Захист інформації в інформаційно-комунікаційних системах
Ч.1

Лекція 13

Безпека CDMA

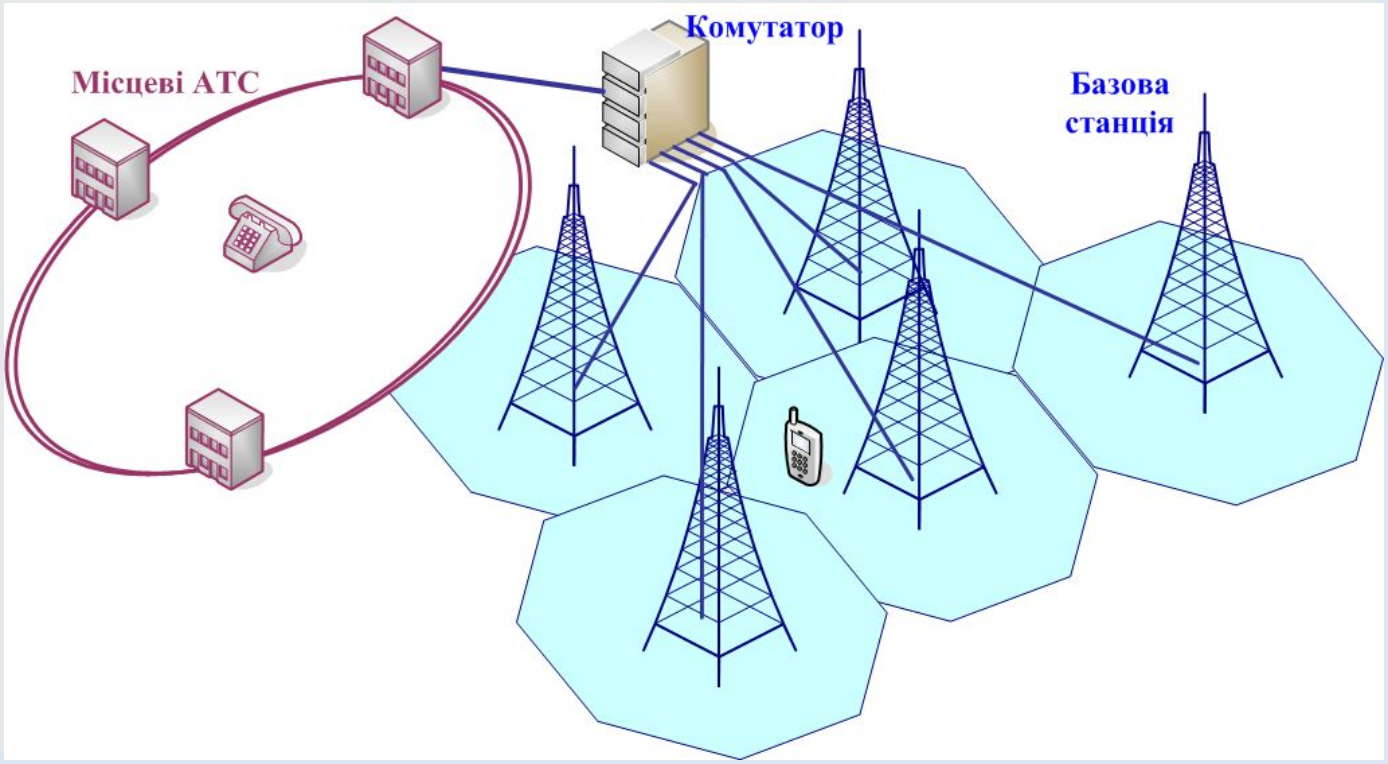
“Захист сильний настільки, наскільки сильною є його найслабша ланка”
Отже “Немає необхідності атакувати найсильнішу ланку, якщо її можна обійти”
“Підсилювати необхідно не тільки найслабшу ланку”

Структура стільникового зв'язку

Дальність дії мобільного стільникового телефону забезпечує стільникова структура зон зв'язку.

Вся територія, що обслуговується стільниковою системою зв'язку, розділена на окремі прилеглі один до одного зони зв'язку (стільники).

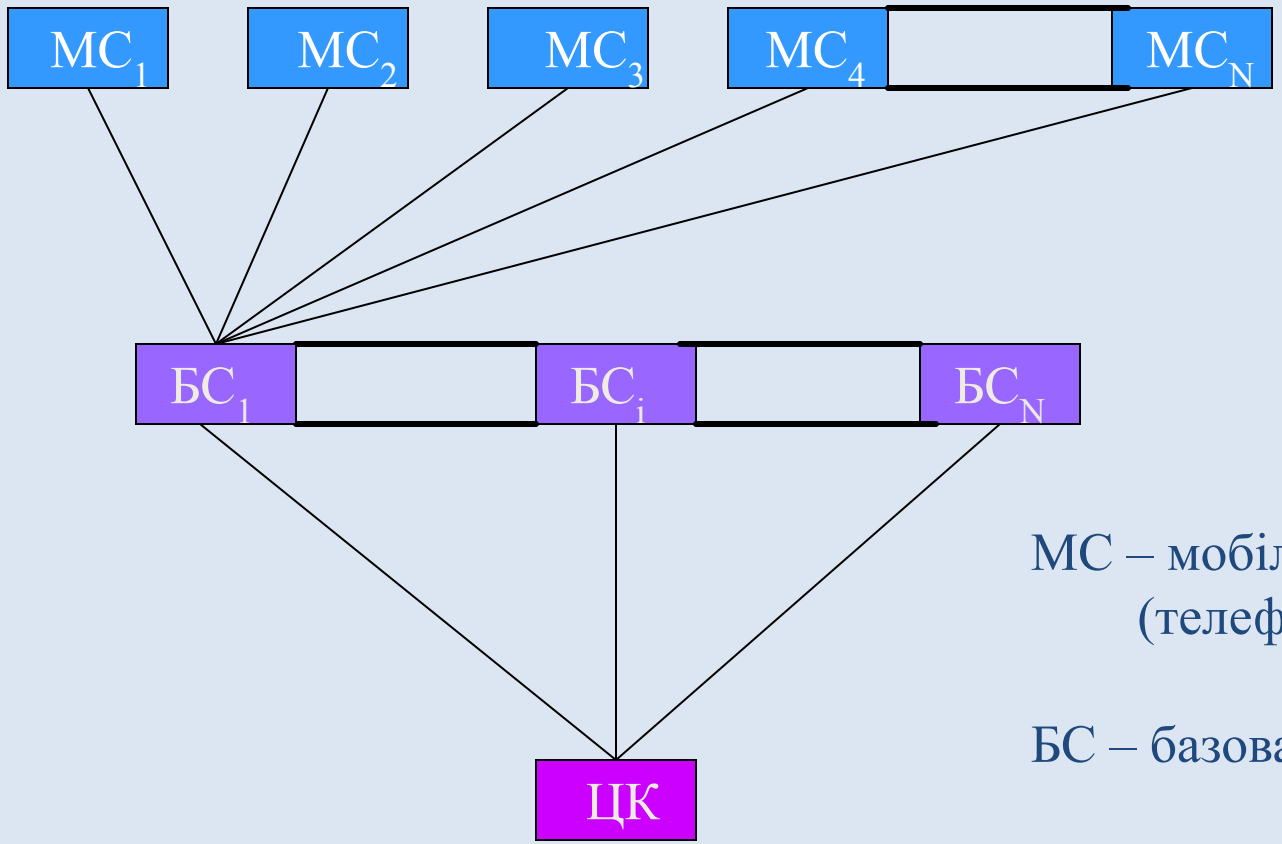
Структура стільникового зв'язку



Телефонний обмін в кожній зоні управляється базовою станцією (БС), здатною приймати і передавати сигнали на великій кількості радіочастот.

Крім того, БС підключена до телефонної мережі фіксованого зв'язку і оснащена апаратурою перетворення високочастотного сигналу стільникового телефону в низькочастотний сигнал телефону фіксованого зв'язку і навпаки, чим забезпечується з'єднання обох систем.

Структура стільникового зв'язку



МС – мобільна станція (телефон)

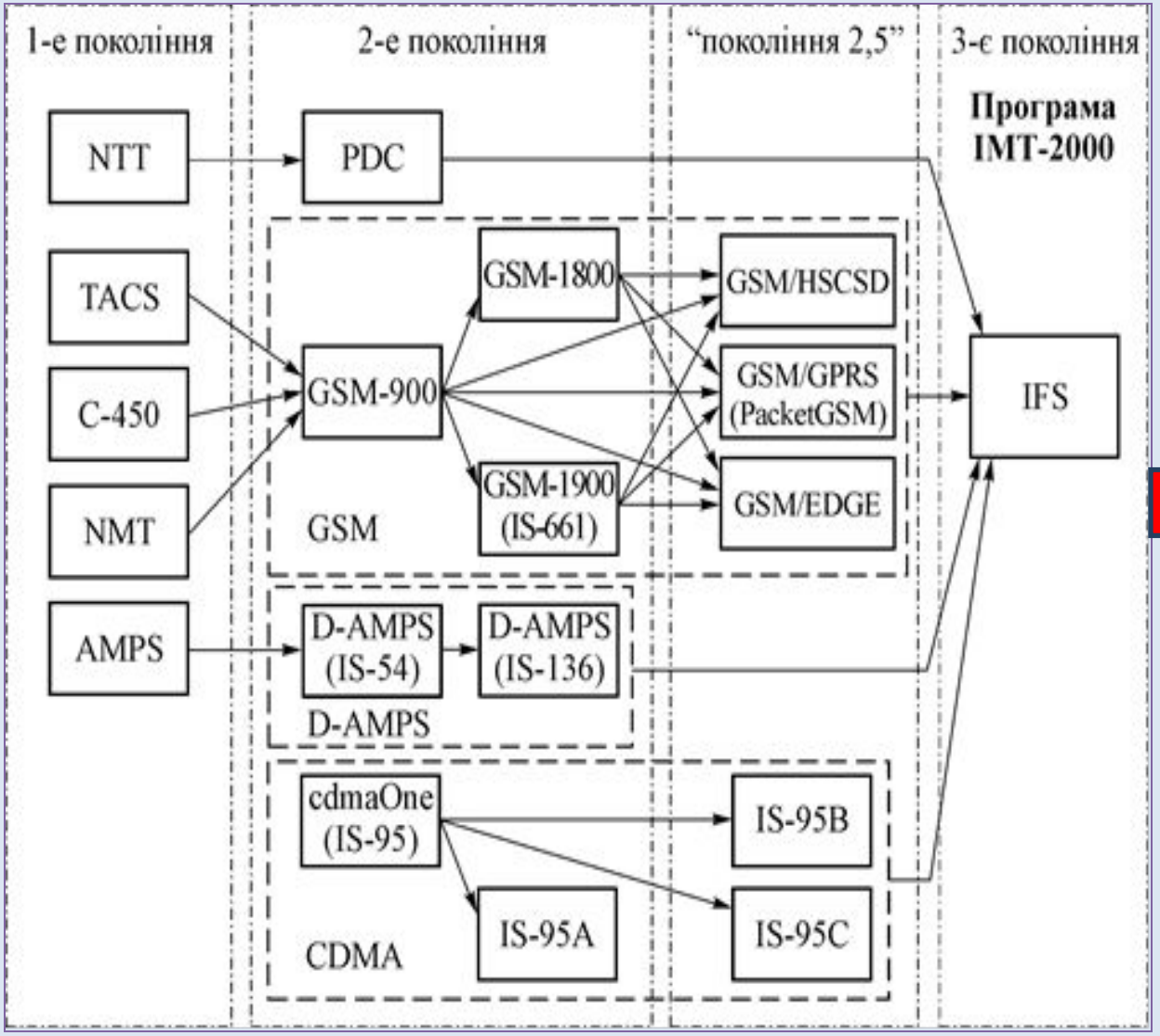
БС – базова станція

ЦК – центр комутації

Технології багатоканального доступу

FDMA	TDMA	CDMA
багатоканальний доступ з частотним розділенням	**багатоканальний доступ з часовим розділенням**	**багатоканальний доступ з кодовим розділенням**
З доступного діапазону абоненту виділяється своя смуга частот, яка може використовуватися 100% часу	Всі абоненти використовують один діапазон частот, але при цьому мають часові обмеження доступу	Кожному абоненту привласнюється окремий код, який поширюється по всій ширині смуги **(дуже широкої)**
Для розділення (диференціації) абонентів використовуються відмінності в частоті	Кожному абонентові виділяється часовий проміжок (кадр), в якому йому дозволяється "мовлення". Після того, як один абонент завершує мовлення, дозвіл передається іншому, потім третьому і так далі	Мовлення абонентів накладається, але оскільки їх коди відрізняються, вони можуть бути легко диференційовані
інформація передається в реальному часі, і використовується вся смуга пропускання	Чим більше абонентів, тим рідше кожному з них надається можливість передати свої дані	Не існує часового або частотного розділення, і всі абоненти постійно використовують всю ширину каналу
Аналогові та цифрові системи стільникового зв'язку	TDMA, як правило, накладається на FDMA і мовлення ведеться у виділеній смузі частот	**CDMA**

Покоління мереж стільникового зв'язку



4-е покоління

WiMAX

LTE

Характеристики цифрових стандартів стільникового зв'язку

Характеристика	GSM-800/ 1800/1900	CDMA (IS-95)
Діапазон робочих частот, МГц: •для передавання МС •для передавання БС	890-915/1710-1785/1850-1910 935-960/1805-1880/1930-1990	 824-849 869-894
Радіус стільників, км	GSM-800 (0,5…35); GSM-1800/1900 (0,5…6)	0,5…25
Дуплексне рознесення каналів, МГц	45/95/80	45
Ширина смуги частот радіоканалу, кГц	200	1288,8
Число частотних каналів (несучих), од.	124/374/239	20
Число каналів на одну несучу, од.	8 або 16	66
Швидкість перетворення мовлення, кбіт/с	13 або 6,5	13 або 8,55
Швидкість передавання інформації в радіоканалі, кбіт/с	270,833	1288,8
Швидкість передавання інформації у фізичному каналі, кбіт/с	9,6; 14,4	1,2; 2,4; 4,8; 9,6; 14,4

Стандарти CDMA

CDMA one

IS 95 | IS 95B | JSTD 008

Вузька смуга

CDMA 2000

CDMA 2000

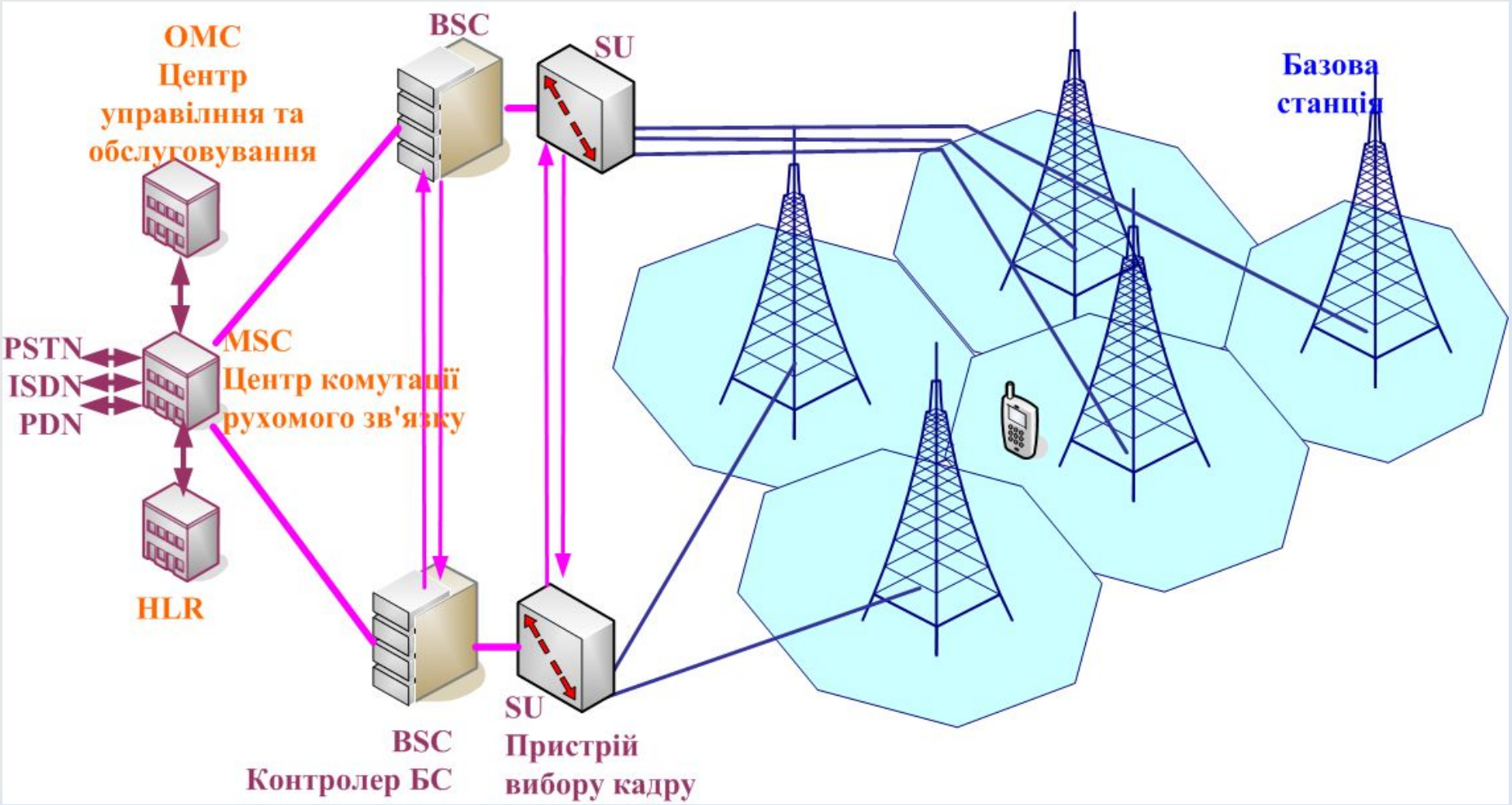
Широка смуга

CDMA - Багатоканальний доступ з кодовим розділенням каналів

На відміну від інших технологій радіозв'язку, в яких наявний частотний спектр розбивається на вузькосмугові канали та часові інтервали, **в CDMA сигнали розподіляються в широкій смузі частот**.

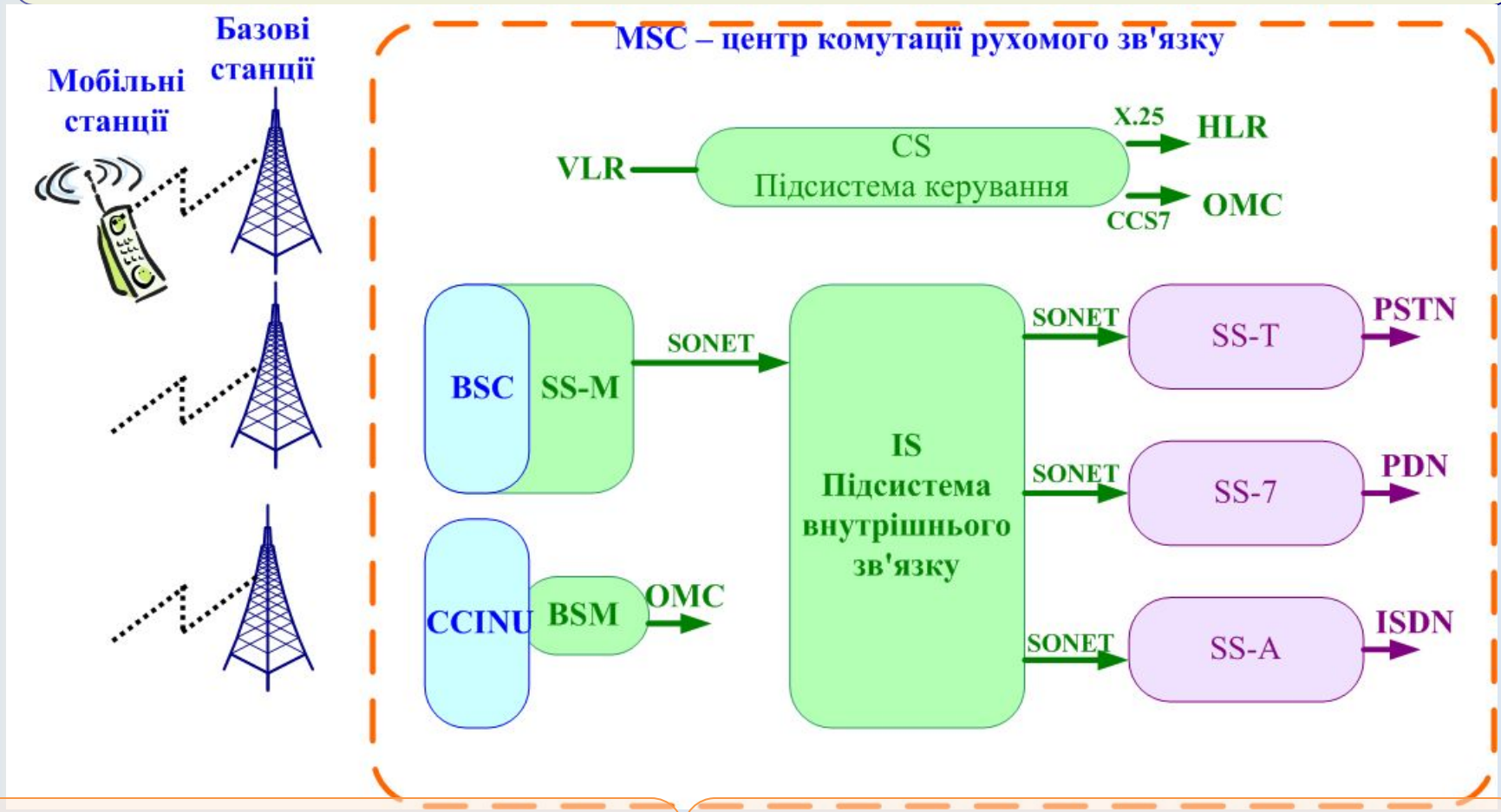
В такий спосіб CDMA забезпечує ефективніше використання наявного частотного спектру, забезпечуючи **значне збільшення пропускної здатності**.

Конфігурація мережі



PSTN – телефонна мережа загального використання
ISDN – цифрова мережа з інтеграцією служб
PDN – мережа з пакетною комутацією

Конфігурація мережі



SS-M – підсистема комутації мобільного зв'язку
SS-T – підсистема комутації з'єднувальних ліній
SS-7 – підсистема комутації SS№7
SS-A – підсистема комутації ARS

CCINU – центральний внутрішньомережевий пристрій
HLR – регістр розміщення
VLR – регістр переміщення
OMC – центр керування та обслуговування

Порівняння технологій CDMA та GSM

Перешкоди та завади

Унікальна для кожного окремого з'єднання схема кодування в CDMA практично повністю усуває перехресні перешкоди і значно знижує вплив перешкод від інших джерел

Зсув несучіх частот, між сусідніми стільниками

Відокремлення каналів за кодами, а не за частотами

Згасання сигналів біля кордонів стільників

Технології управління потужністю

Потужність сигналу - МС GSM - 125 мВт

МС CDMA - 2мВт

Технологія зв'язку CDMA

Передача мовлення та даних за стандартом IS-95 здійснюється

тривалість кадру **20 мс**.

швидкість передачі в межах сеансу зв'язку - **від 1,2 до 9,6 кбіт/с**

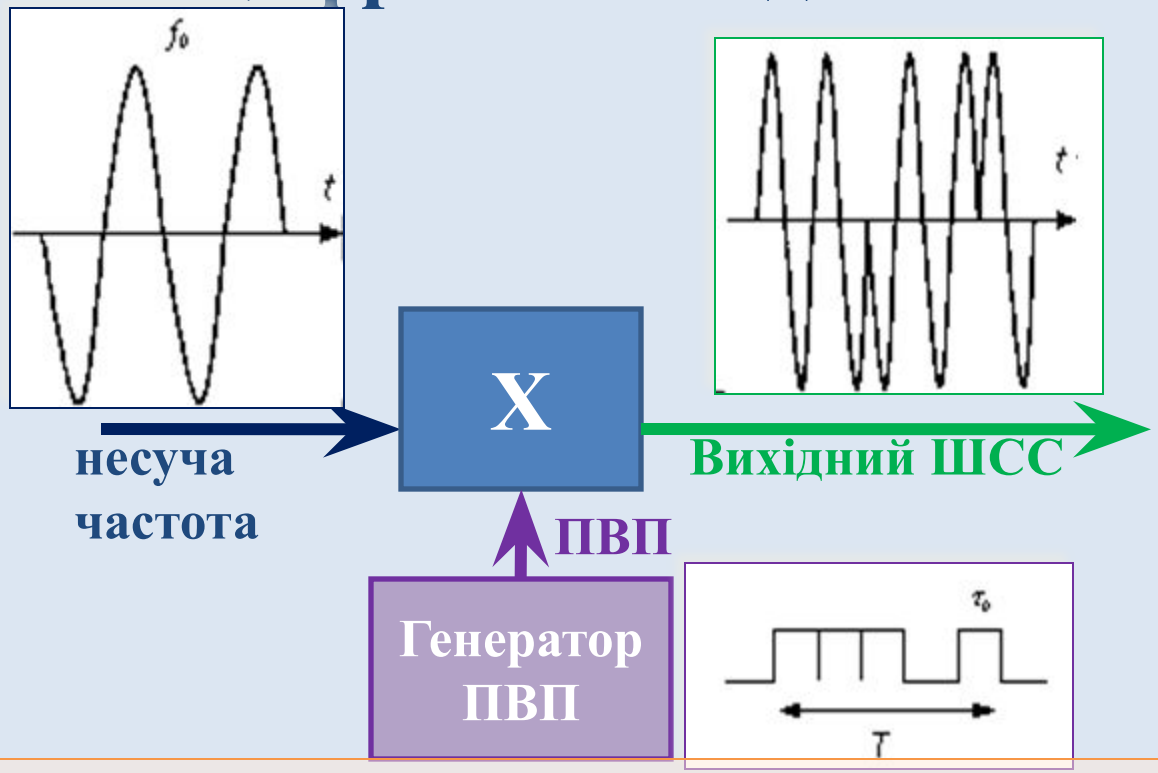
протягом передачі одного кадру залишається незмінною

Якщо кількість помилок в кадрі перевищує допустиму норму, то спотворений кадр видаляється.

Дані кодують, а код перетворюють на **шумоподібний широкосмуговий сигнал (ШШС)** так, що його можна виділити знову, тільки при наявності відповідного коду на приймальній стороні.

Одночасно в широкій смузі частот можна передавати і приймати **низку сигналів**, які не заважають один одному.

Схема розширення спектру частот цифрових повідомлень

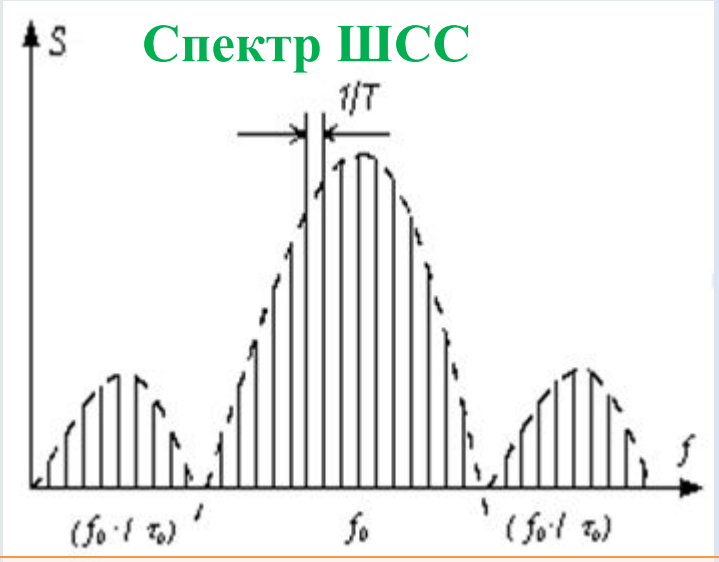


Вихідний модулюючий сигнал (аудіо) з смугою всього кілька кГц розподіляють в смузі частот, ширина якої декілька МГц

Подвійна модуляція несучої переданим інформаційним сигналом і широкосмуговим кодований сигналом

Основна характеристика ШСС - база B = F x T,
F - ширини спектра сигналу, T - його період

Схема розширення спектру частот цифрових повідомлень



У результаті перемножування сигналу джерела псевдовипадкового шуму з інформаційним сигналом енергія останнього розподіляється в широкій смузі частот, тобто його спектр розширюється

Співвідношення сигнал/шум на виході приймача - є функція співвідношення ширини смуг широкосмугового і базового сигналів, отже: **чим більше розширення спектру, тим більше виграш**

Для стандарту IS-95 **Співвідношення сигнал/шум = 21 дБ**

Це дозволяє системі працювати при рівні перешкод у 18 дБ, (при рівні сигнал/шум у 3 дБ на виході приймача).

Технологія зв'язку CDMA : Базові коди

Спільні для МС та БС, проте реалізують різні функції

Коди Уолша

Ортогональність
64 біти (IS95)
128 біт (CDMA-2000)

Коротка ПВП

16 біт - для ідентифікацій БС

Довга ПВП

42 біти - для ідентифікації МС

Технологія зв'язку CDMA : Базові коди

Тип сигналу	Довжина коду	Функції, що виконуються	
		БС	МС
Код Уолша	64	Кодове стиснення або розділення 64 каналів	Завадостійке кодування
Короткий код	32768	Розділення сигналів БС за величиною циклічного зсуву	Код з однаковим фіксованим зсувом – як опорний сигнал для скремблера
Довгий код	2^42 – 1 або 4,4 x 10^12	Проріжений довгий код – як опорна послідовність для скремблера	З різними циклічними зсувами – як адресна послідовність

Технологія зв'язку CDMA : Коди Уолша

Для кодового розділення каналів у **прямому каналі (від БС до МС)** використовуються ортогональні коди Уолша

Коди Уолша формуються із рядків матриці Уолша

кожен рядок матриці Уолша ортогональний будь-якому іншому рядку, отриманого за допомогою операції логічного заперечення

$$W_L = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

У стандарті IS-95 - матриця **64**-го порядку

У CDMA-2000 - **128**-го порядку

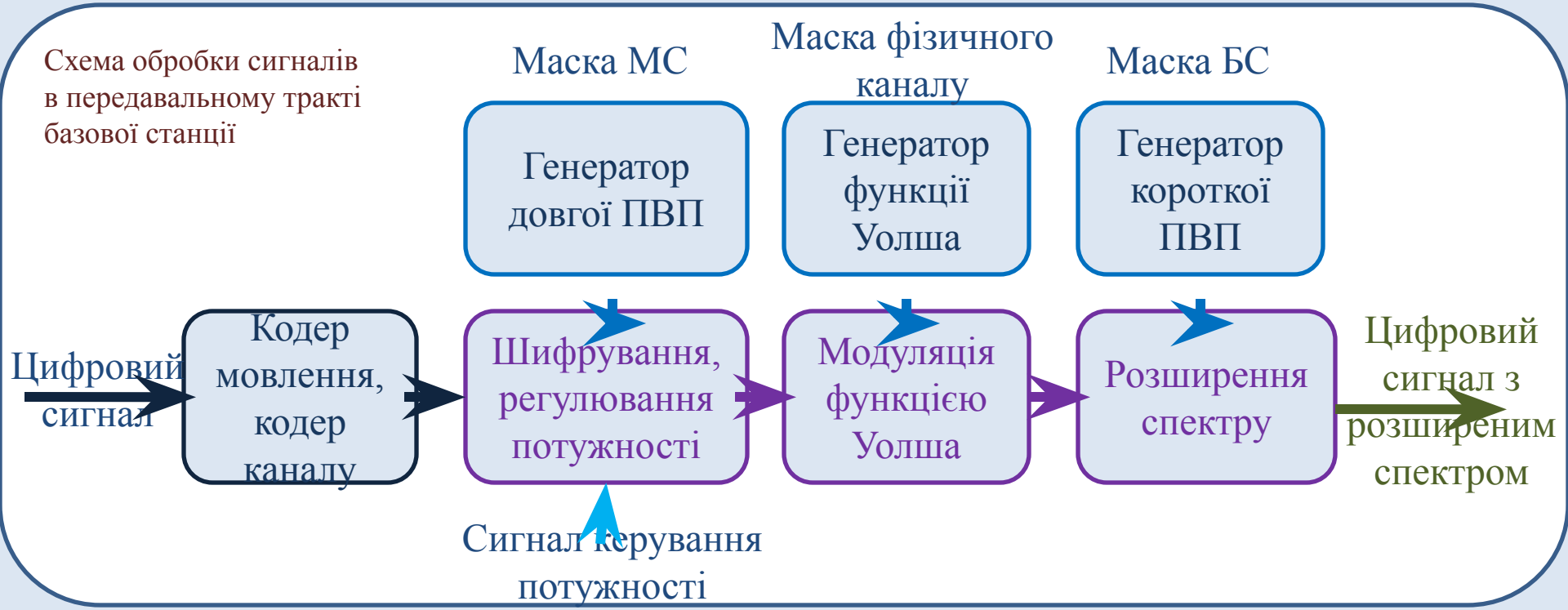
Для виділення сигналу на виході приймача застосовується цифровий фільтр

При ортогональних сигналах фільтр можна налаштувати таким чином, що на його виході завжди буде логічний «0», за винятком випадків, коли приймається той сигнал, на який він налаштований

Узгоджені фільтри приймачів БС дуже чутливі до ефекту «далеко-близько».
Для максимізації абонентської ємності системи необхідно, щоб МС всіх абонентів випромінювали сигнал такої потужності, яка забезпечила б однаковий рівень прийнятих сигналів БС.
Чим точніше керування потужністю, тим більше абонентська ємність системи

Всі БС використовують одну і ту ж пару коротких ПСП, але зі зсувом на 64 дискрет між різними БС (всього в мережі 511 кодів); при цьому всі фізичні канали однієї БС мають одну і ту ж фазу послідовності

Технологія зв'язку CDMA : Прямий канал (від БС до МС)



модуляція сигналу функціями Уолша (бінарна фазова маніпуляція) - для розділення різних фізичних каналів даної БС

модуляція довгою ПВП (бінарна фазова маніпуляція) - шифрування повідомлень

модуляція короткою ПВП (квадратурна фазова маніпуляція двома ПВП однакового періоду) - для розширення смуги і розділення сигналів різних БС

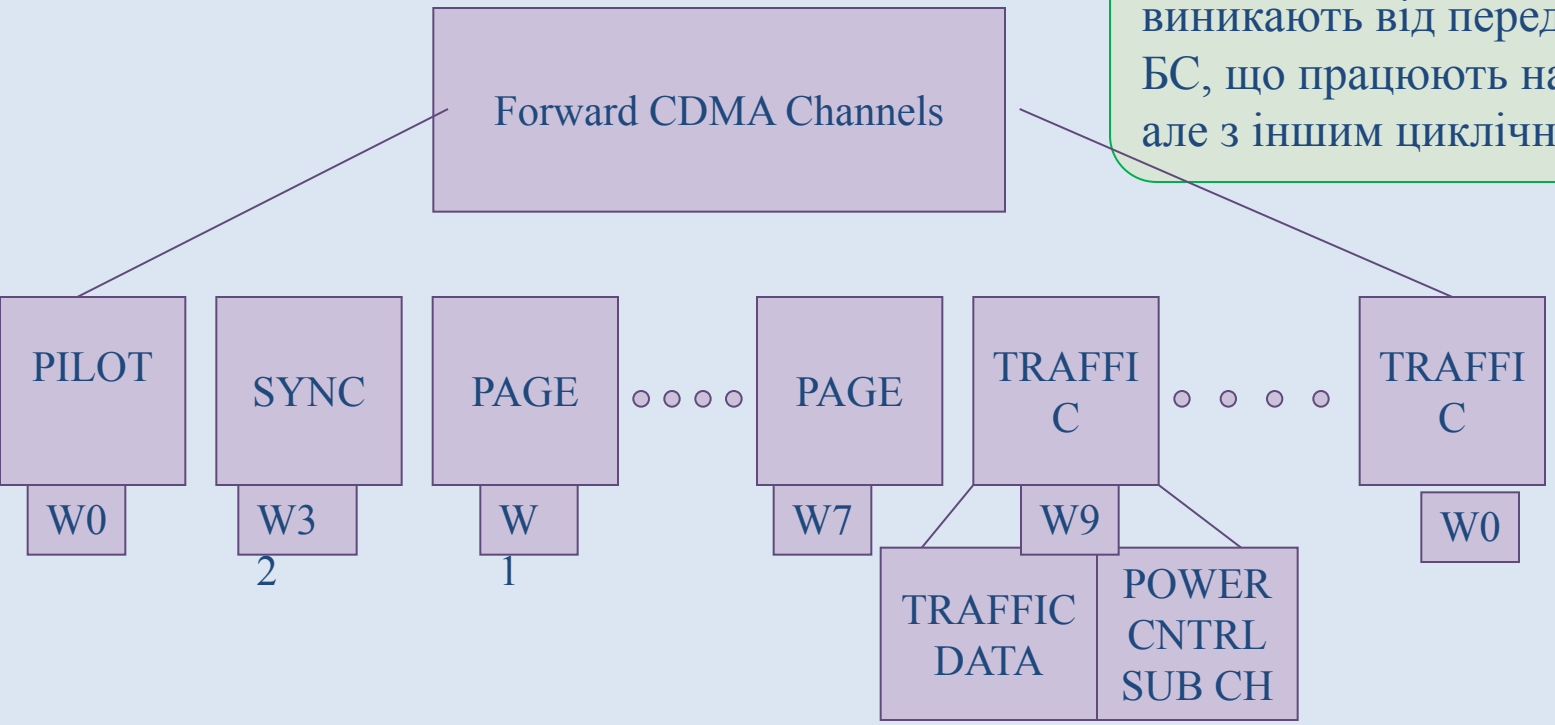
Технологія зв'язку CDMA : Прямий канал (від БС до МС)

На БС формується 4 типи каналів:

- канал пілот-сигналу (PI),
- сінхроканал (SYNC),
- канал виклику (PCH) і
- канал трафіку (TCH).

Сигнали різних каналів взаємно ортогональні, що гарантує відсутність взаємних перешкод між ними на одній БС

Внутрішньосистемні перешкоди виникають від передавачів інших БС, що працюють на тій же частоті, але з іншим циклічним зсувом



Технологія зв'язку CDMA : Прямий канал (від БС до МС)

Пілот-сигнал - це сигнал несучої, який використовується БС для вибору робочої зони (за найбільш потужним сигналом), а також як опорний для синхронного детектування сигналів інформаційних каналів

Випромінювання пілот-сигналу відбувається безперервно

Для передачі використовують функцію Уолша нульового порядку (W0)

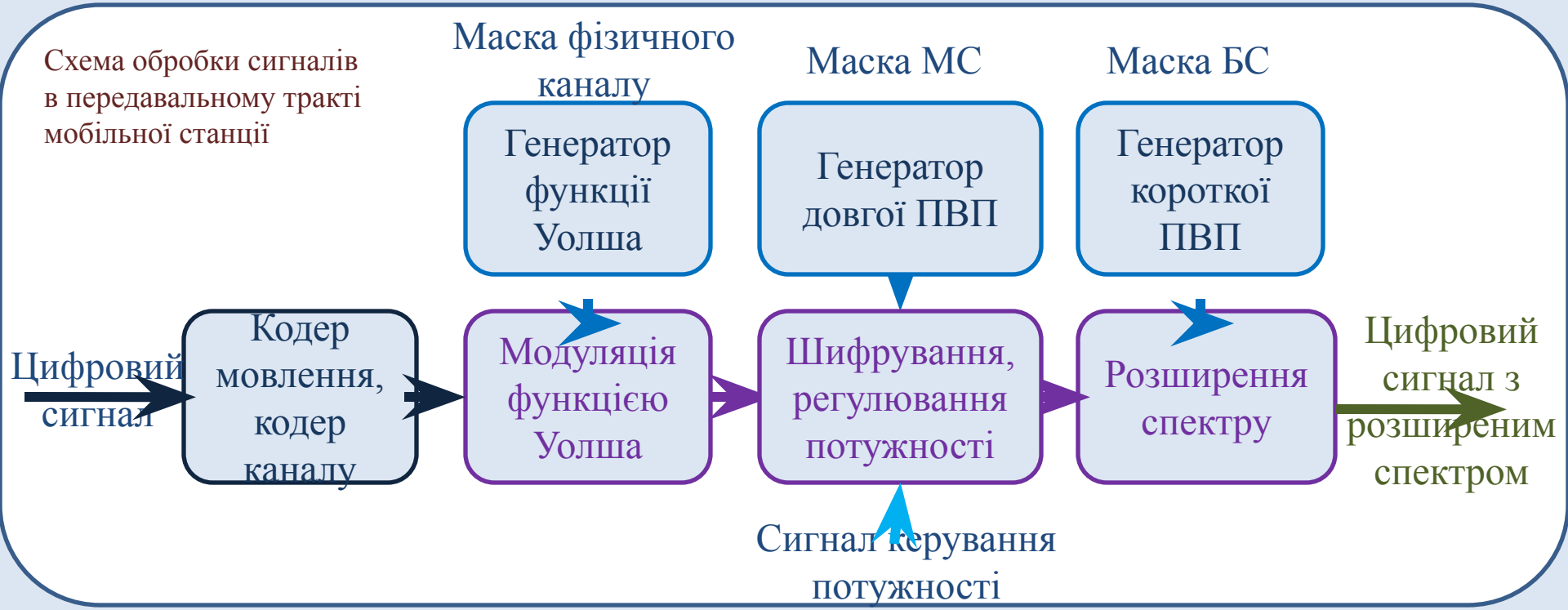
Зазвичай на пілот-сигналі випромінюється близько 20% загальної потужності, що дозволяє МС забезпечити точність виділення несучої частоти і здійснити когерентний прийом сигналів

Технологія зв'язку CDMA : Прямий канал (від БС до МС)

Характеристики каналів

Параметр	БС			МС		
Тип каналу	PI	SYNC	PCH	TCH	ACH	PCH
Кількість каналів, що передаються одночасно	1	1	7	55	1	1
Вхідна швидкість, кбіт/с	Н/п	1,2	2,4	1,2	4,8	1,2
			4,8	2,4		2,4
			9,6	4,8	4,8	
				9,6		9,6
Вихідна швидкість кодованого потоку, кбіт/с	Н/п	4,8	19,2	19,2	28,8	28,8

Технологія зв'язку CDMA : Зворотній канал (від МС до БС)



Модуляція сигналу короткої ПВП використовується тільки для розширення спектру, причому всі МС використовують одну і ту ж пару послідовностей з однаковим (нульовим) зсувом.

Модуляція сигналу довгою ПВП крім шифрування повідомлень несе інформацію про МС у вигляді її закодованого індивідуального номера та забезпечує розрізнення сигналів від різних МС однієї зони за рахунок індивідуального для кожної МС зсуву послідовності

Технологія зв'язку CDMA : Зворотній канал (від МС до БС)

На МС формується 2 типи каналів:

- канал доступу (АСН) і
- канал трафіку (ТСН).

Пілот-сигналу в зворотному каналі немає, а завадостійкість забезпечується за рахунок просторового рознесення

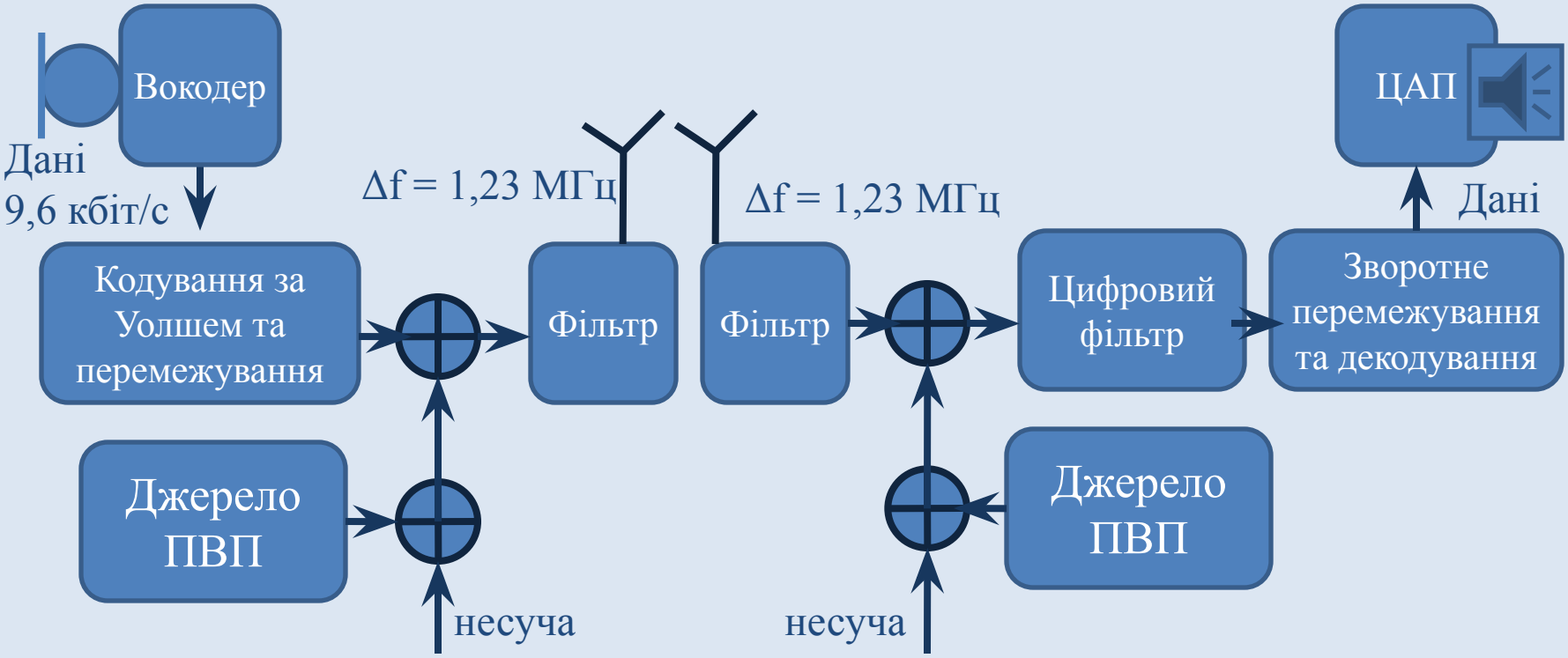
У МС теж застосовуються ортогональні коди Уолша, але не для ущільнення каналів (як на БС), а для підвищення завадостійкості

Вхідний потік даних зі швидкістю **28,8 кбіт/с** розбивається на пакети по 6 біт, і кожному з них однозначно ставиться у відповідність одна з 64 послідовностей Уолша

У результаті швидкість кодованого потоку на вході модулятора зростає до **307,2 кбіт/с**

Це кодування однаково для всіх фізичних каналів, а на приймальному кінці використовуються 64 паралельних каналів, кожен з яких налаштований на свою функцію Уолша, і ці канали розпізнають (декодують) прийняті 6-бітові символи

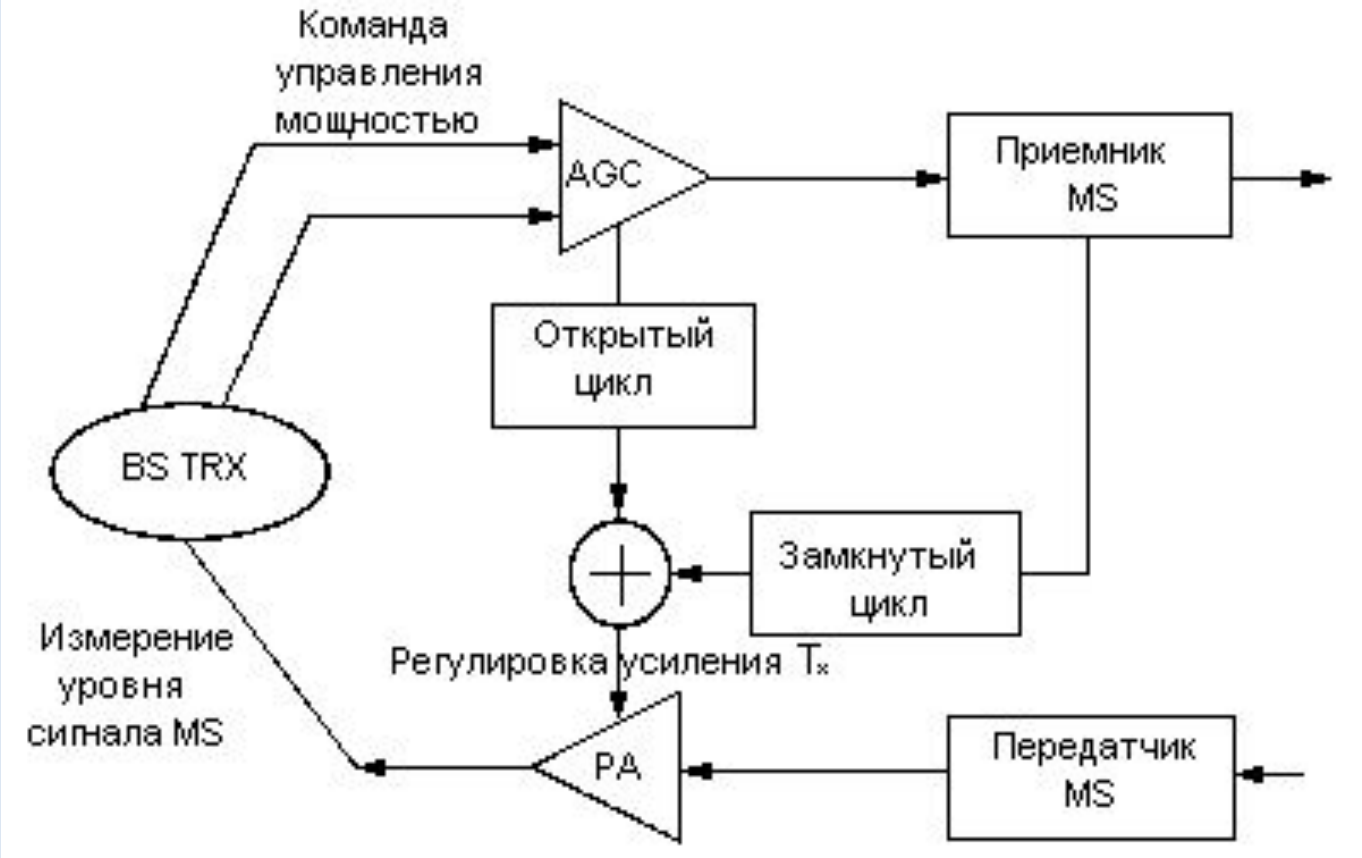
Технологія зв'язку CDMA : Загальна схема



Технологія зв'язку CDMA : Зворотній канал (від МС до БС)

1. Інформаційний сигнал кодується за Уолшем,
2. Змішується з несучою, спектр якої попередньо розширюється перемножуванням з сигналом джерела псевдовипадкового шуму. Кожному інформаційному сигналі призначається свій код Уолша, потім вони об'єднуються в передавачі, пропускаються через фільтр, і загальний шумоподібний сигнал випромінюється передавальною антеною.
3. На вхід приймача надходять корисний сигнал, фоновий шум, перешкоди від БС сусідніх зон та від МС інших абонентів.
4. Після ВЧ-фільтрації сигнал надходить на коррелятор, де відбувається стиснення спектру і виділення корисного сигналу в цифровому фільтрі за допомогою заданого коду Уолша. Спектр перешкод розширюється, і вони з'являються на виході корелятора у вигляді шуму.

Технологія зв'язку CDMA :
Схема керування потужності в прямому каналі



Основні технічні характеристики

Характеристика	Значение
Диапазон частот передачи MS, МГц	824,040-848,860
Диапазон частот передачи BTS, МГц	869,040-893,970
Относительная нестабильность несущей частоты BTS	$\pm 5 \times 10^{-8}$
Относительная нестабильность несущей частоты MS	$\pm 2{,}5 \times 10^{-6}$
Вид модуляции несущей частоты	QPSK (BTS), O-QPSK (MS)
Ширина спектра излучаемого сигнала, МГц:	
по уровню -3 дБ	1.25
по уровню -40 дБ	1.50
Тактовая частота ПСП, МГц	1.2288
Число каналов BTS на одной несущей	1 пилот-канал, 1 канал сигнализации, 7 каналов персонального вызова, 55 каналов связи
Число каналов MS	1 канал доступа, 1 канал связи
Скорость передачи данных, бит/с:	
в канале синхронизации	1200
в канале персонального вызова и доступа	9600, 4800
в каналах связи	9600, 4800, 2400, 1200

Механізми безпеки в CDMA2000

Electronic Serial Number (ESN)

CAVE

- Спеціалізована геш-функція з 64-бітним ключем (A-key)
- Протокол автентифікації типу “запит/відповідь”
- Генератор ключів

XOR

з 520-бітною маскою забезпечує конфіденційність мовного сигналу

Authentication Key (A-key)

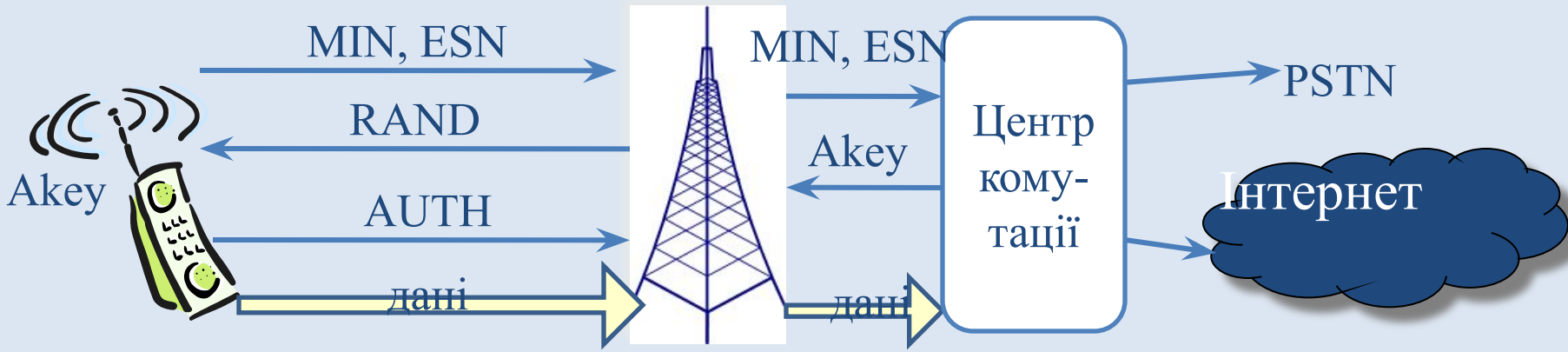
ORYX

Потоковий шифр оснований на LFSR (регістр зсуву з лінійним зворотнім зв'язком) для конфіденційності даних

CMEA

Двухраундовий блоковий шифр змінної довжини для сигнального трафіку

Механізми безпеки в CDMA2000



(AUTH, k) = CAVE(*Akey*, RAND)

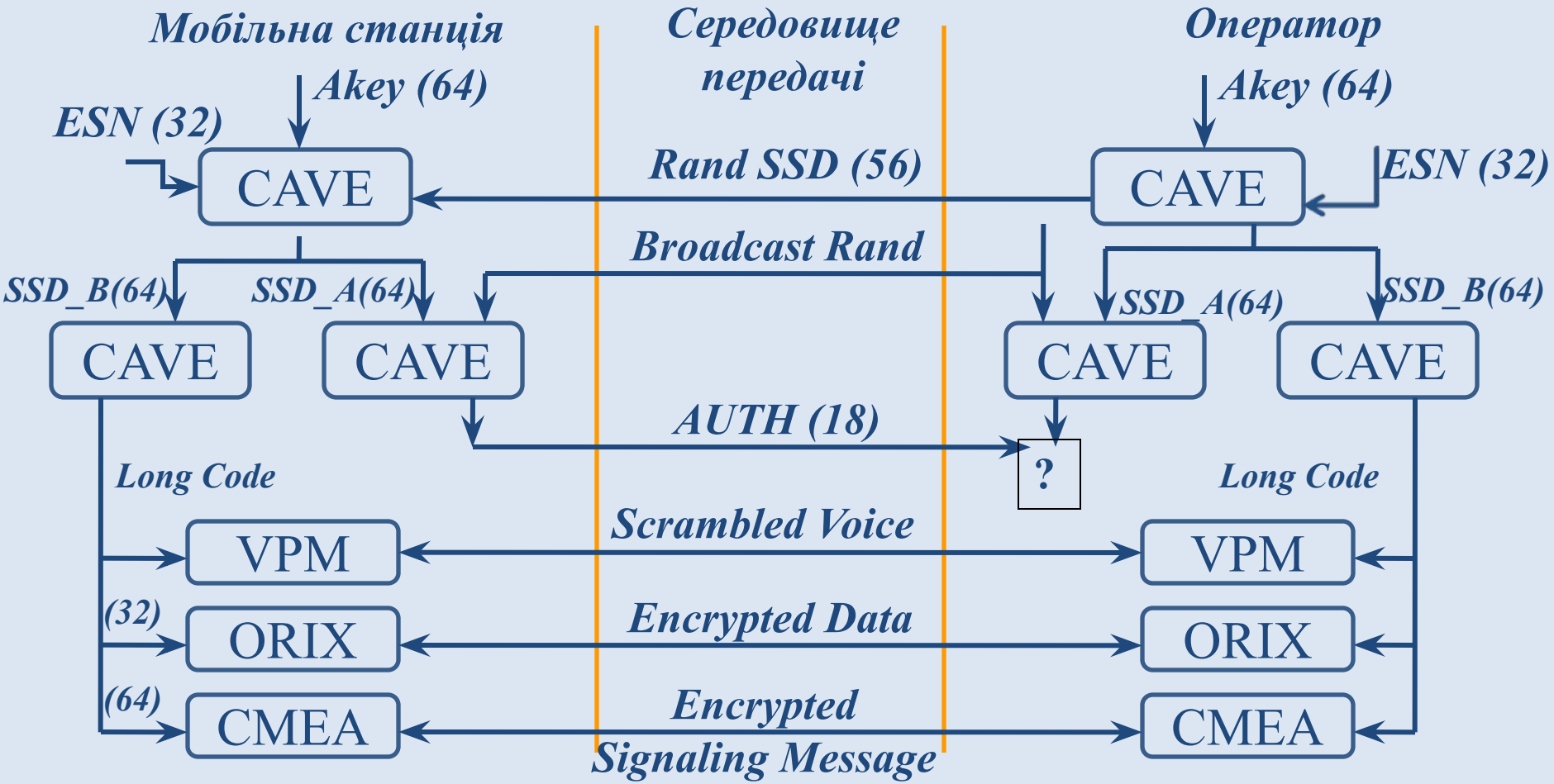
Механізми безпеки в CDMA2000

Криптографічні протоколи базуються на 64-бітному автентифікаційному ключі (A-key) та Electronic Serial Number (ESN).

Для автентифікації абоненту при реєстрації МС в мережі, а також генерації додаткових ключів для забезпечення конфіденційності передачі мовлення та кодування повідомлень використовується випадкове число RANDSSD, яке генерується автентифікаційним центром реєстру власних абонентів (HLR/AC – Home Location Register /Authentification Center).

A-key запрограмований в МС, а також зберігається в HLR/AC мережі.

Механізми безпеки в CDMA2000



Механізми безпеки в CDMA2000

CDMA використовує стандартизований алгоритм CAVE (Cellular Authentification and Voice Encryption) для генерації 128-бітного підключа SSD (Shared Secret Data).

A-key, ESN та випадкове число RANDSSD подаються на вхід CAVE, який генерує SSD.

A-Key Постійна 64-бітна секретна послідовність
Використовується для генерації SSD
Зберігається у MC
Зазвичай прописується у MC при покупці
Відома тільки MC та HLR/AC

SSD складається з двох частин:

- SSD_A (64 біти) - для автентифікаційного цифрового підпису
- SSD_B (64 біти) - генерації ключів для шифрування мовлення та службових повідомлень.

SSD може бути переданий гостьовій мережі для забезпечення локальної автентифікації.
Новий SSD генерується при поверненні абоненту в домашню мережу

Безпека передачі мовлення, даних та службових повідомлень

CAVE Component	A-key Verification	SSD Generation
LFSR	32 MSBs of A-key	32 LSBs of RANDSSD
$sreg[0, 1, \ldots, 7]$	A-key	A-key
$sreg[8]$	Algorithm version	Algorithm version
$sreg[9, 10, 11]$	24 LSBs of A-key	24 MSBs of RANDSSD
$sreg[12, \ldots, 15]$	ESN	ESN
offset_1	128	128
offset_2	128	128

Автентифікація в CDMA2000

Для автентифікації абонента використовується допоміжний ключ SSD_A, який генерується алгоритмом CAVE з A-key, ESN та RANDSSD.

Мережа генерує і розсилає відкрито по ефіру випадкове число RAND *, MC, що реєструються в мережі, використовують його як вхідні дані для CAVE, який генерує 18-бітний автентифікаційний цифровий підпис (AUTH_SIGNATURE), і посилає його на БС.

Цифровий підпис звіряється MSC (мобільний центр комутації послуг) з підписом, який генерується самим MSC для перевірки легітимності абонента.

Число RAND * може бути як одним і тим же для всіх користувачів, так і генеруватися кожен раз нове. Використання конкретного методу визначається оператором.

Перший випадок забезпечує дуже швидку автентифікацію.

Автентифікація в CDMA2000

І МС, і БС ведуть 6-бітні лічильники викликів, що забезпечує можливість детектування роботи двійників: для цього достатньо лише контролювати відповідність значень лічильників на телефоні і в MSC.

Секретний ключ A-key є перепрограмованим, в разі його зміни інформація на МС і в HLR/AC повинна бути синхронізована.

Ключ A-key може бути перепрошитий декількома способами:

- на заводі,
- дилером в точці продажів,
- абонентом через інтерфейс телефону,
- OTASP (over the air service provisionig). OTASP-передачі використовують 512-бітний алгоритм узгодження ключів Діффі-Хелмана, гарантує достатню безпеку.

OTASP забезпечує легкий спосіб зміни A-keyMC на випадок появи в мережі двійника. Зміна A-key автоматично спричинить за собою відключення послуг двійникові МС і повторне включення послуг легітимному абоненту. Секретність ключа A-key є найважливішою компонентою безпеки CDMA системи.

Геш-функція CAVE

Алгорим геш-функції CAVE має багато варіацій.

Основними елементами є
- шістнадцять 8-бітних регістрів даних
- два 8-бітних зсуви (offset_1 and offset_2)
- 32-бітний регістр зсуву з лінійним зворотнім зв'язком

Має 4 або 8 раундів, на кожному з яких відбувається 16 фаз оновлення регістрів

32-бітний регістр зсуву з лінійним зворотнім зв'язком складається з чотирьох незалежних байтових регістрів LFSRA, LFSRB, LFSRC та LFSRD.

Зворотна функція виглядає так

$$Lt+32 = Lt \oplus Lt+1 \oplus Lt+2 \oplus Lt+22$$

Для зміни регістра на кожній фазі використовуються байти з РЗЛЗЗ, зсувів та двох (8*4) довідникових таблиць або S-боксів (кожен по 256 значень).

Зсуви offset_1 та offset_2 використовуються як покажчики для таблиць CT_low[·] та CT_high[·]. Наприклад

$$offset\_1 = offset\_1\_prev + (LFSRA \oplus sreg[i]) \bmod 256$$

$$Temp\_low = CT\_low[offset\_1]$$

Геш-функція CAVE

Байт offset_1_prev - це попереднє значення байту offset, яке ініціалізовано як стала. CAVE циклічно змінює LFSR лінійно вправо поки вузли рівні відповідним low/high order бітам sreg[i], де i – номер фази в етапі.

Коли вони стають нерівними, CAVE обчислює тимчасовий байт як конкатенацію тимчасових вузлів low/high та переходом до наступної фази етапу.

Якщо порівнювальні значення стають рівними, проходить додатковий цикл над LFSR та описані вище обчислення повторюється з останнім байтом LFSR та значеннями offset.

Дуже рідко кількість циклів досягають 32, тоді байти LFSRD беруться по модулю 256.

Після завершення фази LFSR cycles once resulting in як мінімум в 16 зсувах LFSR на кожному етапі CAVE.

Між етапами біту у регістрі зсуваються з використанням таблиці low для визначення byte permutation якій іде за однобітною rotation на 128-bit блоці регістра як на цілому.

Безпека передачі мовлення, даних та службових повідомлень

МС використовує підключ SSD_B і алгоритм CAVE для генерації
- Private Long Code Mask (успадковану від TDMA-мереж),
- 64-бітного підключа CMEA (Cellular Message Encryption Algorithm) і
- 32-бітного DATA-ключ.

Private Long Code Mask використовується як МС та і БС для зміни характеристик Long Code

Long Code Mask - модифікований Long Code використовується для мовлення, що підвищує секретність їх передачі.

Private Long Code Mask не шифрує інформацію, просто замінює відомі величини, використовувані в кодуванні CDMA-сигналу, секретними величинами. Таким чином підслуховування розмов без знання Private Long Code Mask є надзвичайно складним завданням.

МС та БС використовують CMEA і поліпшений ECMEA (Enchanced_CMEA) алгоритми для шифрування службових повідомлень при передачі їх по ефіру.

Окремий DATA-ключ і алгоритм шифрування ORYX використовується МС та БС для шифрування потоку інформації по каналу зв'язку CDMA

Безпека передачі даних: Потоковий шифр ORYX

ORYX – це простий потоковий шифр, який оснований на регістрах зсуву з лінійним зворотнім зв'язком (РЗЛЗЗ). Використовується для забезпечення конфіденційності даних, що передаються у мережі CDMA.
Шифр ORYX має чотири основних компоненти: три 32-бітних РЗЛЗЗ, які позначаються як LFSRA, LFSRB та LFSRK, а також S-box, що містить відому перестановку P цілих значень від 0 до 255

LFSRA має таку зворотну функцію
$Lt+32=Lt+26 \oplus Lt+23 \oplus Lt+22 \oplus Lt+16 \oplus Lt+12 \oplus Lt+11 \oplus Lt+10 \oplus Lt+8 \oplus Lt+7 \oplus Lt+5 \oplus Lt+4 \oplus Lt+2 \oplus Lt+1 \oplus Lt$
Або
$Lt+32=Lt+27 \oplus Lt+26 \oplus Lt+25 \oplus Lt+24 \oplus Lt+23 \oplus Lt+22 \oplus Lt+17 \oplus Lt+13 \oplus Lt+11 \oplus Lt+10 \oplus Lt+9 \oplus Lt+8 \oplus Lt+7 \oplus Lt+2 \oplus Lt+1 \oplus Lt$

LFSRB має таку зворотну функцію
$Lt+32=Lt+31 \oplus Lt+21 \oplus Lt+20 \oplus Lt+16 \oplus Lt+15 \oplus Lt+6 \oplus Lt+3 \oplus Lt+1 \oplus Lt$

LFSRK має таку зворотну функцію $Lt+32=$
$Lt+28 \oplus Lt+19 \oplus Lt+18 \oplus Lt+16 \oplus Lt+14 \oplus Lt+11 \oplus Lt+10 \oplus Lt+9 \oplus Lt+6 \oplus Lt+5 \oplus Lt+1 \oplus Lt$

Безпека передачі даних: Потоковий шифр ORYX

Перестановка L незмінна на час виклику і формується з відомого алгоритму, вона ініціалізується зі значенням, яке передається в незашифрованому вигляді під час встановлення виклику. Кожен байт ключової послідовності генерується в такий спосіб:

1. LFSR_K виконує один крок.
2. LFSR_A виконує один крок, з одним з двох різних поліномів зворотної функцій залежно від стану LFSR_K.
3. LFSR_B виконує один або два кроки залежно від вмісту іншого стану LFSR_K.
4. Старші байти поточного стану LFSR_K, LFSR_A та LFSR_B комбінуються у ключову послідовність використовуючи комбінаційну функцію:

$$Keystream = \{High8\_K + L[High8\_A] + L[High8\_B]\} \bmod 256$$

Оскільки ORYX використовує 96-бітну ключову послідовність, то підібрати її та перевірити на коректність достатньо складно, проте при використанні методу “розділяй та владарюй” можна значно зменшити складність підбору при атаці з відомим шифротекстом.

Безпека передачі службових повідомлень : Блоковий шифр CMEA

Симетричний блоковий шифр, який призначений для шифрування каналу управління.

Це байт-орієнтований, із змінним розміром блоку (як правило, від 2 до 6 байт).
Розмір ключа становить всього 64 біта.
Алгоритм складається всього з 3 проходів за даними:

- нелінійна зліва направо операція дифузії
- безключове лінійне переміщування
- та нелінійна операція дифузії, яка по суті є оберненою до першої.

Для нелінійних операцій використовується ключова довідникова (lookup) таблиця під назвою *T-Box,* яка використовує безключову довідникову (lookup) таблицю під назвою *Cave Table*.

Шифр CMEA є дуже небезпечним. Існуюча атака з відомим текстом потребує лише 338 зразків, а при 3-х байтовому блоці (найчастіше використовується) достатньо 80 відомих текстів.

Безпека передачі мовлення

Voice Privacy Mask

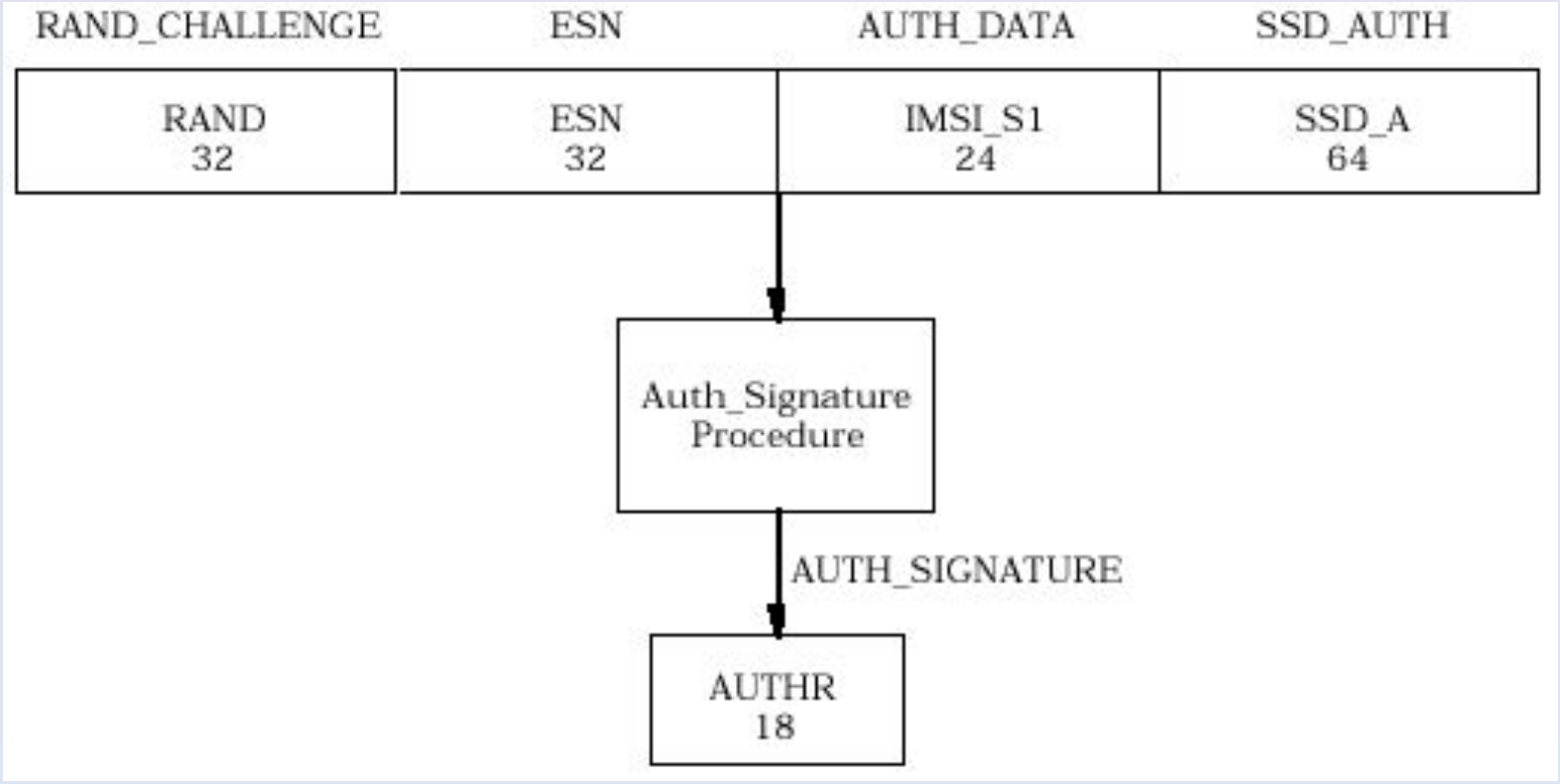
Безпека передачі мовленевого сигналу може бути реалізована на основі скремблювання за допомогою

-Довгого коду успадкованого з TDMA (занадто слабкий і підбирається на основі одного відомого тексту).

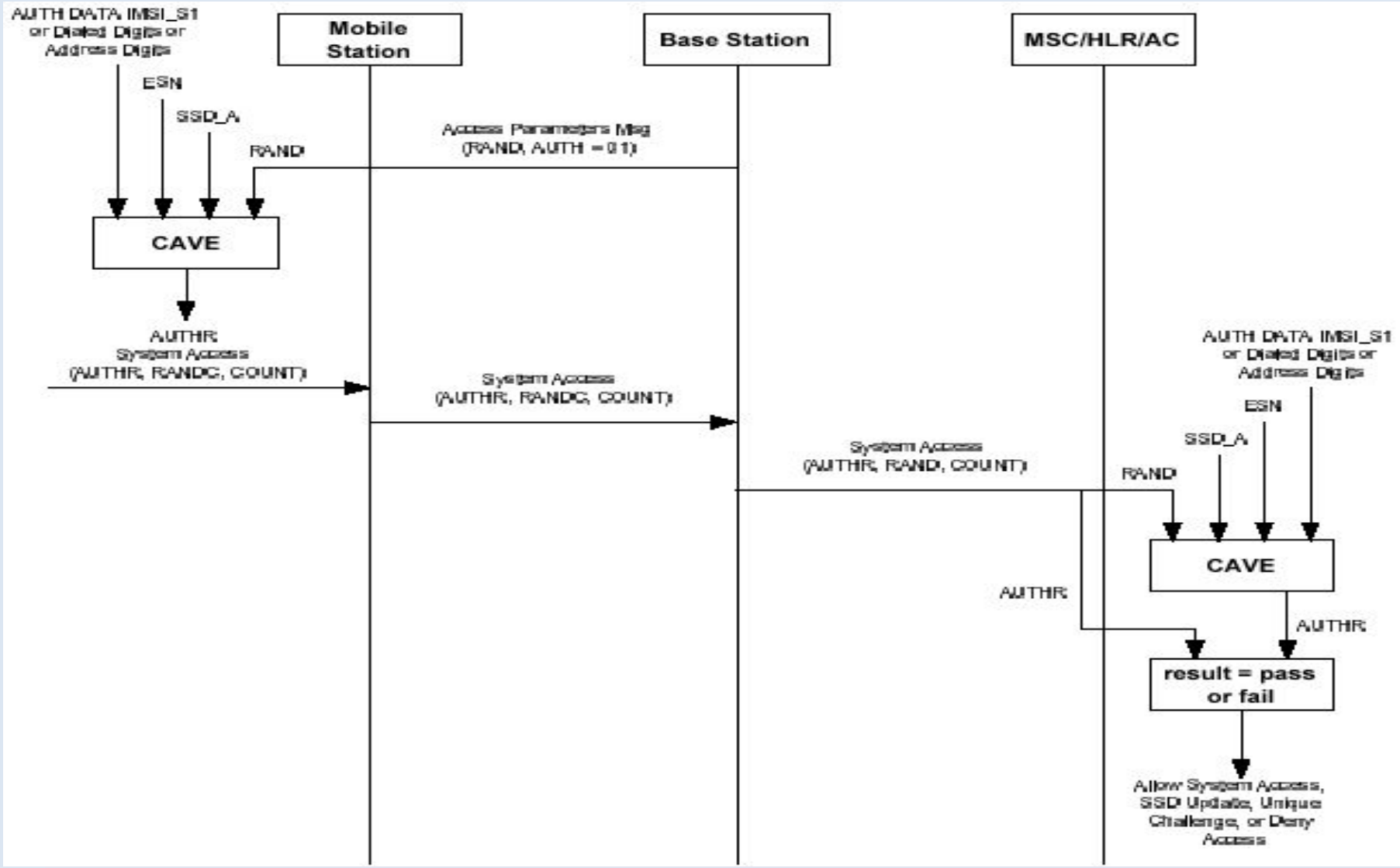
- ключових спектральних методів з маскою, що генерується регістром зсуву з лінійним зворотнім зв'язком.

AUTHR calculation

For Registration:



AUTHR calculation (Cont.)



Authentication Procedures

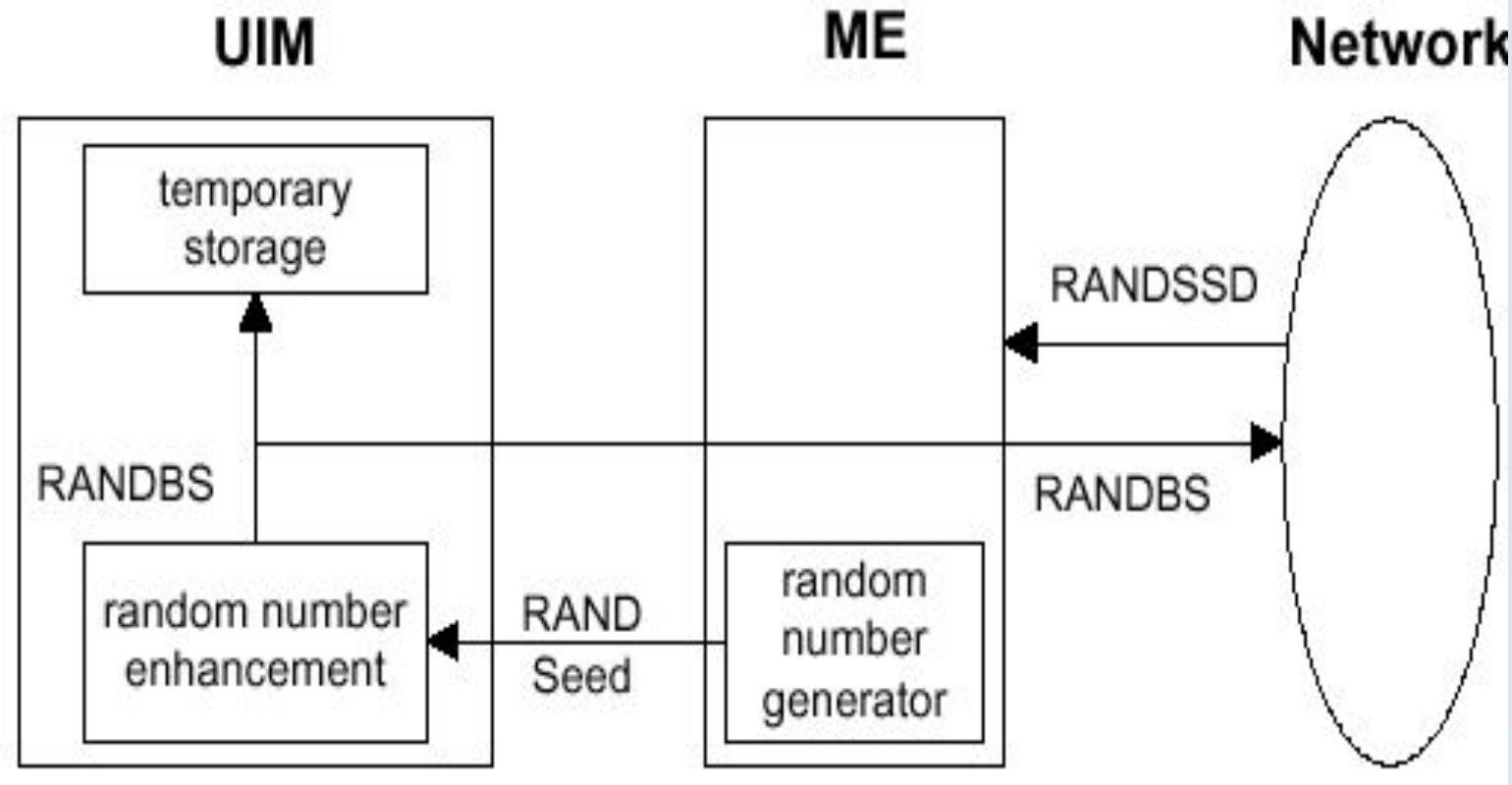
Managing Shared Secret Data

Authentication Calculations

Managing the Call History Parameter

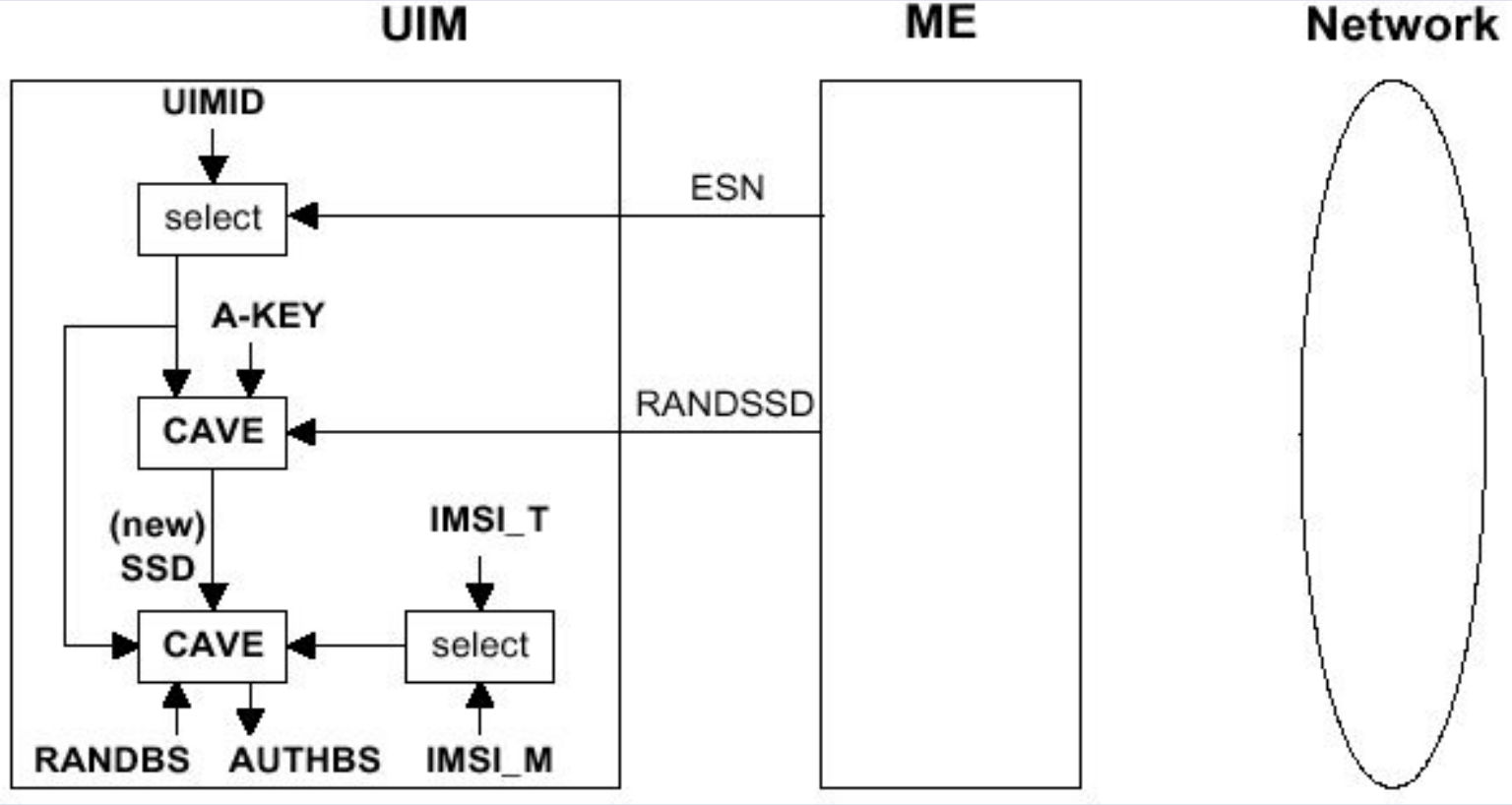
Managing Shared Secret Data

Base Station Challenge Function:



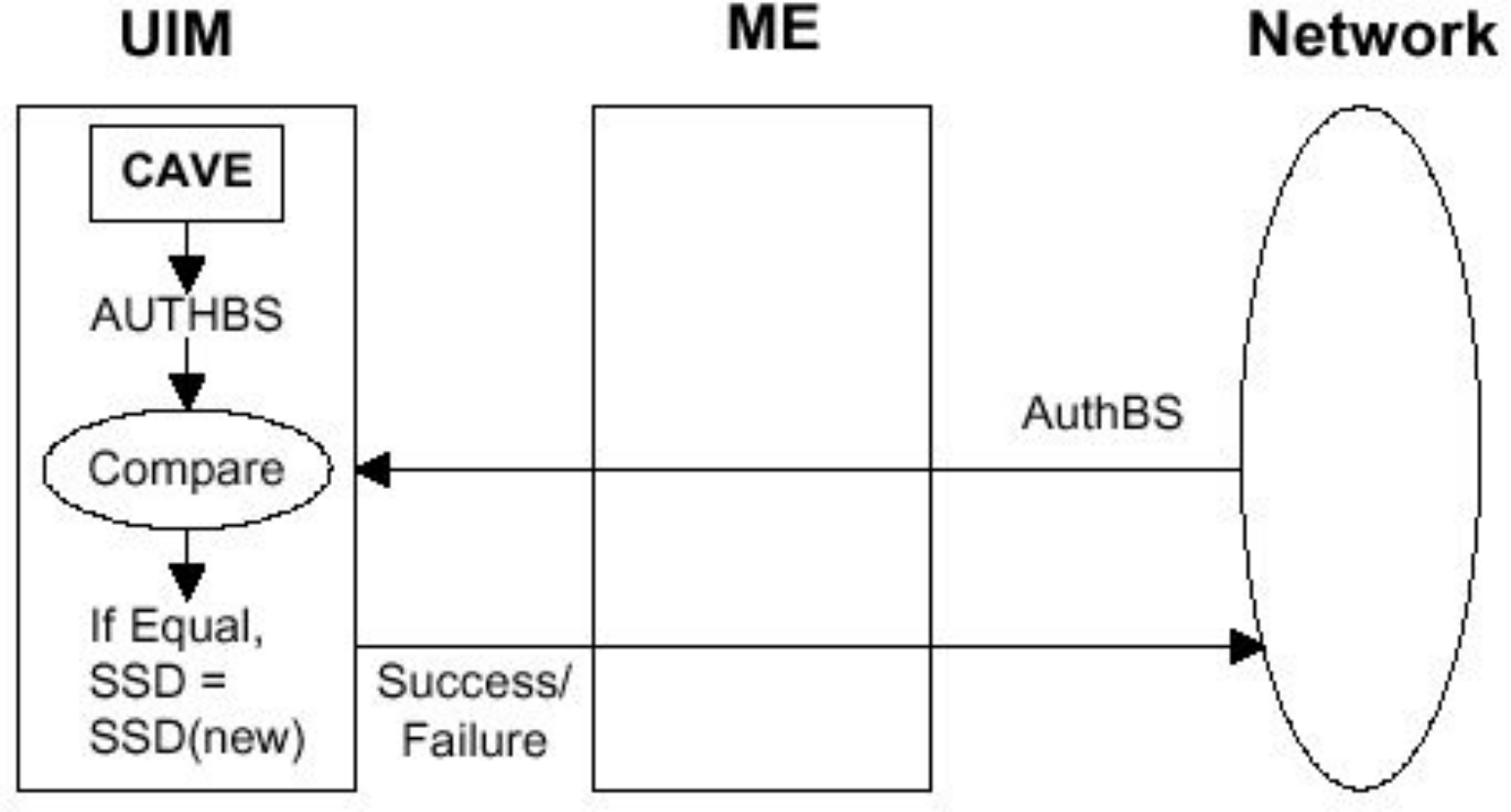
Managing Shared Secret Data(Cont.)

Update SSD, AUTHBS Calculation:



Managing Shared Secret Data(Cont.)

Confirm SSD



Криптоаналіз

- Захист мовлення забезпечується 520-бітною маскою XOR
  - Може бути зламаний в режимі реального часу через атаку з відомим шифротекстом (часто перший фрейм – це “тиша” (всі нулі)
- Контрольний канал використовує CMEA, блоковий шифр з блоками змінної довжини з двома раундами
  - Може бути зламаний з 80 відомими текстами
- Для захисту даних, що передаються, запропоновано шифр ORYX, який базується на потоковому LFSR
  - Може бути зламаний в режимі реального часу через атаку з відомим шифротекстом
- CAVE – спеціалізована геш-функція з 64-бітним ключем
  - Найкраща атака вимагає 2^{21} обраних текстів

Безпека A-key

Перепрограмований

- Завод
- Продавець в точці продажу
- Абонент по телефону
- Через бездротове надання послуг - Over the air service provisioning (OTASP)

  Обмін ключами за 512-бітний Діффі-Хелман

Безпека CDMA

- Загальні питання
  - Всі мобільні визначаються за тим самим випадковим числом
  - Дозволяється швидка автентифікація
- Особливості
  - Унікальне RAND використовується для кожного запитаної MC
- Лічильник викликів (6-біт)
  - Ведеться як MC так і БС
  - Забезпечує захист від клонування, оскільки у провайдера видається сигнал при неспівпадінні
- Анонімність
  - Temporary Mobile Station Identifier (TMSI)
- CDMA 2000 порівняно стійкий
- Проблема у неефективному впровадженні.
  - A-key залишається слабким
  - Не впроваджений лічильник хронології викликів