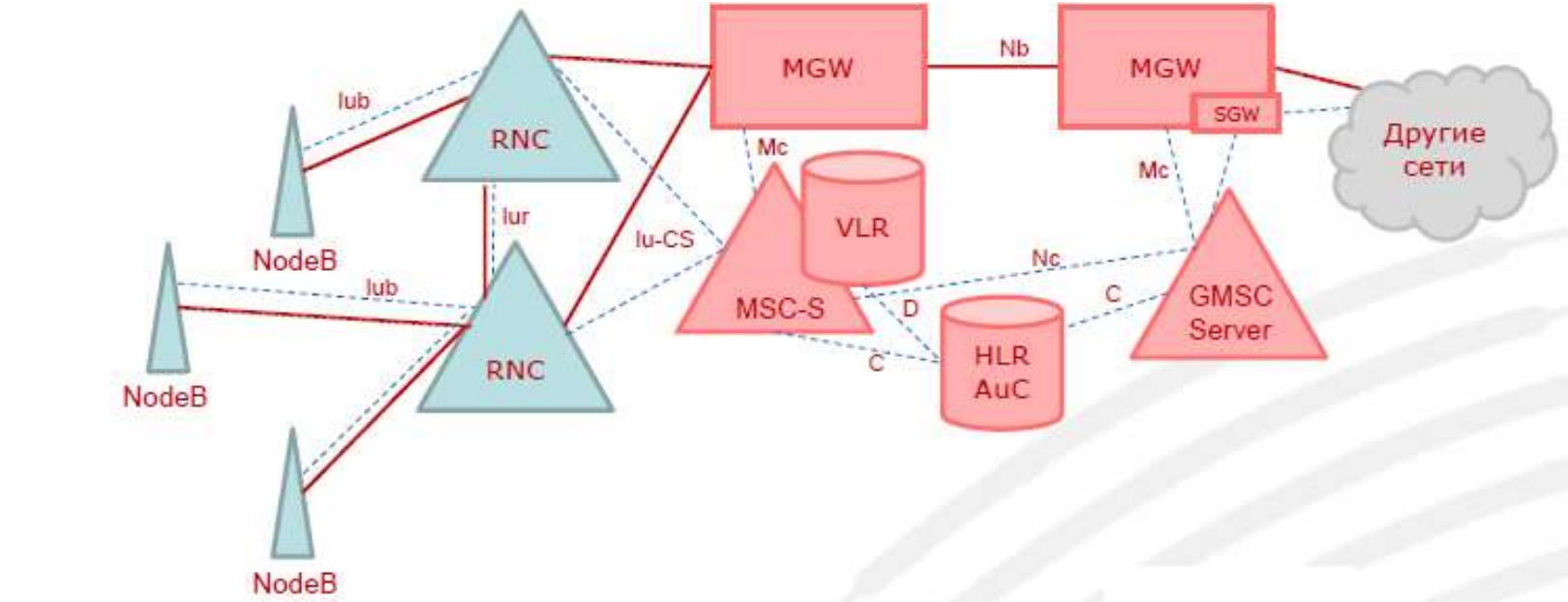


Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць
HLR - Реєстр домашнього місцезнаходження
AuC - Центр аутентифікації

Призначення HLR:

- Зберігання інформації про всіх зареєстрованих абонентів своєї мережі (поточний MSC-S/VLR, ідентифікатори, всі дозволені послуги та ін.)
- Забезпечення керуючої сторони інформацією про поточний MSC-S/VLR абонента.
- Приймає рішення про дозвіл або заборону послуги для абонента.

Стандарт UMTS – Регістр Домашніх Абонентів і Центр Аутентифікації



Призначення AuC:

- Зберігання даних для аутентифікації.
- Забезпечення аутентифікації абонентів.

Node - Базова станція 3G
RNC - Контролер радіомережі
MSC-S - MSC-сервер
VLR - Регістр відвіданих місць
HLR - Реєстр домашнього місцезнаходження
AuC - Центр аутентифікації

Стандарт UMTS – Вузли Підтримки Сервісу Пакетної Комутації

Призначення SGSN (Serving GPRS Support Node, вузол обслуговування абонентів GPRS) **:**

• Маршрутизація пакетів між підсистемою базових станцій і зовнішніми мережами.

• Маршрутизація відеодзвінків.

• Забезпечення мобільності абонентів під час пакетних сервісів (інтернет, ММС, відеодзвінки).

• Участь в аутентифікації абонентів.

• Реєстрація абонентів для забезпечення пакетних сервісів.

• Обробка первинної білінгової інформації і передача її в білінговий центр.

Призначення GGSN (Gateway GPRS Service Node або Gateway GPRS Support Node):

• Шлюз в зовнішні IP мережі.

• Динамічна роздача IP адрес.

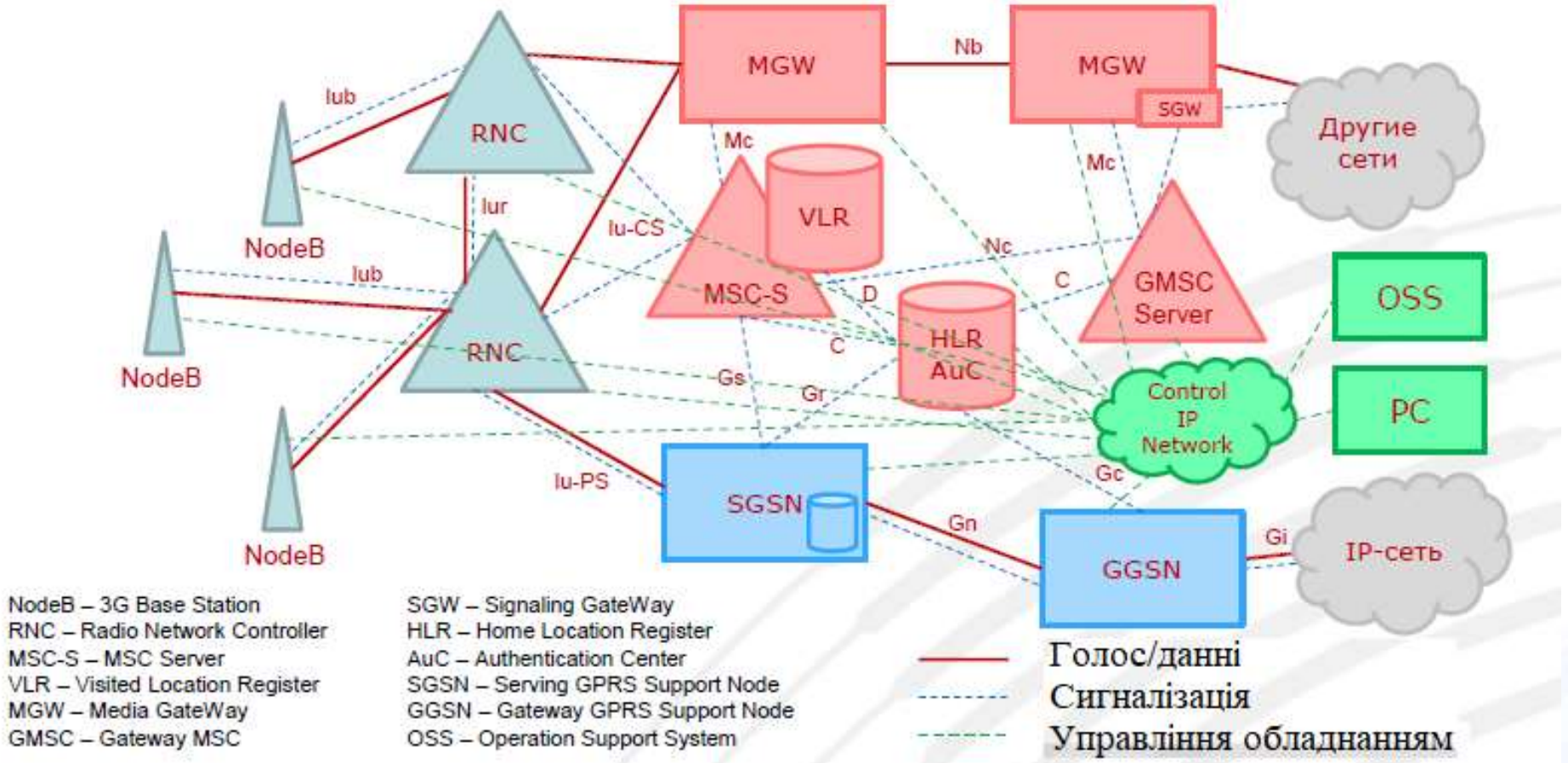
• Забезпечення запитів на аутентифікацію до RADIUS сервера.

• Зберігання баз даних маршрутизації, адрес і фільтрів.

• Отримання від HLR інформації про поточний SGSN абонента при вхідному відеодзвінкі.

• Маршрутизація вхідних відеодзвінків на відповідний SGSN.

Стандарт UMTS – Підсистема Підтримки Управління



OSS - Система підтримки управління

- Перехід голосового трафіку в пакети - IP або ATM.
- Транспортний рівень сигналізації - IP/SCTP.
- Технологія SS7 через IP отримала назву SIGTRAN.

ОСНОВНІ АЛГОРИТМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В 3G

Перед початком обміну інформацією кожна сторона повинна переконатися в тому, що спілкується саме з тим, хто їй потрібен, а не зі зловмисником, що імітує співрозмовника з метою перехоплення цієї інформації. У разі каналу радіо зв'язку мобільних мереж такими сторонами є Абонент (User Equipment кінцевого користувача) і Мережа (передавальний вузол провайдера мобільного зв'язку). Основні поняття, якими оперують в цьому питанні це:

- ***домашнє оточення і аутентифікаційний центр;***
- ***ідентифікаційні модулі користувача (USIM або UICC);***
- ***регістри місця розташування користувача (VLR).***

АУТЕНТИФІКАЦІЯ І ВИРОБЛЕННЯ КЛЮЧА

Кожне поняття визначено стандартомі виконує строго певні функції. Аутентифікаційні центр (AuC) і USIM зберігають по копії основного ключа абонента, на основі якого будується спілкування абонента з мережею. За запитом яка обслуговує мережі AuC виробляє таблицю з n (обичнon = 5) п'яти роздільних аутентифікаційних векторів. Компонентами кожного вектора є: випадкове число RAND, очікувана відповідь XRES, ключ шифрування CK, ключ цілісності IK і маркера утентіфікації AUTN, з яких останні 4 компоненти виходять з RAND, K і порядкового номера вектора SQN.

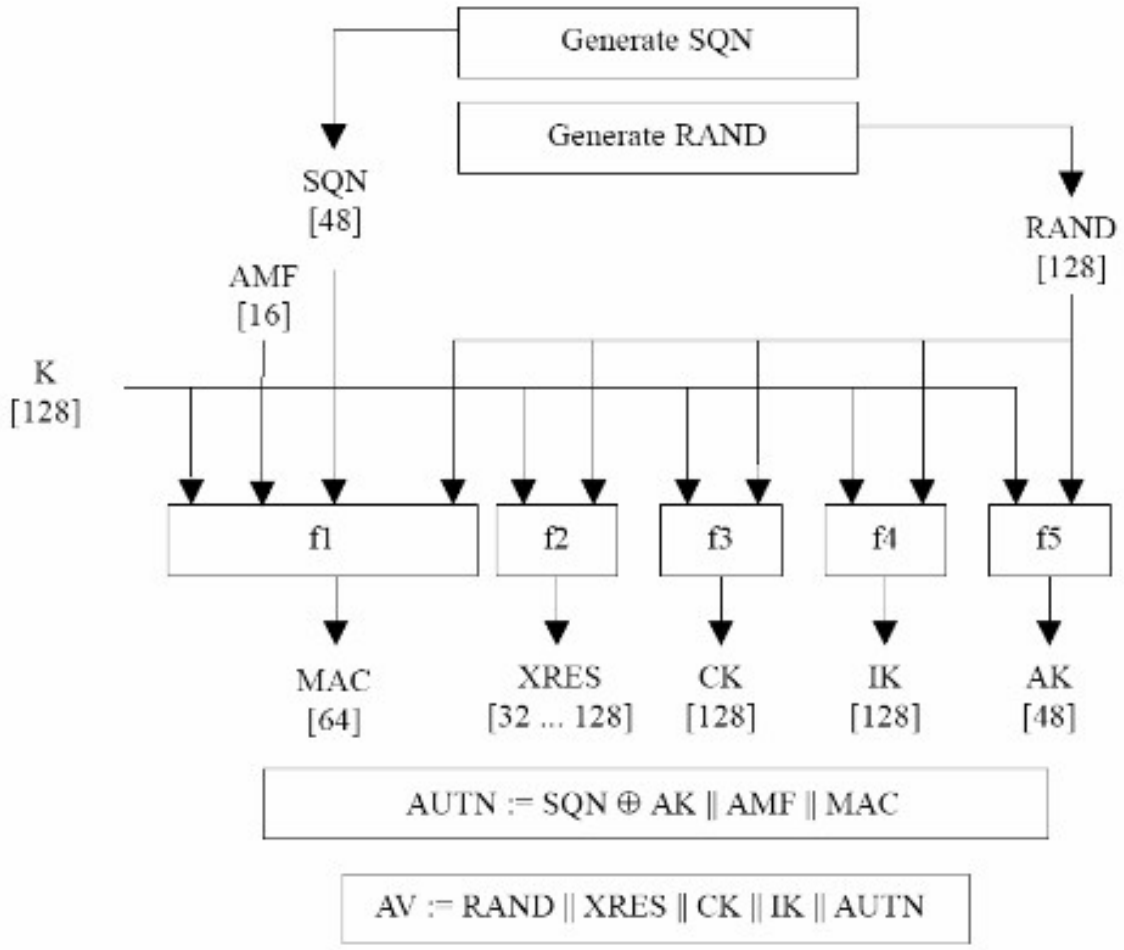


Рисунок 1. Генерація аутентифікаційних векторів

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

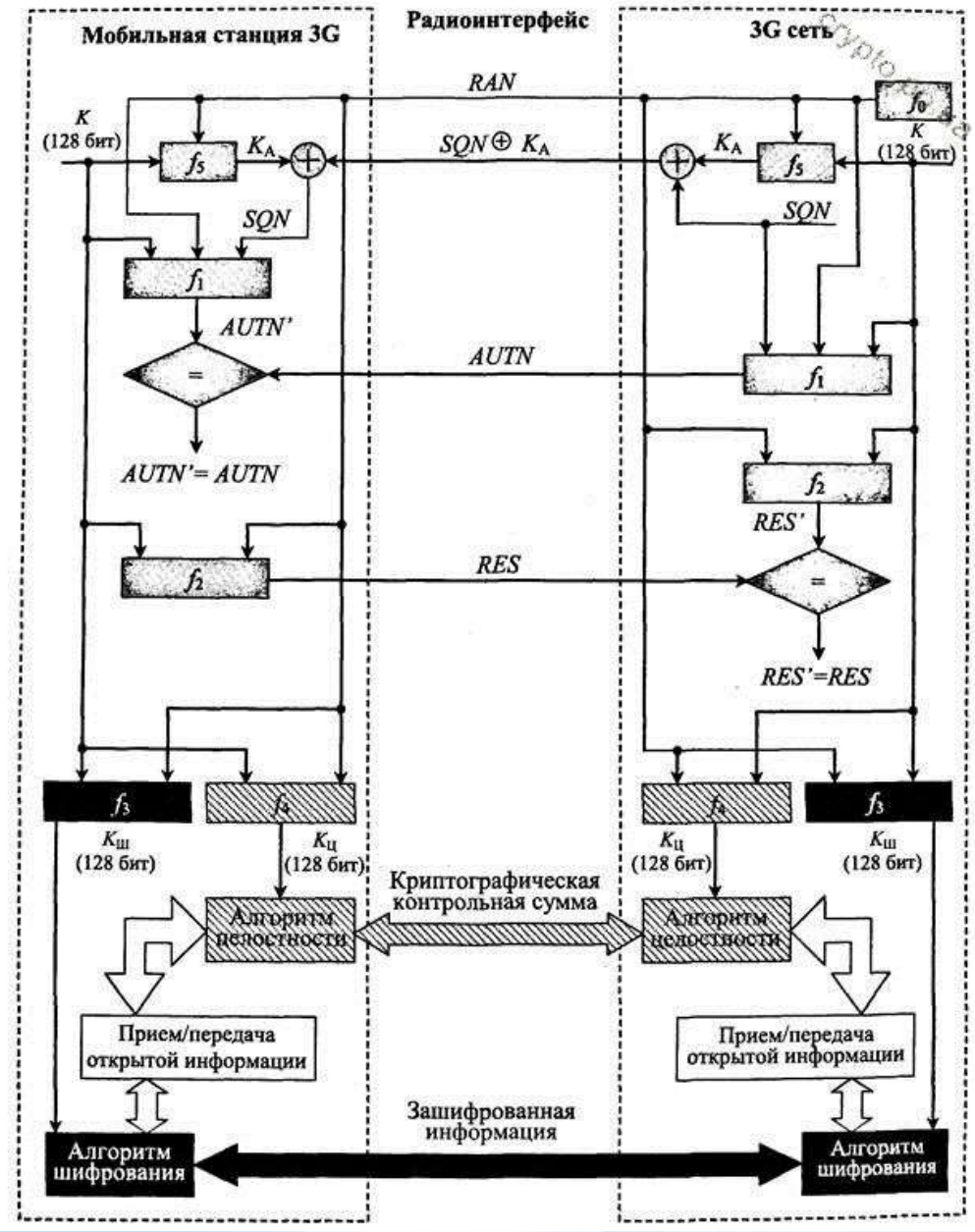


Рисунок 2. Узагальнена схема аутентифікації і криптозахисту в 3G

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

Процедура аутентифікації МС мережею нагадує аналогічну процедуру в GSM. МС обчислює параметр RES («відгук» - response) за допомогою функції f2, на вхід якої надходить секретний ключ К і прийняте число RAND. Параметр RES передається в мережу, яка виробляє аналогічні обчислення, отримує RES 'і порівнює його з RES. Якщо два значення рівні, мережа визнає МС «своєю». Таким чином, в 3G передбачені процедури підтвердження достовірності, як самої МС, так і безпосередньо мережі. Модуль ідентичності користувача 3G в разі фрода (спробі обману) може відхилити послуги мережі, в якій йому належить реєструватися. Така можливість була відсутня в системі GSM.

Для забезпечення криптографічного захисту інформації в каналі зв'язку мережу і МС, використовуючи функції f3 і f4, генерують ключі шифрування і перевірки цілісності. Вхідними параметрами при цьому є числа RAND і К. Довжина кожного ключа - 128 біт. Після цього сторони можуть здійснювати потокове шифрування переданих даних. Перевірка цілісності повідомлень проводиться шляхом формування та перевірки криптографічних контрольних сум.

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

В рамках загальної концепції стандарту функції, що відповідають за шифрування і цілісність визначили як f3 і f4. З урахуванням специфіки використовуваного каналу і переданих даних, а також технологічних можливостей попроізводству обслуговуючих схем, для f3 і f4 були визначені наступні вимоги:

- f3 повинна являти собою потоковий шифр;
- f4 повинна бути функцією множення / підсумовування;
- обидві функції повинні задовільно вважатися на невеликих чіпах з низьким енергоспоживанням;
- неповинно бути обмежень по заміні цих функцій на терміналах (в абонентському обладнанні);
- поширення мережевого обладнання повинно бути відповідно до Вассенарскімі угодами.

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

1994р. Міцуру Мацуї (Mitsuru Matsui) запропонував лінійний криптоаналіз для DES, що дозволяють за розумний час зламувати мало раундові реалізації цього шифру. Дана обставина привела його до розробки в 1997р. нового блочного шифру з 128-бітовим ключем, 64-бітними блоками і варійованою кількістю ітерацій. Цей шифр, названий, MISTY, виявився набагато більш стійким, ніж DES, і був використаний в якості ядра для f3. Ключ в MISTY складається з 16 подключей: K0, ..., K7 і K8, ..., K15 - після кожної ітерації з'єднання і в групах циклічно зсуваються на 1. перші 8 ключів виходять простим розбиттям головного ключа, а друга група може бути отримана шляхом зашифровування першої групи за допомогою елементарної ітерації MISTY: K0, зашифрований на K1 дає K8 і т.д. послідовно.

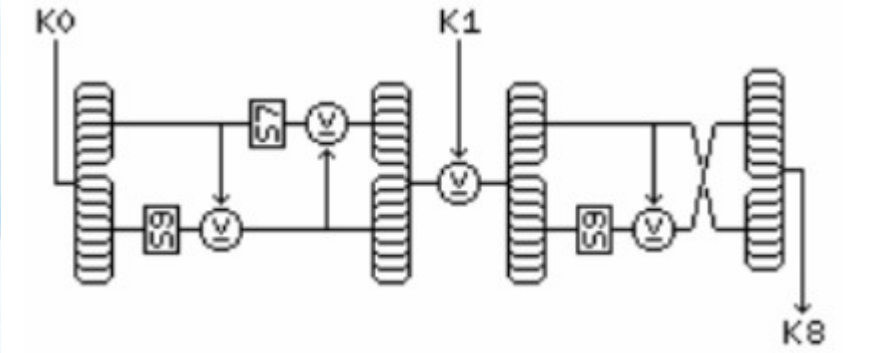


Рисунок 3. Отримання другої групи підключів

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

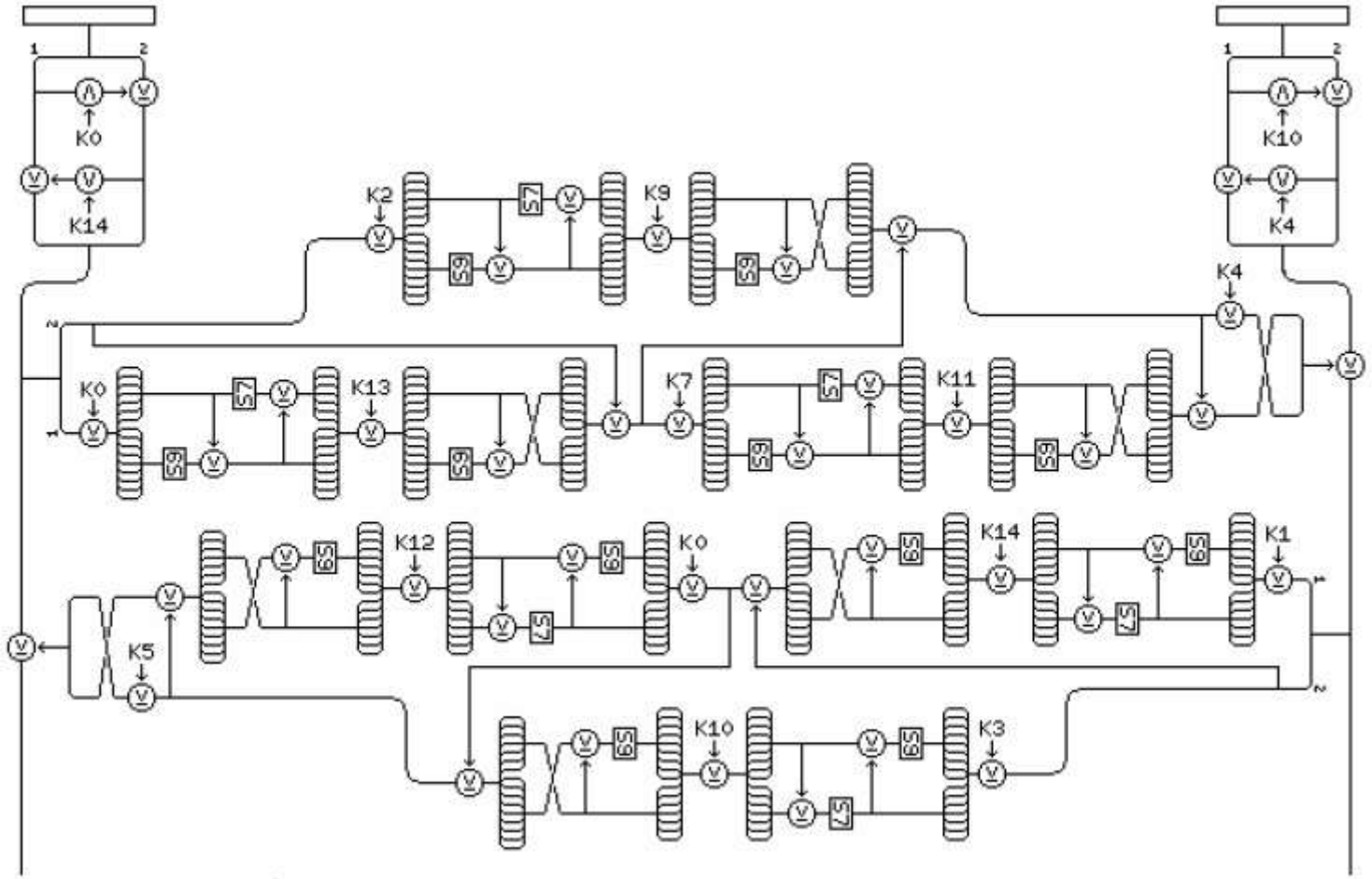


Рисунок 4. Схема роботи MISTY

АУТЕНТИФІКАЦІЯ І СТВОРЕННЯ КЛЮЧА

ПОТОЧНИЙ ШИФР F3

Для того, щоб ядро задовольняло вищевказаним вимогам стандарту, його злегка модифікували, і був отриманий блоковий шифр KASUMI. Детальний опис підсумкового шифру, отриманого з KASUMI, дається в [3GPP TS 35.201]. Для перетворення блокового MISTY в потоковий KASUMI була використана комбінація зворотного зв'язку по виходу і режиму лічильника. Схема роботи f4 представлена на ілюстрації нижче.

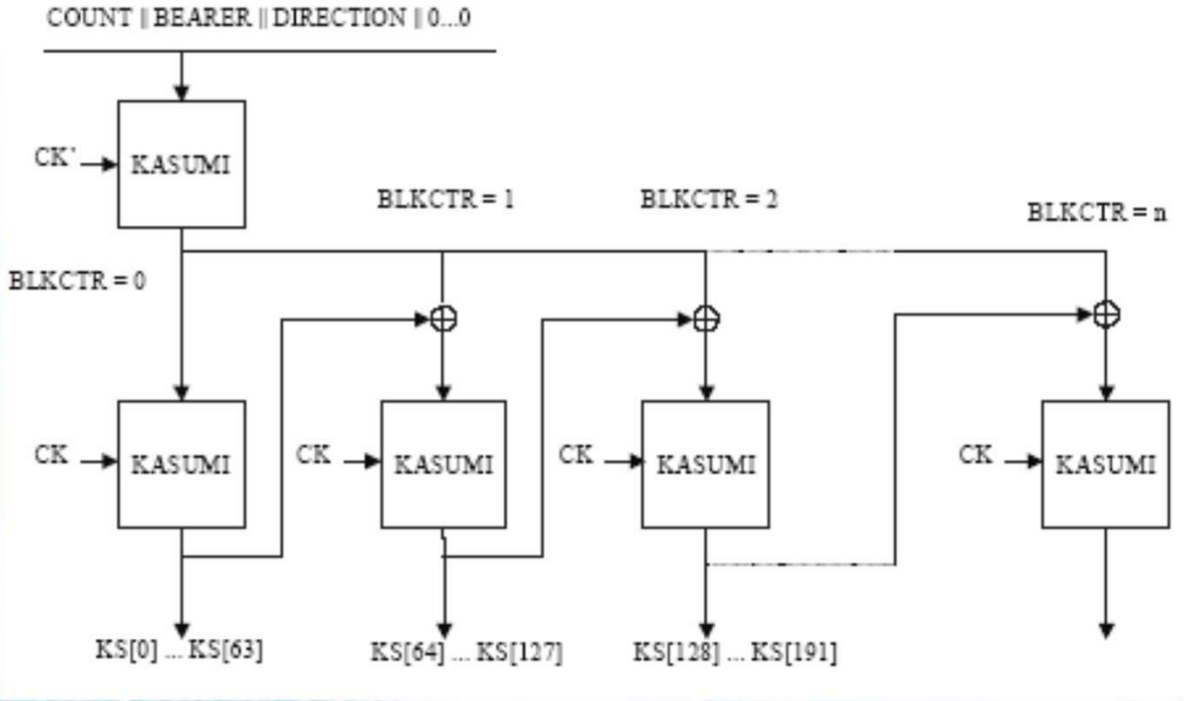


Рисунок 5. F3—KASUMI

ПОТОЧНИЙ ШИФР F3

Для того, щоб ядро задовольняло вищевказаним вимогам стандарту, його злегка модифікували, і був отриманий блоковий шифр KASUMI. Детальний опис підсумкового шифру, отриманого з KASUMI, дається в [3GPP TS 35.201]. Для перетворення блокового MISTY в потоковий KASUMI була використана комбінація зворотного зв'язку по виходу і режиму лічильника. Схема роботи f3 представлена на ілюстрації нижче.

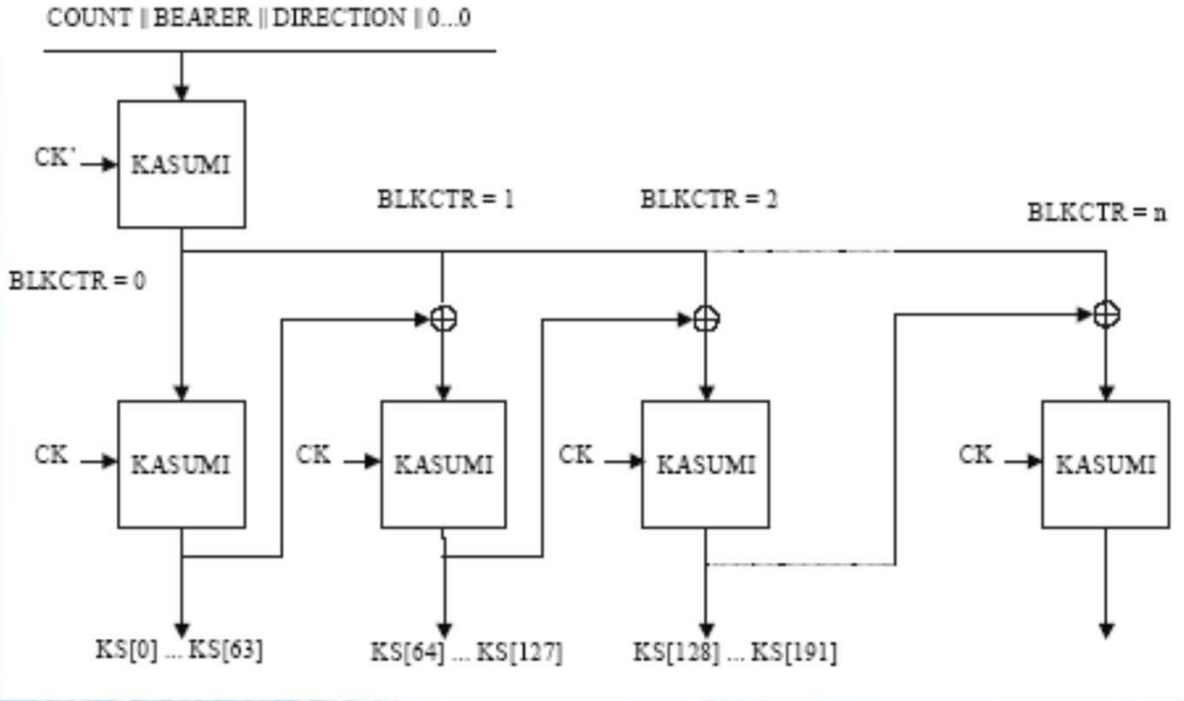


Рисунок 5. F3—KASUMI

АЛГОРИТМ ПЕРЕВІРКИ ЦІЛІСНОСТІ В UMTS

Функція f4 є послідовну функцію множення-накопичення з KASUMI в ядрі. До кожного відсилають повідомлення прикріплюється MAC-I (32-х бітна псевдовипадковий рядок - вихід f4), і такий же рядок обчислюється приймаючою стороною. Справа в тому, що вихід функції f4 практично непередбачуваним чином залежить від вхідних параметрів, так що тільки правильне поєднання IK і лічильника несе відповідальность за достовірність отриманого повідомлення.

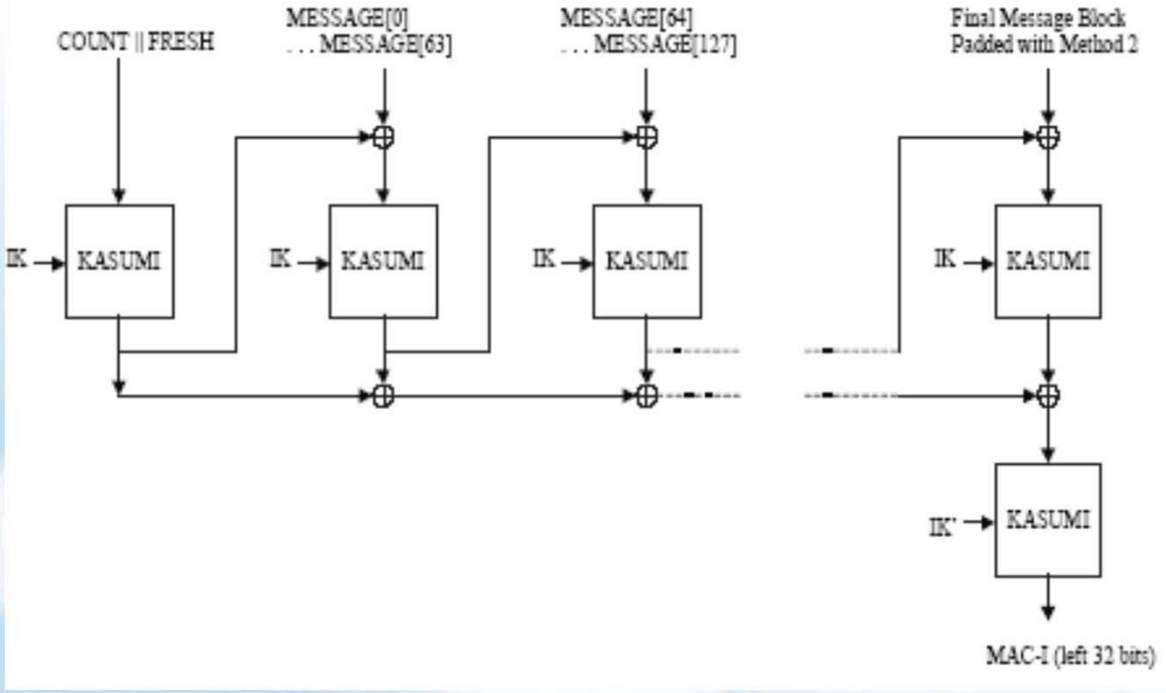


Рисунок 6. Генерация MAC-I