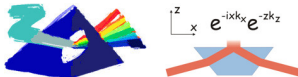


## Fizyczne podstawy działania telefonii komórkowej

Tomasz Kawalec

12 maja 2010

Zakład Optyki Atomowej, Instytut Fizyki UJ



[www.coldatoms.com](http://www.coldatoms.com)

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych

### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych

### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia

- Fale elektromagnetyczne, anteny
    - Z których pasm korzysta telefonia komórkowa
    - Jak przesyłać głos za pomocą fal elektromagnetycznych

### Trzy generacje telefonii komórkowej

- NMT
  - GSM oraz co jest w telefonie w środku
  - UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
  - Czy telefonia komórkowa może szkodzić?



- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?



- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?



- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?



- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?

- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?



- Podstawy

- Historia
- Fale elektromagnetyczne, anteny
- Z których pasm korzysta telefonia komórkowa
- Jak przesyłać głos za pomocą fal elektromagnetycznych



### Trzy generacje telefonii komórkowej

- NMT
- GSM oraz co jest w telefonie w środku
- UMTS

### Zdrowie psychiczne i fizyczne

- Czy można nas podsłuchać?
- Czy telefonia komórkowa może szkodzić?



Wykorzystanie fal radiowych:

radio, telewizja (w tym — satelitarna), łączność profesjonalna, telefony komórkowe, Wi-Fi, Bluetooth, GPS, pagery, telefony bezprzewodowe, zdalne sterowanie, piloty do bram itp., bezprzewodowe akcesoria do komputerów

Wykorzystanie fal radiowych:

radio, telewizja (w tym — satelitarna), łączność profesjonalna, telefony komórkowe, Wi-Fi, Bluetooth, GPS, pagery, telefony bezprzewodowe, zdalne sterowanie, piloty do bram itp., bezprzewodowe akcesoria do komputerów

Wpływ telefonii komórkowej na zachowanie ludzi:



Wykorzystanie fal radiowych:

radio, telewizja (w tym — satelitarna), łączność profesjonalna, telefony komórkowe, Wi-Fi, Bluetooth, GPS, pagersy, telefony bezprzewodowe, zdalne sterowanie, piloty do bram itp., bezprzewodowe akcesoria do komputerów

Wpływ telefonii komórkowej na zachowanie ludzi:

- badania w dziedzinie psychologii społecznej, rozwojowej, poznawczej, psychopatologii, psychologii osobowości
- badanie emocji, komunikacji, cyberprzemocy, marketingu

## Kilka dat:

- po II wojnie światowej — idea telefonii komórkowej
- lata 50'/60' — pierwsze systemy automatyczne w samochodach (MTA, Szwecja)
- 1973 — Martin Cooper (Motorola) — pierwszy ręczny telefon komórkowy
- 1979 — pierwsza komercyjna sieć 1G w Japonii
- 1981 — uruchomienie sieci 1G NMT w Europie z roamingiem (kraje skandynawskie)
- 1991 — pierwsza sieć 2G GSM w Finlandii
- 2001 — pierwsza komercyjna sieć 3G w Japonii

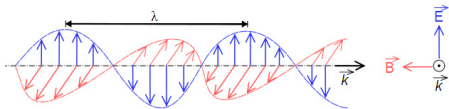
## Kilka dat:

- po II wojnie światowej — idea telefonii komórkowej
- lata 50'/60' — pierwsze systemy automatyczne w samochodach (MTA, Szwecja)
- 1973 — Martin Cooper (Motorola) — pierwszy ręczny telefon komórkowy
- 1979 — pierwsza komercyjna sieć 1G w Japonii
- 1981 — uruchomienie sieci 1G NMT w Europie z roamingiem (kraje skandynawskie)
- 1991 — pierwsza sieć 2G GSM w Finlandii
- 2001 — pierwsza komercyjna sieć 3G w Japonii



## Fale radiowe, anteny

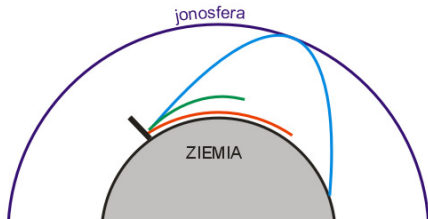
fale elektromagnetyczne o częstotliwości do  
3000 GHz



James Clerk Maxwell, 1831-1879

## Propagacja i zastosowania fal radiowych

- fala powierzchniowa
- fala troposferyczna
- fala jonosferyczna

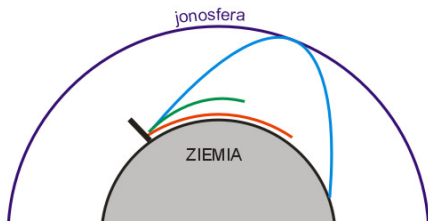


uproszczony podział fal radiowych:

- bardzo długie, 3–30 kHz (VLF)
- długie, do 300 kHz (LF)
- średnie, do 3 MHz (MF)
- krótkie, do 30 MHz (HF)
- ultrakrótkie, do 300 MHz (VHF)
- do 3 GHz (mikrofale, UHF)
  
- mikrofale, do 3000 GHz

## Propagacja i zastosowania fal radiowych

- fala powierzchniowa
- fala troposferyczna
- fala jonosferyczna

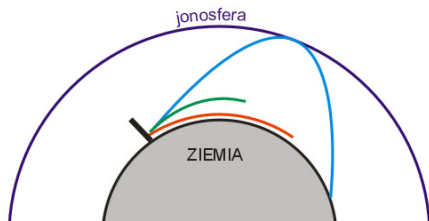


uproszczony podział fal radiowych:

- bardzo długie, 3–30 kHz (VLF)
- długie, do 300 kHz (LF)
- średnie, do 3 MHz (MF)
- krótkie, do 30 MHz (HF)
- ultrakrótkie, do 300 MHz (VHF)
- do 3 GHz (mikrofale, UHF) ⇒ telefonia komórkowa,
- mikrofale, do 3000 GHz

## Propagacja i zastosowania fal radiowych

- fala powierzchniowa
- fala troposferyczna
- fala jonosferyczna



uproszczony podział fal radiowych:

- bardzo długie, 3–30 kHz (VLF)
- długie, do 300 kHz (LF)
- średnie, do 3 MHz (MF)
- krótkie, do 30 MHz (HF)
- ultrakrótkie, do 300 MHz (VHF)
- do 3 GHz (mikrofale, UHF) ⇒ telefonia komórkowa, 450 MHz, 900 MHz, 1800 MHz, okolice 2 GHz
- mikrofale, do 3000 GHz

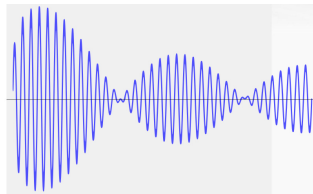
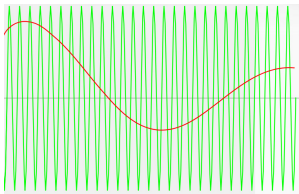




## Jak przesać głos dzięki falom radiowym (przykłady)

fala nośna sygnał fala po modulacji

- modulacja amplitudy

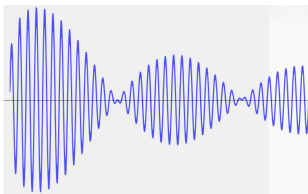
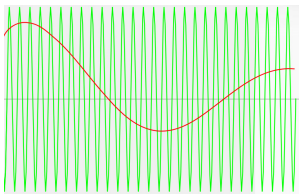


- modulacja częstotliwości

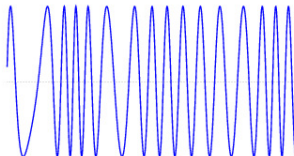
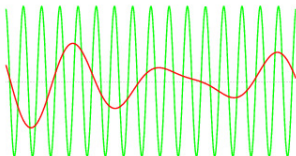
## Jak przesać głos dzięki falom radiowym (przykłady)

fala nośna sygnał fala po modulacji

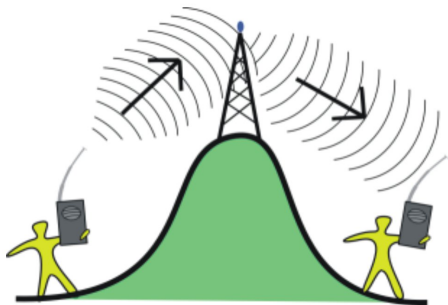
- modulacja amplitudy



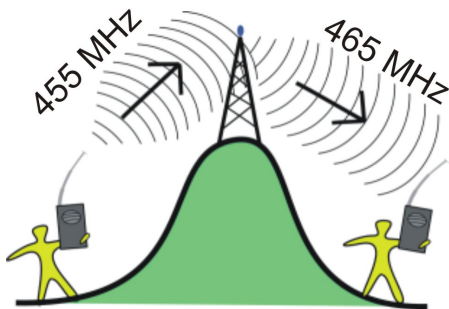
- modulacja częstotliwości



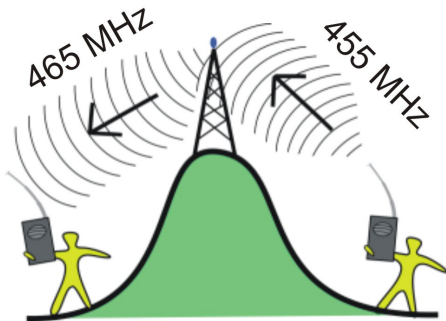
## Organizacja łączności radiowej



## Organizacja łączności radiowej

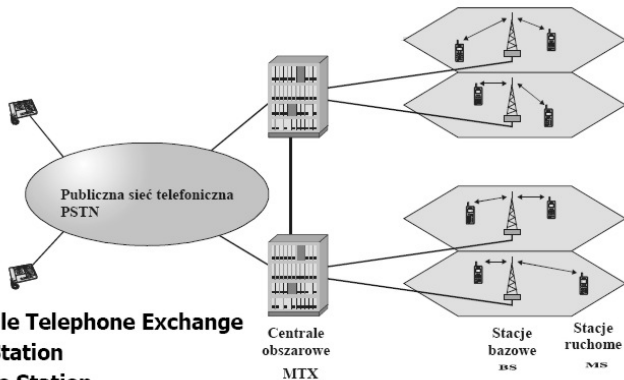


## Organizacja łączności radiowej



## sieć 1G — Nordic Mobile Telephony (NMT)

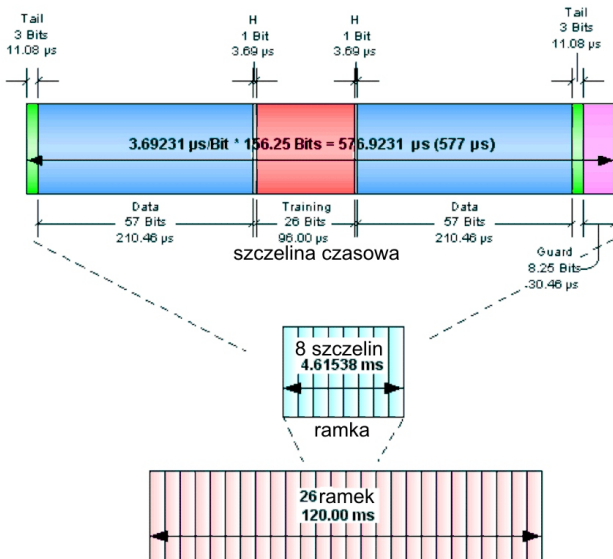
- pasmo 450 i 900 MHz, modulacja FM (prywatność!)
- wielodostęp — FDMA (Frequency Division Multiple Access)
- używana też w telefonii stacjonarnej



- **MTX- Mobile Telephone Exchange**
- **BS- Base Station**
- **MS –Mobile Station**

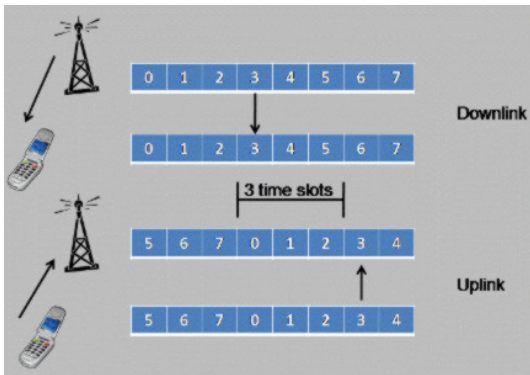
Jacek Stępień

## GSM — TDMA (Time Division Multiple Access) + FDMA



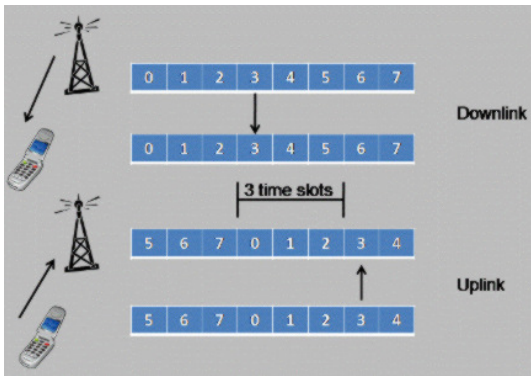
na podstawie: [www.rfcafe.com](http://www.rfcafe.com)

## GSM — TDMA, fizyka i rozmiar komórki



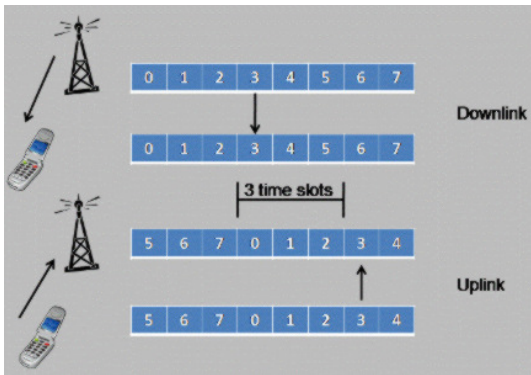


## GSM — TDMA, fizyka i rozmiar komórki



Uwaga: prędkość fal elektromagnetycznych jest duża, ale nie nieskończona!

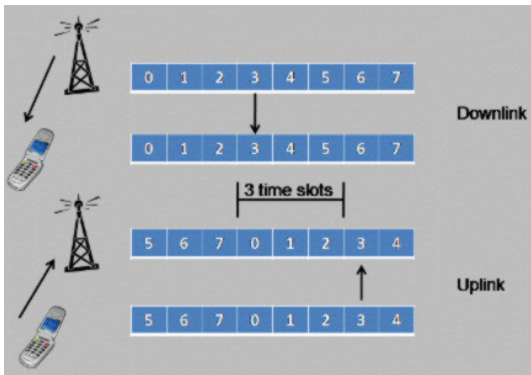
## GSM — TDMA, fizyka i rozmiar komórki



Uwaga: prędkość fal elektromagnetycznych jest duża, ale nie nieskończona!

- 30 km — 100  $\mu$ s (0.1 ms)

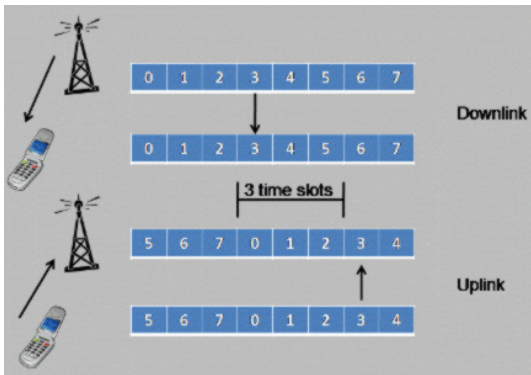
## GSM — TDMA, fizyka i rozmiar komórki



Uwaga: prędkość fal elektromagnetycznych jest duża, ale nie nieskończona!

- 30 km — 100  $\mu$ s (0.1 ms)
- konieczne sygnały Timing Advance (uwaga na prywatność!)

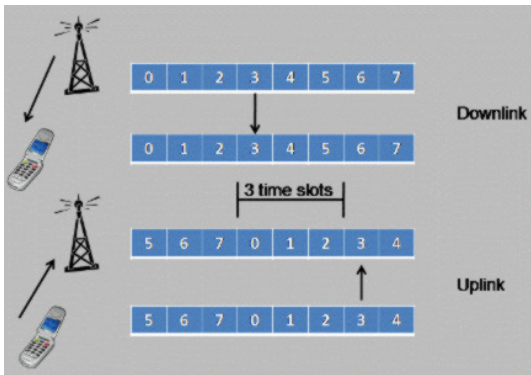
## GSM — TDMA, fizyka i rozmiar komórki



Uwaga: prędkość fal elektromagnetycznych jest duża, ale nie nieskończona!

- 30 km — 100  $\mu$ s (0.1 ms)
- konieczne sygnały Timing Advance (uwaga na prywatność!)
- maksymalny rozmiar komórki: 35 km

## GSM — TDMA, fizyka i rozmiar komórki



Uwaga: prędkość fal elektromagnetycznych jest duża, ale nie nieskończona!

- 30 km — 100  $\mu$ s (0.1 ms)
- konieczne sygnały Timing Advance (uwaga na prywatność!)
- maksymalny rozmiar komórki: 35 km
- możliwość zwiększenia zasięgu przez przydzielenie dwóch szczelin

## GSM — jak przesyłać głos cyfrowo

## GSM — jak przesyłać głos cyfrowo

- 1 zamiana sygnału analogowego (zmienne napięcie) na liczby w systemie dwójkowym

## GSM — jak przesyłać głos cyfrowo

- 1 zamiana sygnału analogowego (zmienne napięcie) na liczby w systemie dwójkowym
- 2 przesłanie za pomocą fal radiowych liczb dwójkowych — ciągów zer i jedynek

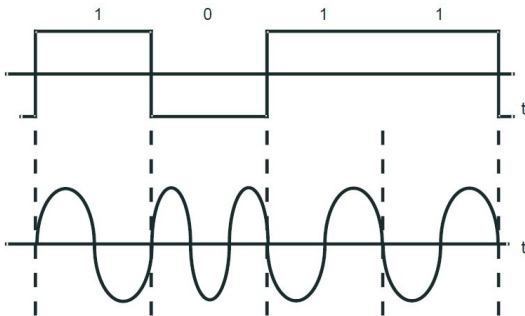


## GSM — jak przesyłać głos cyfrowo

- 1 zamiana sygnału analogowego (zmienne napięcie) na liczby w systemie dwójkowym
- 2 przesłanie za pomocą fal radiowych liczb dwójkowych — ciągów zer i jedynek
- 3 jedna z metod: zmiana częstotliwości fali (FSK, Frequency Shift Keying)

## GSM — jak przesyłać głos cyfrowo

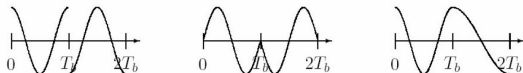
- 1 zamiana sygnału analogowego (zmiennie napięcie) na liczby w systemie dwójkowym
- 2 przesłanie za pomocą fal radiowych liczb dwójkowych — ciągów zer i jedynek
- 3 jedna z metod: zmiana częstości fali (FSK, Frequency Shift Keying)



MX-COM

GSM — zajmowane pasmo radiowe musi być jak najmniejsze!

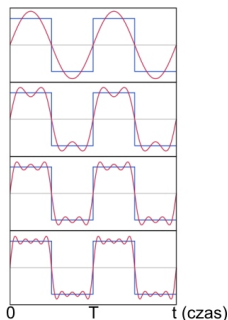
różne scenariusze zmiany częstotliwości



przykład: przebieg prostokątny o okresie  $T$

$$\sum_n \frac{1}{n} \sin\left(n \frac{2\pi t}{T}\right), n = 1, 3, 5 \dots$$

$$\sin\left(\frac{2\pi t}{T}\right) + \frac{1}{3} \sin\left(3 \frac{2\pi t}{T}\right) + \dots$$



- różnica częstotliwości dla zer i jedynek =  $0.5 \times$  szybkość transmisji
- modulacja MSK (Minimum Shift Keying) z dodatkowym zawężeniem pasma (GMSK, Gaussian MSK)
- w GSM: różnica częstotliwości:  $\pm 67.708$  kHz, szybkość transmisji: 270.833 kbps

## GSM — stacje bazowe (BTS, Base Transceiver Station), sieć szkieletowa

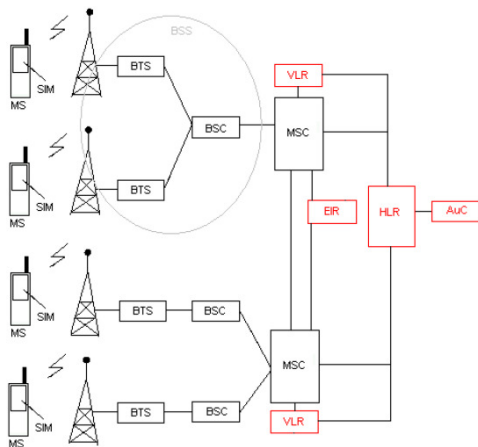
### Elementy BTS:

- anteny (np. sektorowe,  $120^{\circ}$ )
- układ nadawczo-odbiorczy ze wzmacniaczem
- układ sterowania
- układ zasilania i akumulatory
- układ testujący i alarmowy
- klimatyzacja
- radiolinia lub kabel do sieci szkieletowej



## GSM — stacje bazowe (BTS, Base Transceiver Station), sieć szkieletowa

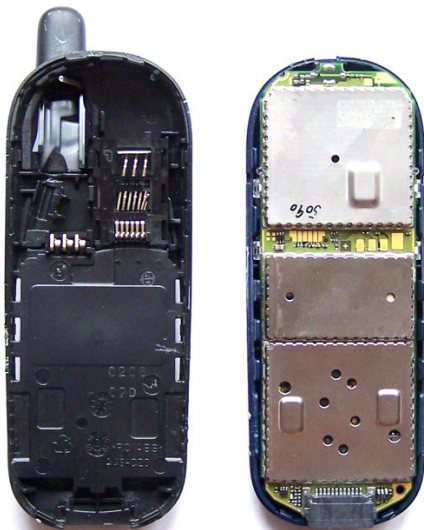
- BSC — kontroler stacji bazowych
- MSC — centrala telefoniczna
- HLR, VLR, EIR — rejestry abonentów i telefonów



Krzysztof Liszewski, Porównanie bezpieczeństwa systemów GSM i UMTS, 2007

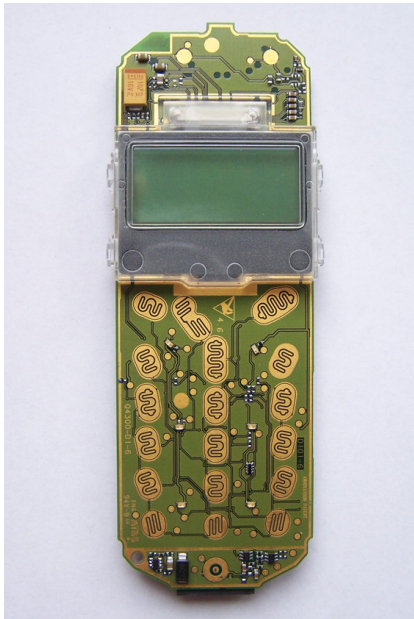


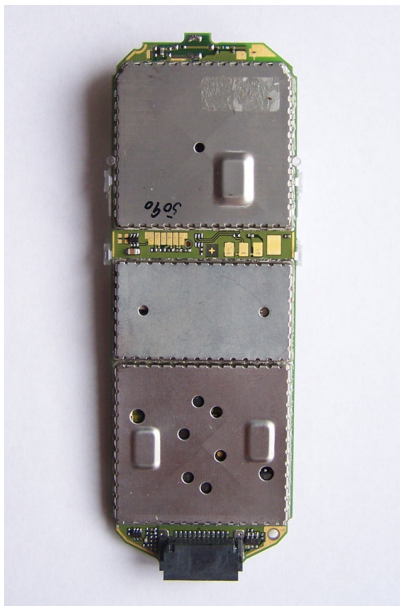
## GSM — budowa telefonu (Siemens A36)

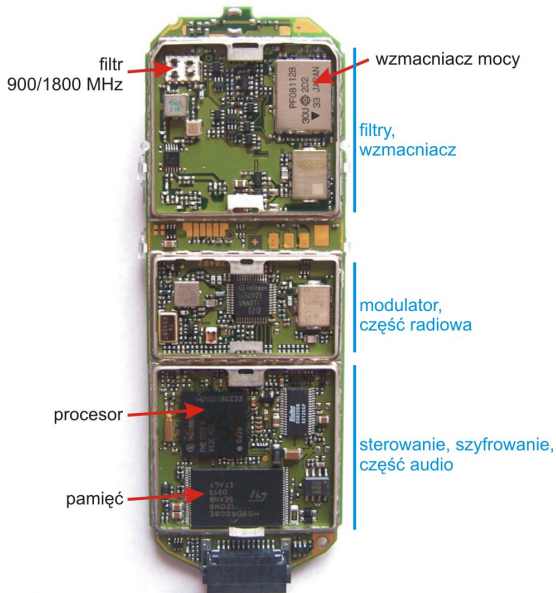




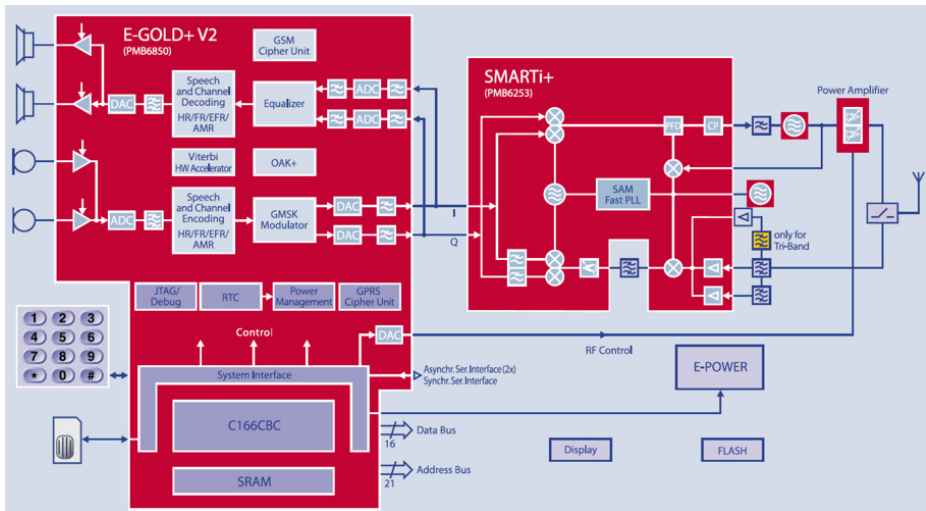








## GSM — budowa telefonu — przykładowy schemat blokowy



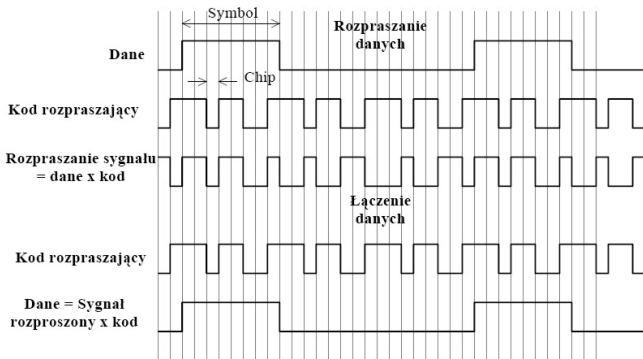
Infineon Technologies

## System 3G UMTS — Universal Mobile Telecommunications System

- wielodostęp realizowany przez CDMA — Code Division Multiple Access

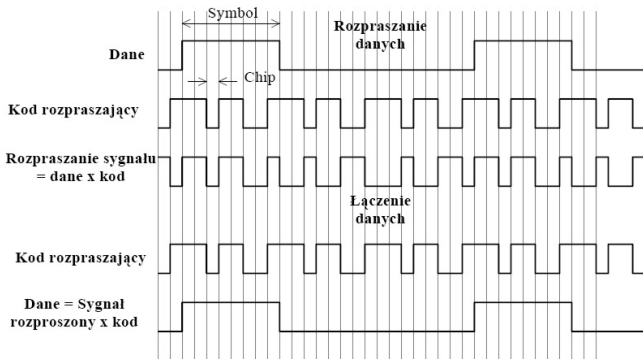
## System 3G UMTS — Universal Mobile Telecommunications System

- wielodostęp realizowany przez CDMA — Code Division Multiple Access
- rozpraszanie widma sygnału do 5 MHz przez tzw. ciągi ortogonalne



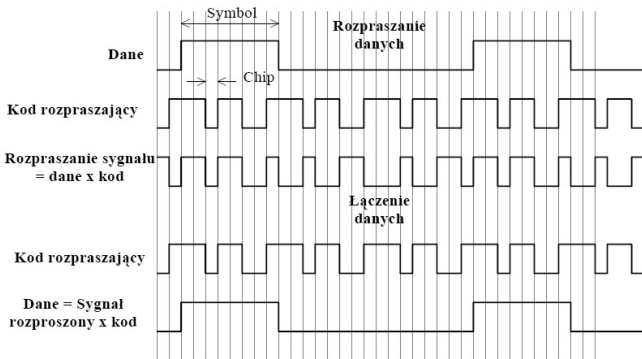
## System 3G UMTS — Universal Mobile Telecommunications System

- wielodostęp realizowany przez CDMA — Code Division Multiple Access
- rozpraszanie widma sygnału do 5 MHz przez tzw. ciągi ortogonalne
- transmisje wielu telefonów — w tym samym kanale jednocześnie



## System 3G UMTS — Universal Mobile Telecommunications System

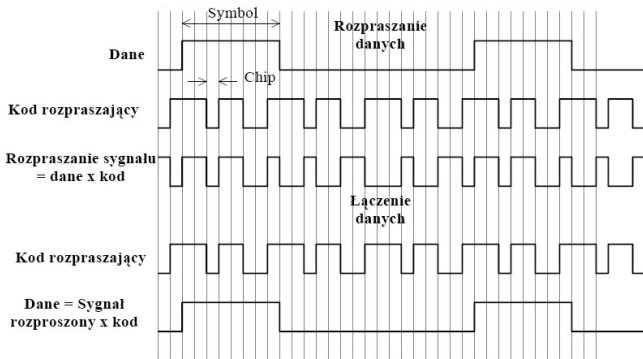
- wielodostęp realizowany przez CDMA — Code Division Multiple Access
- rozpraszanie widma sygnału do 5 MHz przez tzw. ciągi ortogonalne
- transmisje wielu telefonów — w tym samym kanale jednocześnie
- odporność na zakłócenia, sąsiednie stacje bazowe (Node B) mogą pracować na tej samej częstotliwości





## System 3G UMTS — Universal Mobile Telecommunications System

- wielodostęp realizowany przez CDMA — Code Division Multiple Access
- rozpraszanie widma sygnału do 5 MHz przez tzw. ciągi ortogonalne
- transmisje wielu telefonów — w tym samym kanale jednocześnie
- odporność na zakłócenia, sąsiednie stacje bazowe (Node B) mogą pracować na tej samej częstotliwości
- konieczna budowa nowej infrastruktury radiowej względem BTS GSM



Czy korzystanie z telefonów komórkowych jest bezpieczne dla zdrowia?

- orientacyjna moc telefonu: 1–4 W (sieci analogowe), 10 mW – 2 W (GSM, UMTS)
- orientacyjna moc stacji bazowej: < 100 W (GSM)
- częstotliwość: 0.45 – 2.1 GHz (kuchenka mikrofalowa: 2.4 GHz)

Czy korzystanie z telefonów komórkowych jest bezpieczne dla zdrowia?

- orientacyjna moc telefonu: 1–4 W (sieci analogowe), 10 mW – 2 W (GSM, UMTS)
  - orientacyjna moc stacji bazowej: < 100 W (GSM)
  - częstotliwość: 0.45 – 2.1 GHz (kuchenka mikrofalowa: 2.4 GHz)
- 
- efekty termiczne promieniowania elektromagnetycznego (mózg, rogówka)
  - efekty nietermiczne (?)
  - zwiększenie ryzyka powstania nowotworów (?)
  - zaburzenia snu, bóle głowy, zmęczenie (?)
  - konieczne więcej badań, przebadanie osób używających telefonów komórkowych przez wiele lat (> 10), uwzględnienie wpływu zarówno telefonu jak i stacji bazowej

Czy korzystanie z telefonów komórkowych jest bezpieczne dla zdrowia?

- orientacyjna moc telefonu: 1–4 W (sieci analogowe), 10 mW – 2 W (GSM, UMTS)
- orientacyjna moc stacji bazowej: < 100 W (GSM)
- częstotliwość: 0.45 – 2.1 GHz (kuchenka mikrofalowa: 2.4 GHz)
  
- efekty termiczne promieniowania elektromagnetycznego (mózg, rogówka)
- efekty nietermiczne (?)
- zwiększenie ryzyka powstania nowotworów (?)
- zaburzenia snu, bóle głowy, zmęczenie (?)
- konieczne więcej badań, przebadanie osób używających telefonów komórkowych przez wiele lat (> 10), uwzględnienie wpływu zarówno telefonu jak i stacji bazowej
- udowodniona szkodliwość pośrednia: rozproszenie uwagi w aspekcie fizycznym, poznawczym, słuchowym, wzrokowym ⇒ **WYPADKI SAMOCHODOWE**

Czy da się podsłuchiwać rozmowy w systemie GSM bez pośrednictwa operatora sieci i bez modyfikacji telefonu ofiary?

### Słabe strony systemu GSM:

- brak kontroli autentyczności sieci przez telefon
- używanie tego samego klucza do kilku rozmów oraz w różnych algorytmach
- używanie zbyt słabego algorytmu szyfrującego A5/1, a wcześniej bardzo słabego A5/2

### ⇒ potencjalna możliwość:

- podsłuchiwanie rozmów i przechwytywanie SMSów
- fałszowania rozmów i SMSów
- rozmów na czyjś koszt

Rodzaje ataków:

- **pasywne** — tylko podsłuch, konieczny sprzęt, duża moc obliczeniowa lub dostęp do karty SIM ofiary
- **aktywne** — podsłuch i nadawanie: man in the middle, konieczny dodatkowy sprzęt, umiarkowana moc obliczeniowa, jeśli telefon obsługuje słaby algorytm A5/2

## Przykładowy scenariusz...

