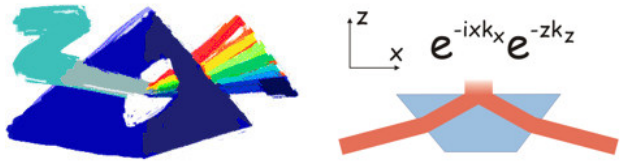
Jak działa telefonia komórkowa

Tomasz Kawalec

28 stycznia 2013

Zakład Optyki Atomowej, Instytut Fizyki UJ



www.coldatoms.com

- Jak przesłać głos i dane przy pomocy fal radiowych?
- Do czego naprawdę służy karta SIM?
- Czym różnią się kolejne generacje sieci komórkowych?
- Czy można nas podsłuchać?
- Skąd bierze się rozmiar komórki w GSM?

Kilka dat

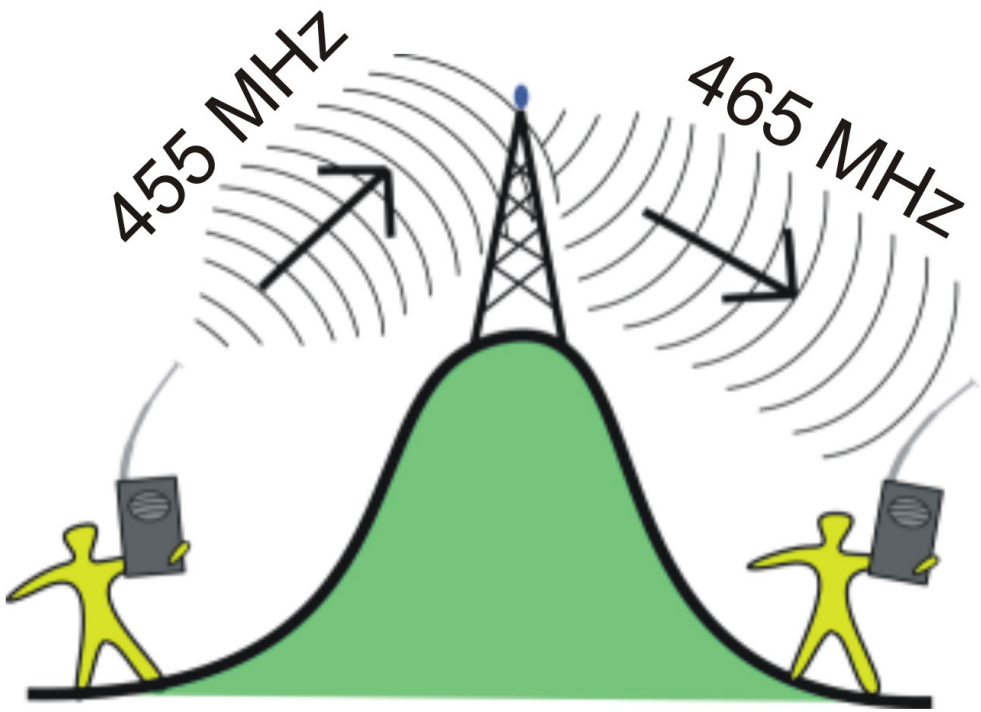
- po II wojnie światowej — idea telefonii komórkowej
- podstawy cyfrowego przesyłania sygnałów
- lata 50'/60' — pierwsze systemy automatyczne w samochodach (np. MTA, Szwecja)
- 1973 — Martin Cooper (Motorola) — pierwszy ręczny telefon komórkowy
- 1979 — pierwsza komercyjna sieć 1G w Japonii
- 1981 — 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
- podstawy cyfrowego przesyłania sygnałów
- lata 50'/60' — pierwsze systemy automatyczne w samochodach (np. 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

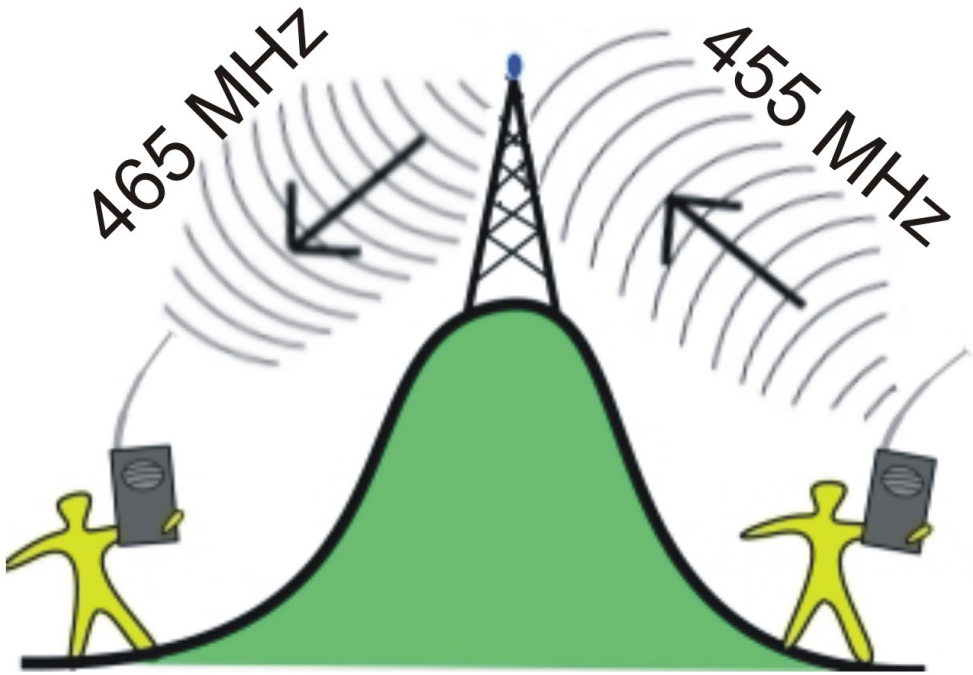
Organizacja łączności radiowej

- przemienniki, stacje bazowe
- wielodostęp, sieci trunkingowe
- simplex, duplex, duosimplex
- modulacja — głos: cyfrowa lub analogowa, kanał kontrolny: cyfrowa



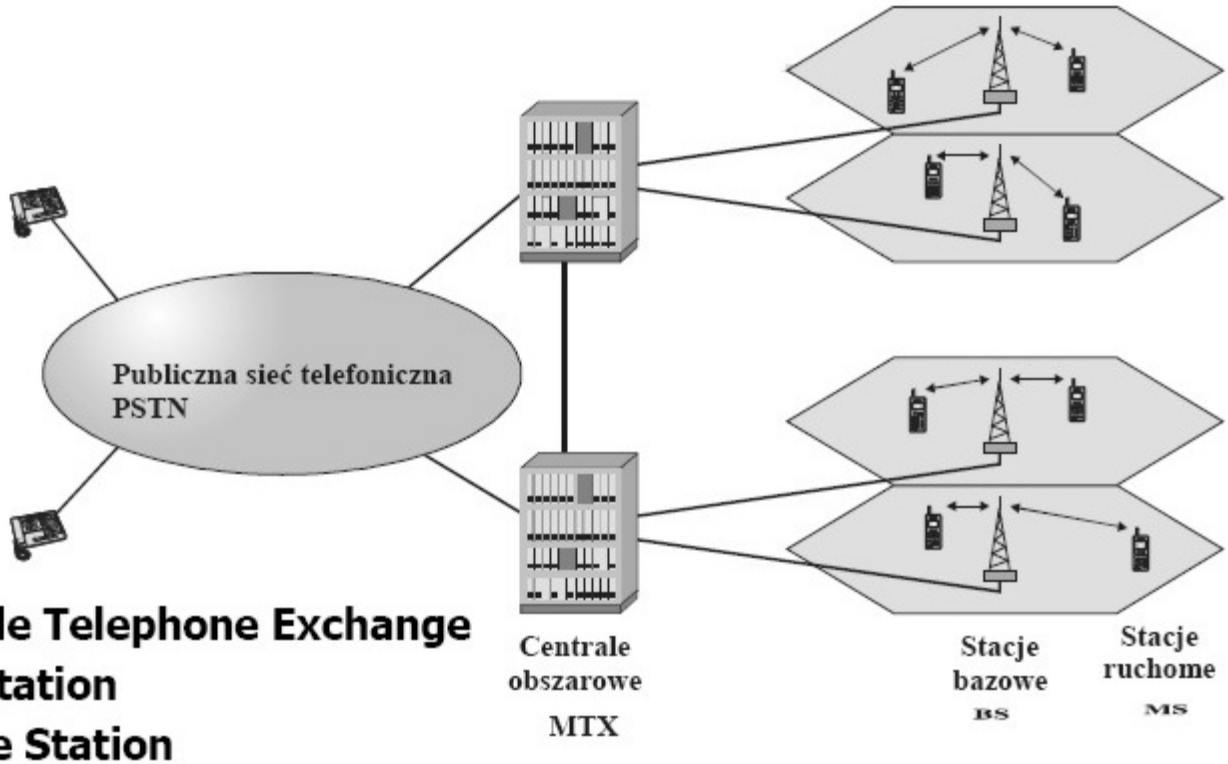
Organizacja łączności radiowej

- przemienniki, stacje bazowe
- wielodostęp, sieci trunkingowe
- simplex, duplex, duosimplex
- modulacja — głos: cyfrowa lub analogowa, kanał kontrolny: cyfrowa



sieć 1G — Nordic Mobile Telephony (NMT)

- pasmo 450 i 900 MHz, modulacja FM bez szyfrowania (prywatność!)
- kanał kontrolny nie jest szyfrowany
- wielodostęp — FDMA (Frequency Division Multiple Access)
- używana też w telefonii stacjonarnej na terenach wiejskich
- używana chętnie przez rybaków i przy granicy polsko-ukraińskiej



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

Jacek Stępień

sieć 1G — Nordic Mobile Telephony (NMT)

- ramka: 166 bitów, 1200 bit/s
- synchronizacja: 15 + 11 bitów, dane: 140 bitów
- dane bez korekcji błędów: 64 bity (16 znaków)

sieć 1G — Nordic Mobile Telephony (NMT)

- ramka: 166 bitów, 1200 bit/s
- synchronizacja: 15 + 11 bitów, dane: 140 bitów
- dane bez korekcji błędów: 64 bity (16 znaków)

przykładowa ramka informacji

1010101010101011110001001010001000101000
0010011111100000010000010101100000111111011010 11
1010101010101010101010101010101010101010101010101
0101010101010101010101010101010101010

1. 0101 1000 1001: średnia moc, kanał 89
2. 1100 0111 1001: kanał sygnalizacyjny, kod obszaru 79

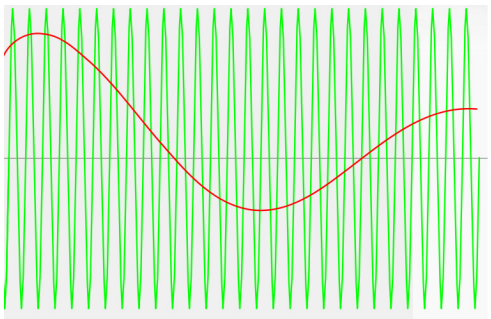
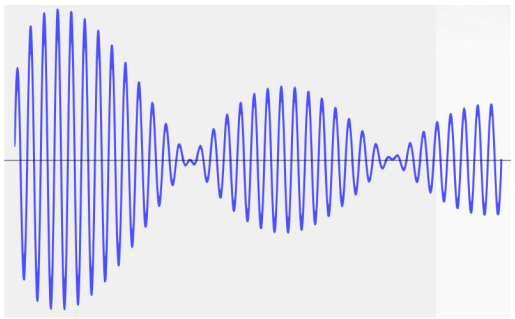
Modulacje analogowe

Możliwości modulacji fali radiowej:

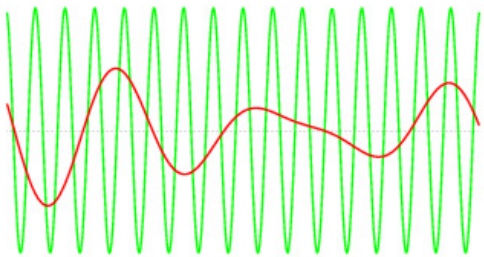
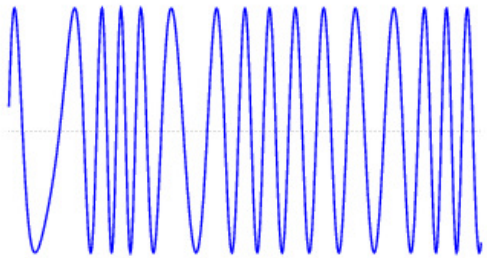
$$\vec{E}(t) = \hat{\epsilon} E_0(t) \cos(\omega(t)t + \phi(t))$$

fala nośna sygnał fala po modulacji

- modulacja amplitudy AM oraz modulacja wstęgowa (SSB i inne)

- modulacja częstotliwości FM (używana w NMT)

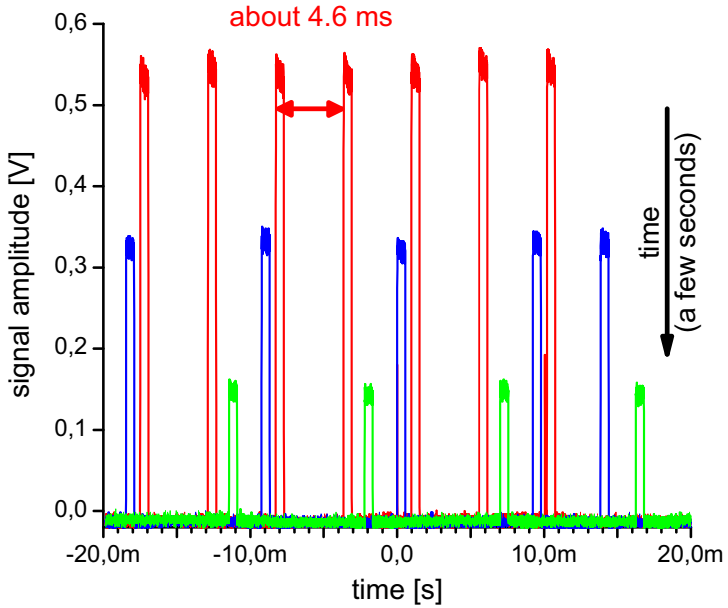
- modulacja fazy PM (używana w modulacjach cyfrowych)

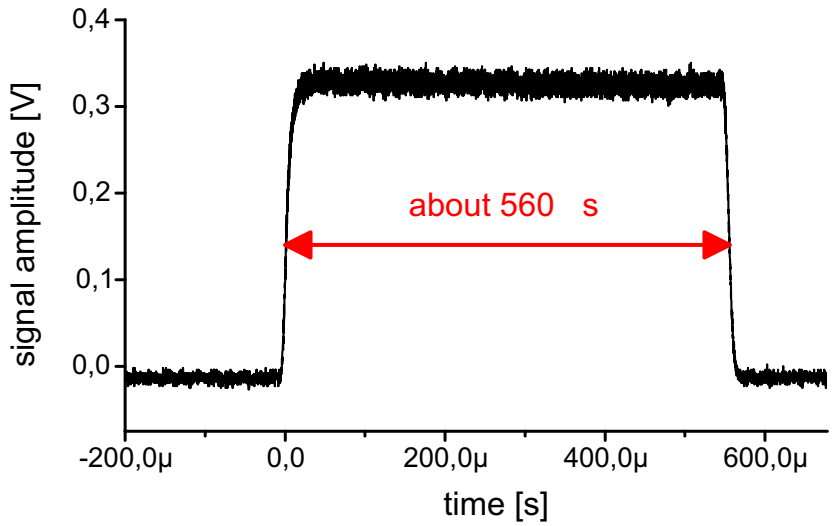
GSM — TDMA (Time Division Multiple Access) + FDMA

- telefon w trybie GSM
- prosta antena

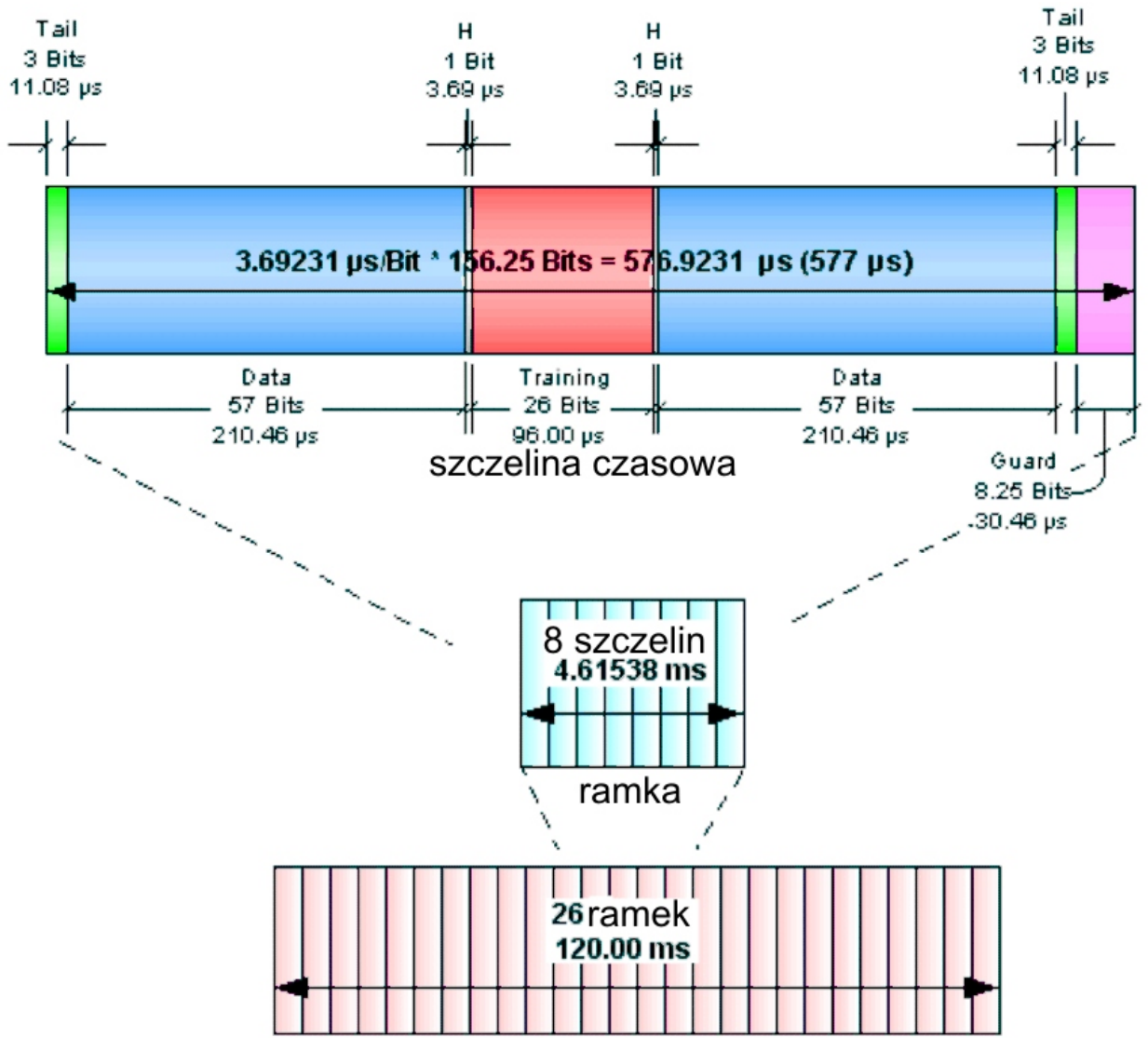
GSM — TDMA (Time Division Multiple Access) + FDMA

- telefon w trybie GSM
- prosta antena



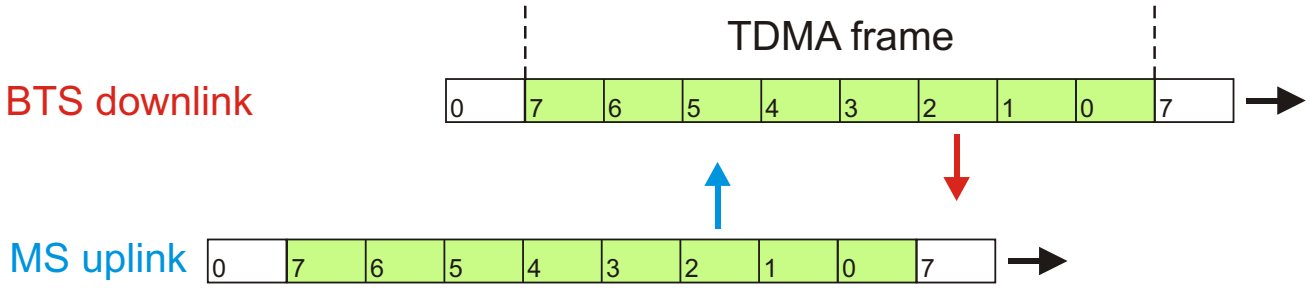


GSM — TDMA (Time Division Multiple Access) + FDMA

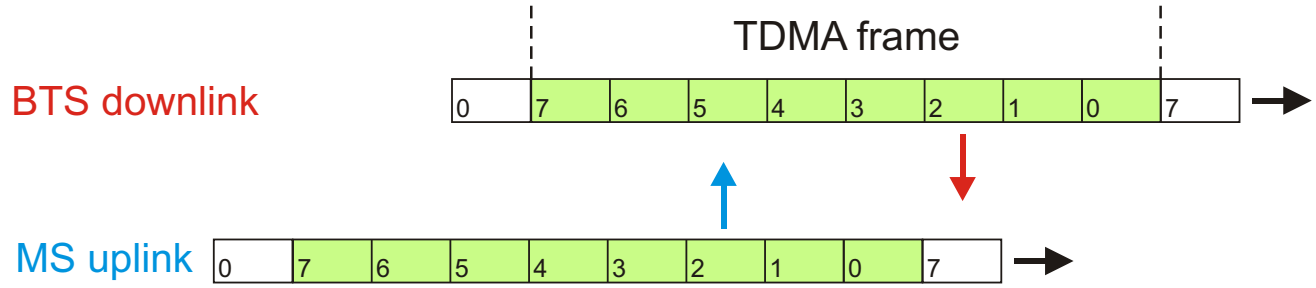


na podstawie: www.rfcafe.com

GSM — TDMA, rozmiar komórki

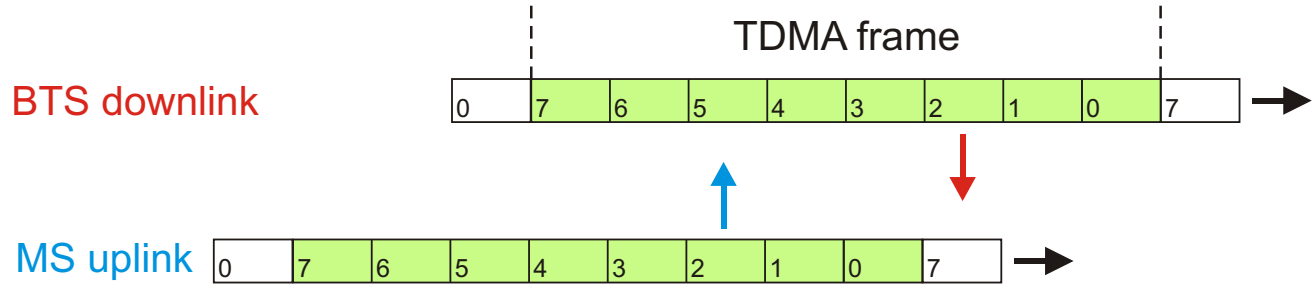


GSM — TDMA, rozmiar komórki



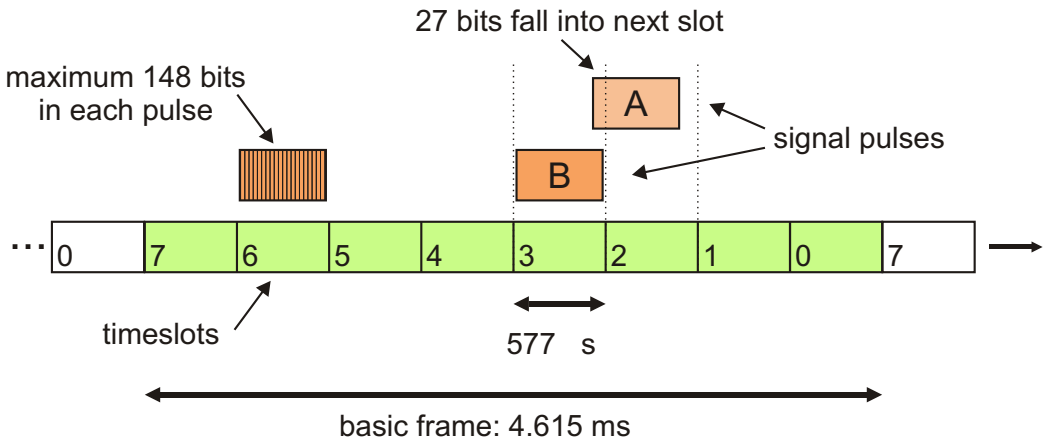
Prędkość fal elektromagnetycznych — skończona $\Rightarrow$

GSM — TDMA, rozmiar komórki



Prędkość fal elektromagnetycznych — skończona $\Rightarrow$

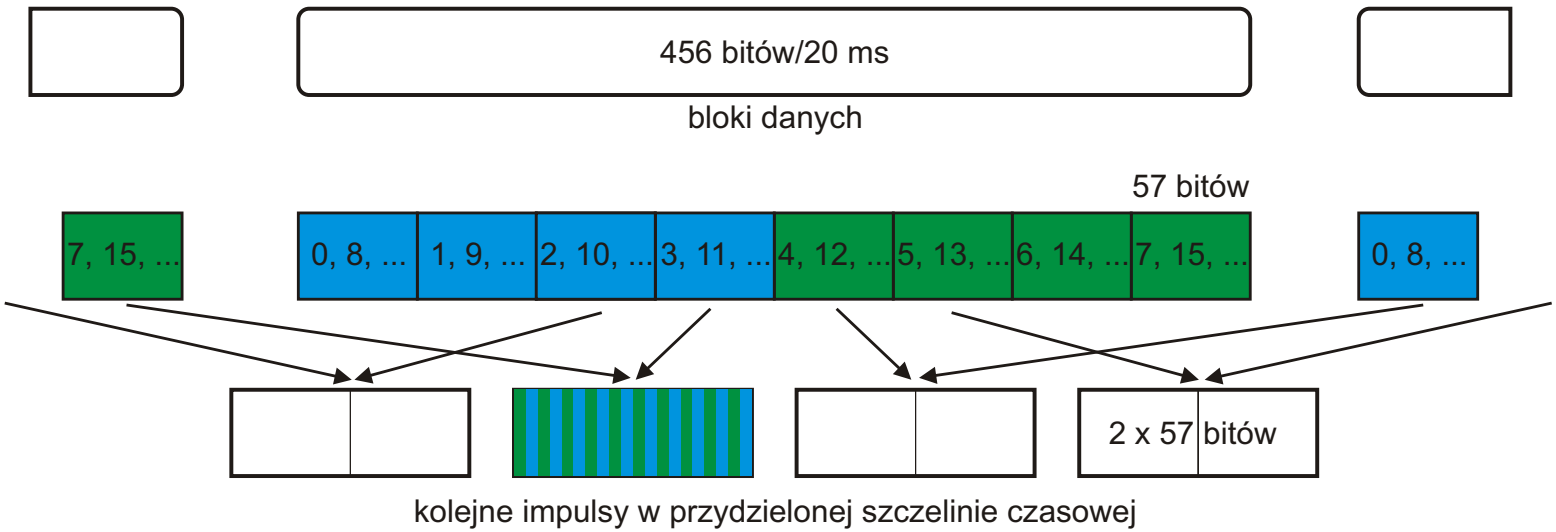
- 30 km — 100 μs
- konieczne sygnały Timing Advance, maksymalny rozmiar komórki: 35 km
- możliwość zwiększenia zasięgu przez przydzielenie dwóch szczelin



TK, Physics Education, **21**, 392 (2012)

Wybrane parametry transmisji

- przepustowość kanału: 270.833 kb/s, ale 8 szczelin czasowych (impulsów)
- 2×57 bitów informacji w 1 impulsie
- głos: ADC @ (8kHz, 13 bit); 104 kb/s $\rightarrow$ 13 kb/s, czyli 260 bitów/20 ms
- bity parzystości + nadmiarowe: 260 bitów $\rightarrow$ blok 456 bitów dzielonych na fragmenty po 57 bitów
- przeplot bitowy i międzyimpulsowy: blok 456 bitów $\rightarrow$ przesyłany w 8 impulsach



Modulacje cyfrowe — FSK, MSK

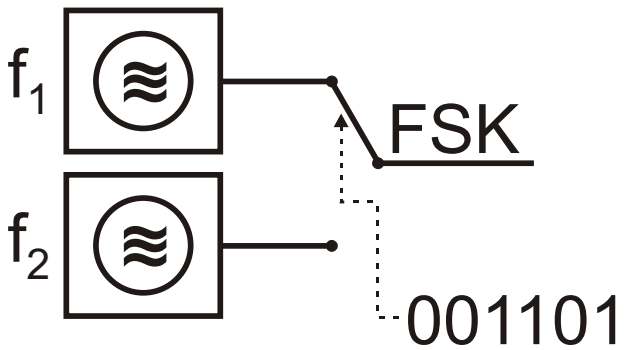
przełączanie częstotliwości f_1 i f_2

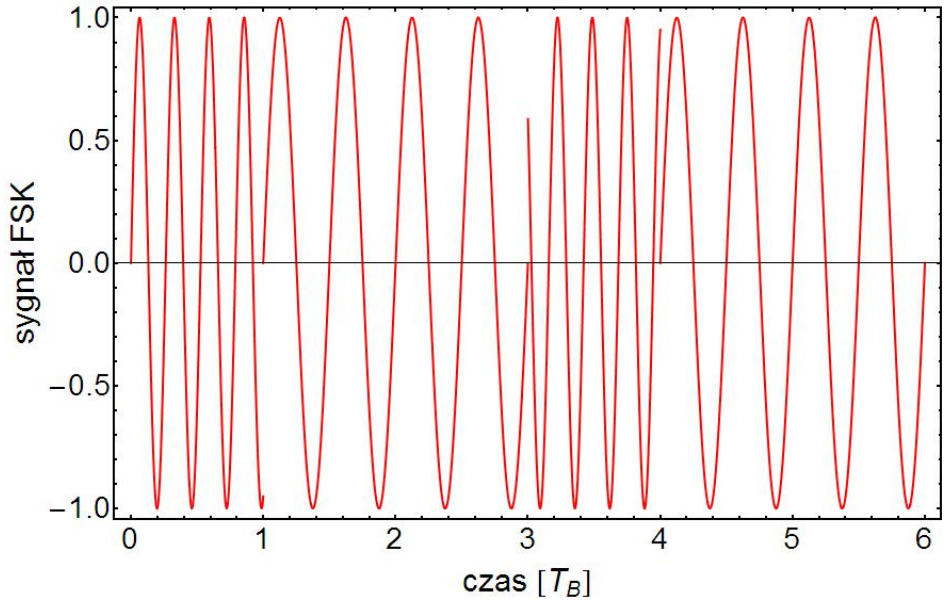
ciągłość fazy $\Leftrightarrow \frac{f_2-f_1}{f_T} \in \mathbb{N}$,
ale z warunku ortogonalności

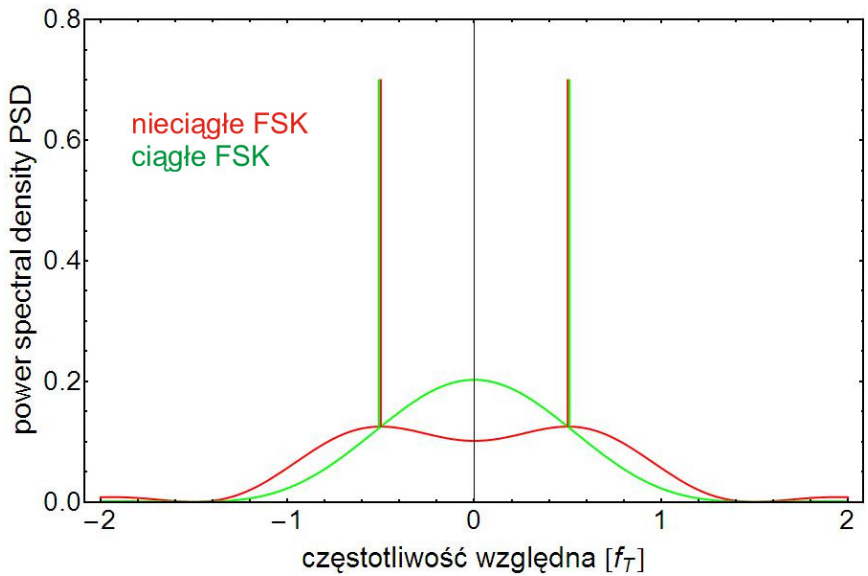
$$\int_0^{T_B} \sin(2\pi f_1 t)\sin(2\pi f_2 t) = 0$$

$$\Rightarrow h \equiv \frac{f_2-f_1}{f_T} \geq \frac{i}{2},\ i = 1,\ 2, \ldots$$

$h = \frac{1}{2}$: modulacja MSK







Modulacje cyfrowe — FSK, MSK

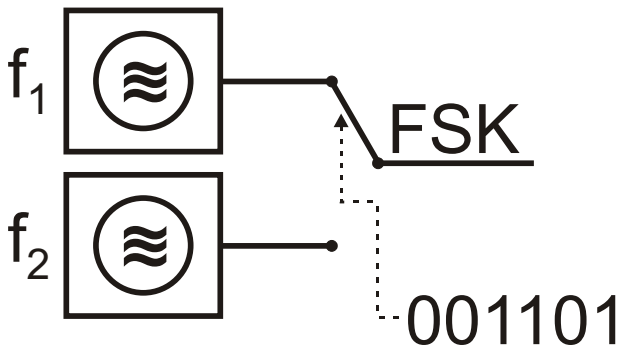
przełączanie częstotliwości f_1 i f_2

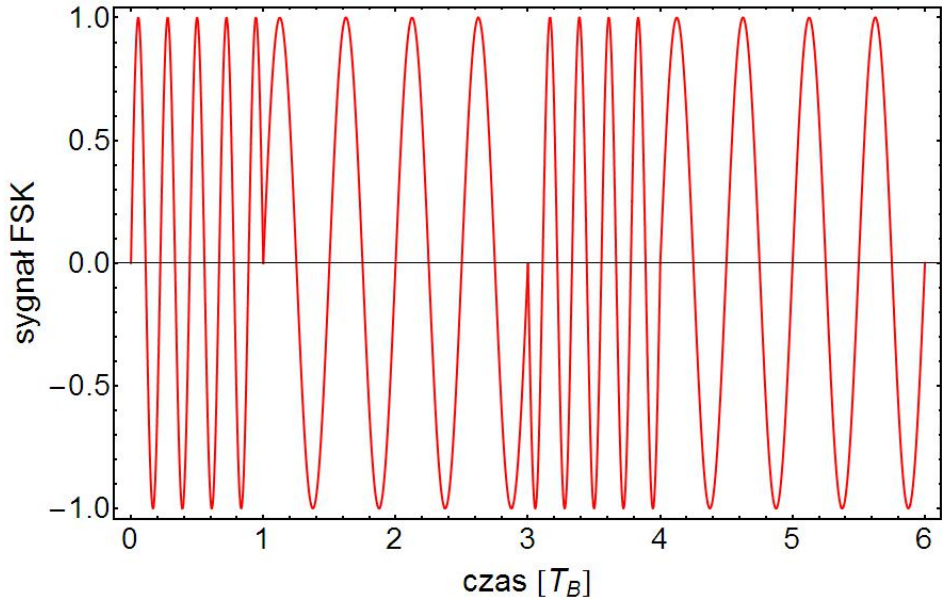
ciągłość fazy $\Leftrightarrow \frac{f_2-f_1}{f_T} \in \mathbb{N}$,
ale z warunku ortogonalności

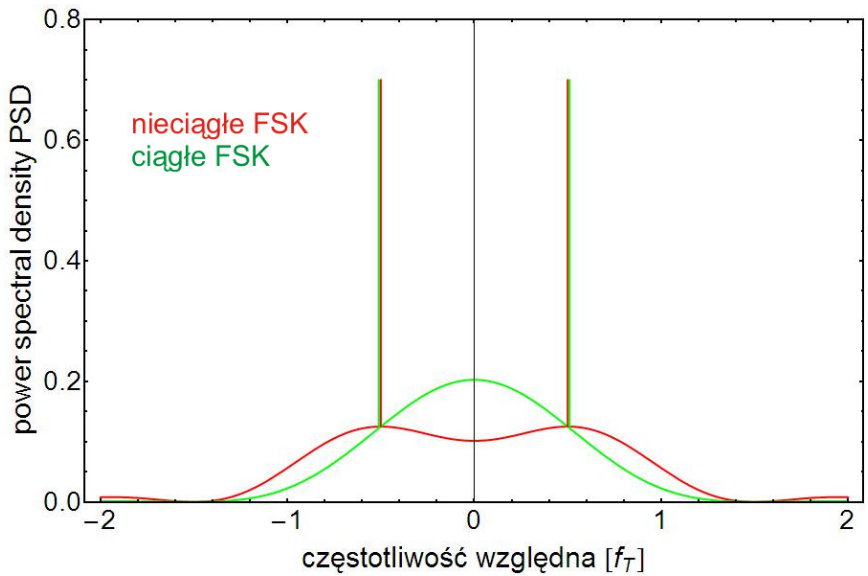
$$\int_0^{T_B} \sin(2\pi f_1 t)\sin(2\pi f_2 t) = 0$$

$$\Rightarrow h \equiv \frac{f_2-f_1}{f_T} \geq \frac{i}{2},\ i = 1,\ 2, \ldots$$

$h = \frac{1}{2}$: modulacja MSK







Modulacje cyfrowe — FSK, MSK

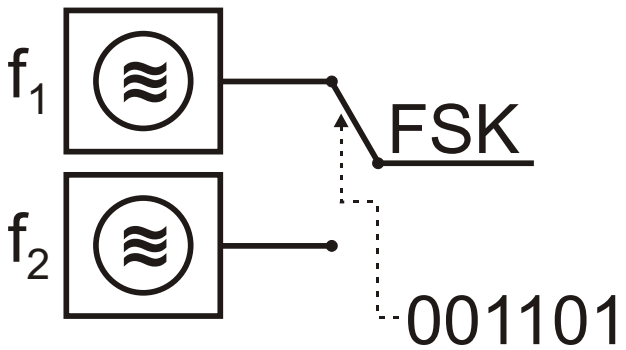
przełączanie częstotliwości f_1 i f_2

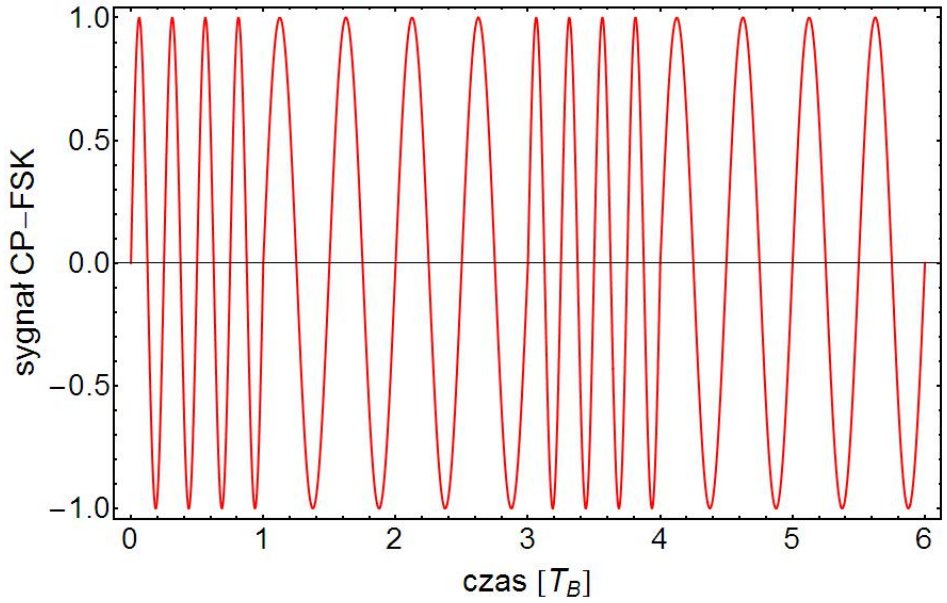
ciągłość fazy $\Leftrightarrow \frac{f_2-f_1}{f_T} \in \mathbb{N}$,
ale z warunku ortogonalności

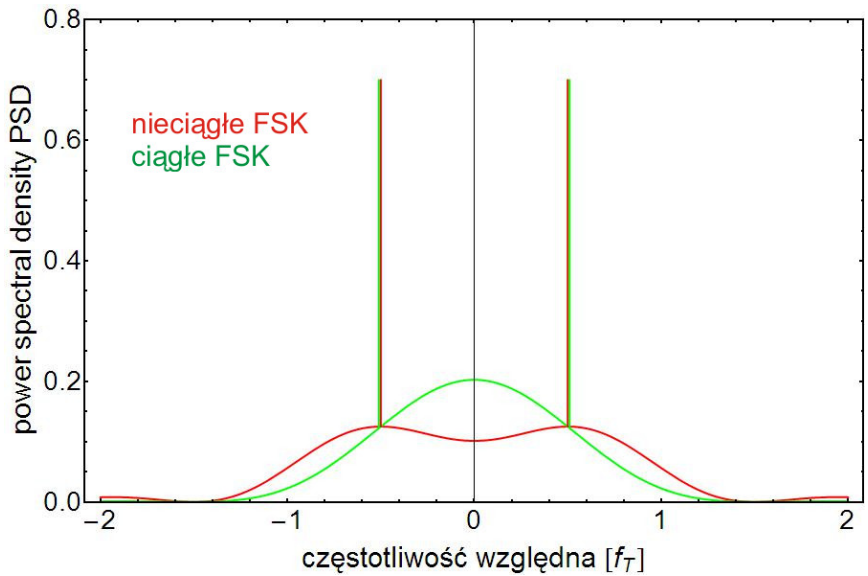
$$\int_0^{T_B} \sin(2\pi f_1 t)\sin(2\pi f_2 t) = 0$$

$$\Rightarrow h \equiv \frac{f_2-f_1}{f_T} \geq \frac{i}{2},\ i = 1,\ 2, \ldots$$

$h = \frac{1}{2}$: modulacja MSK







Modulacje cyfrowe — ASK, BPSK

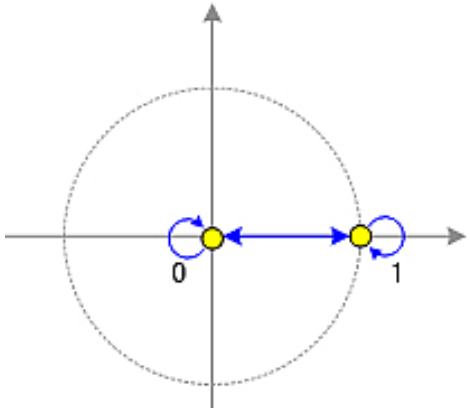
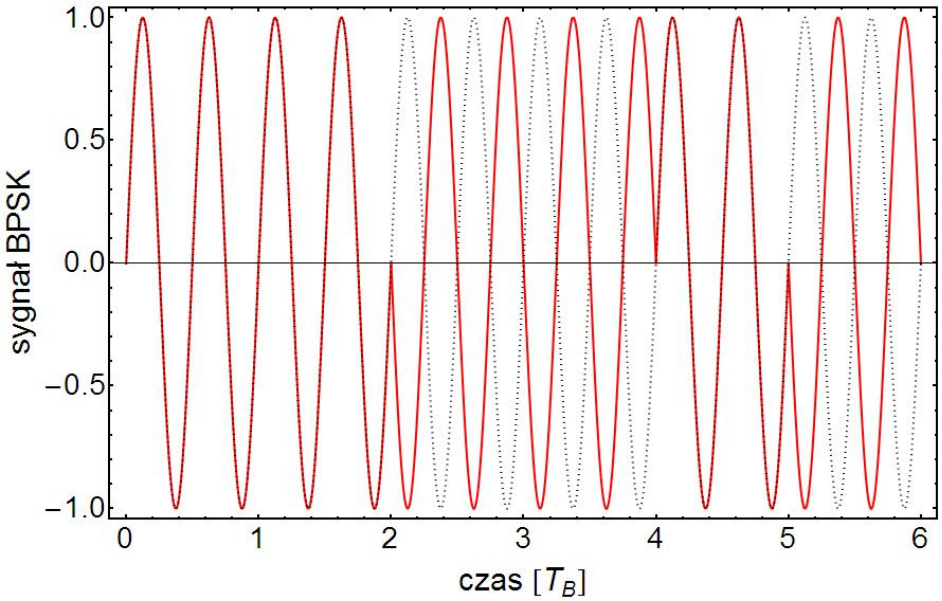
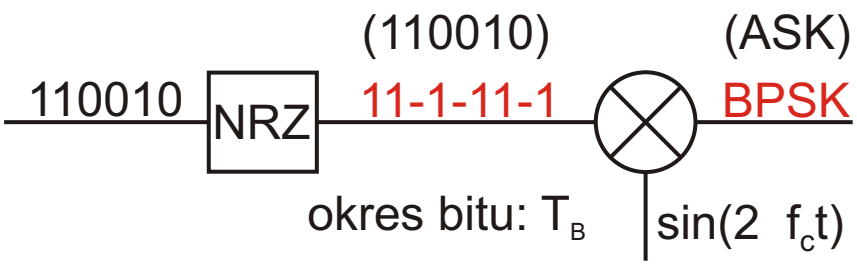
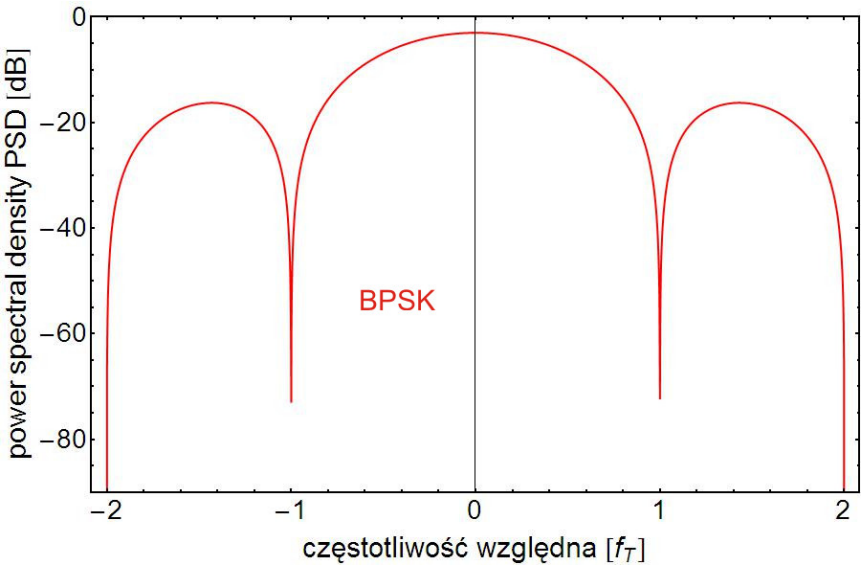


diagram konstelacyjny ASK







Modulacje cyfrowe — ASK, BPSK

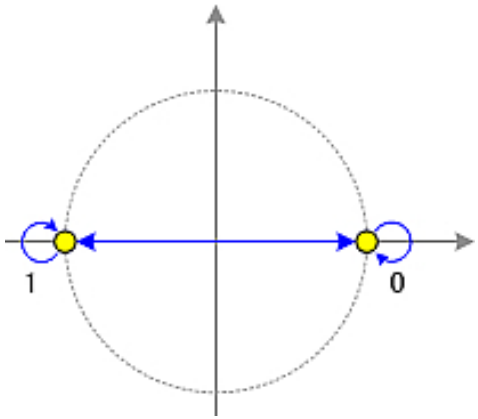
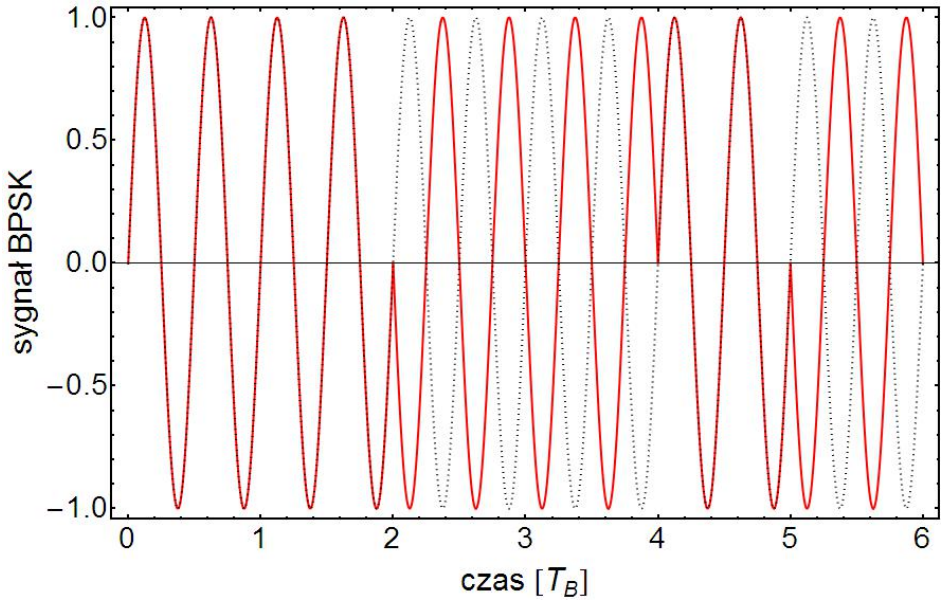
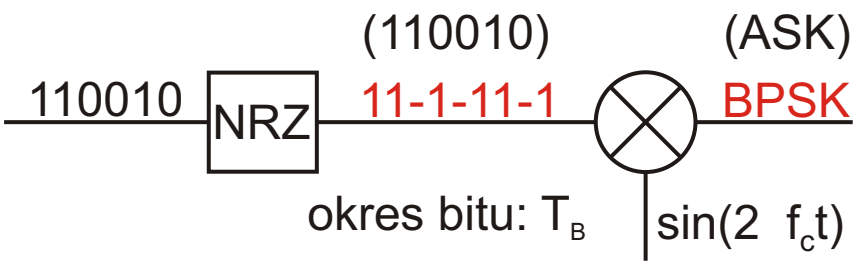
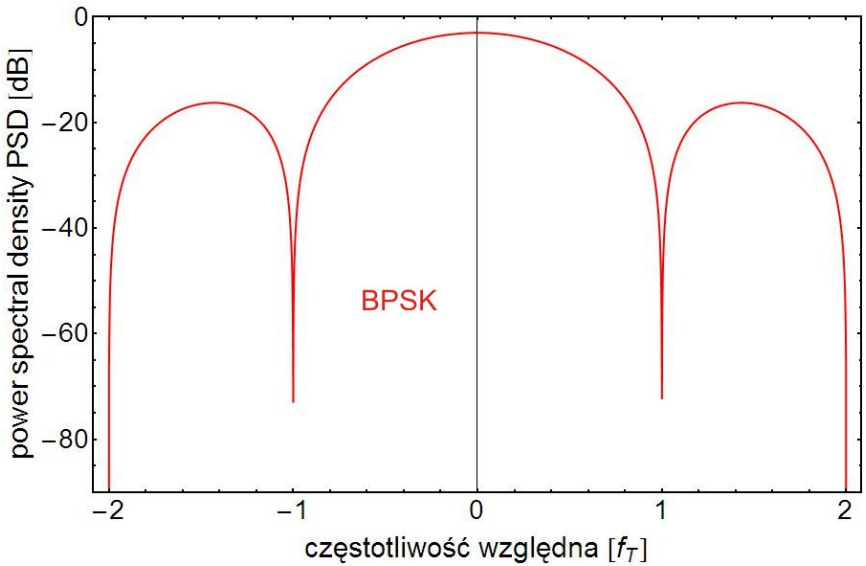


diagram konstelacyjny BPSK







Modulacje cyfrowe — QPSK

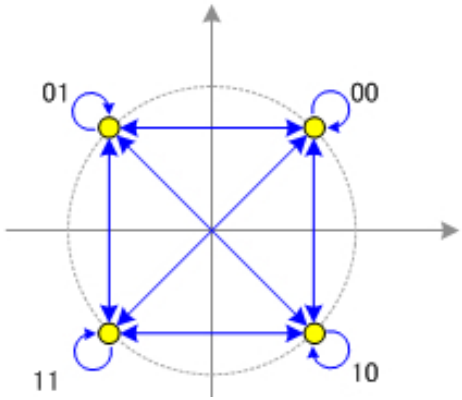
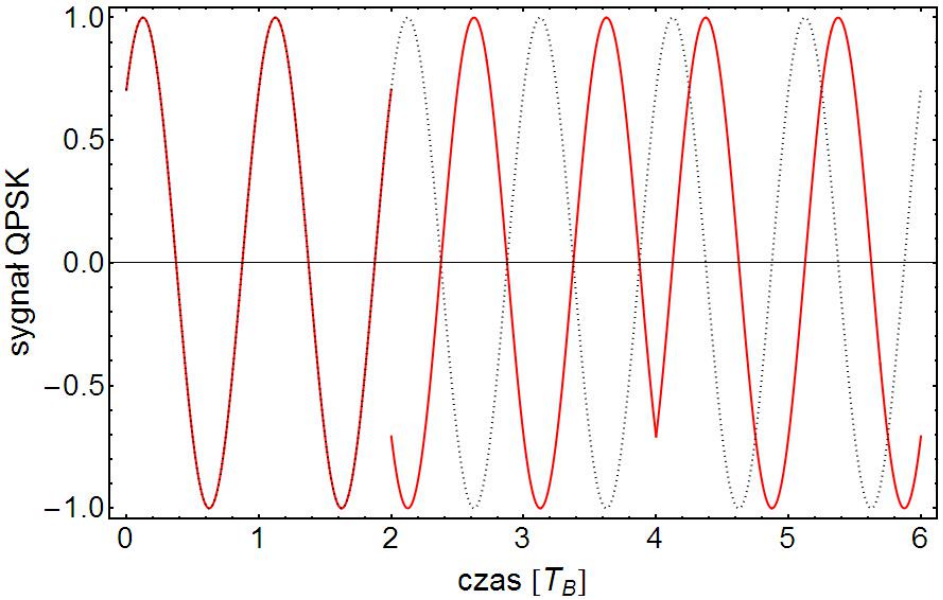
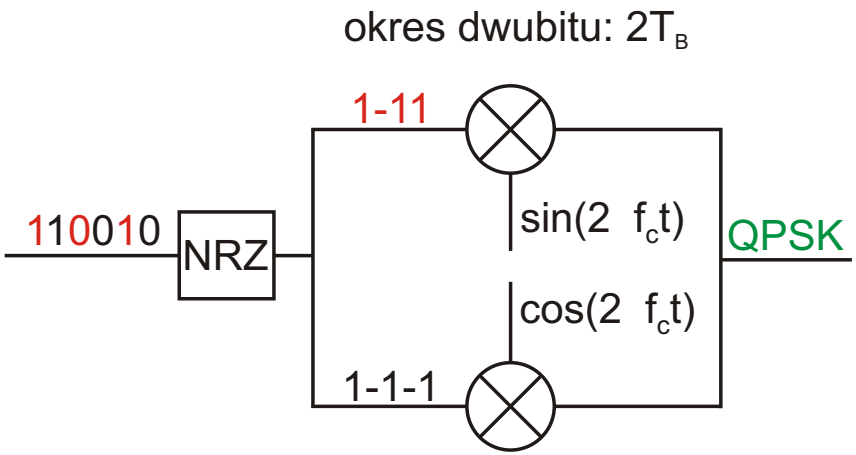
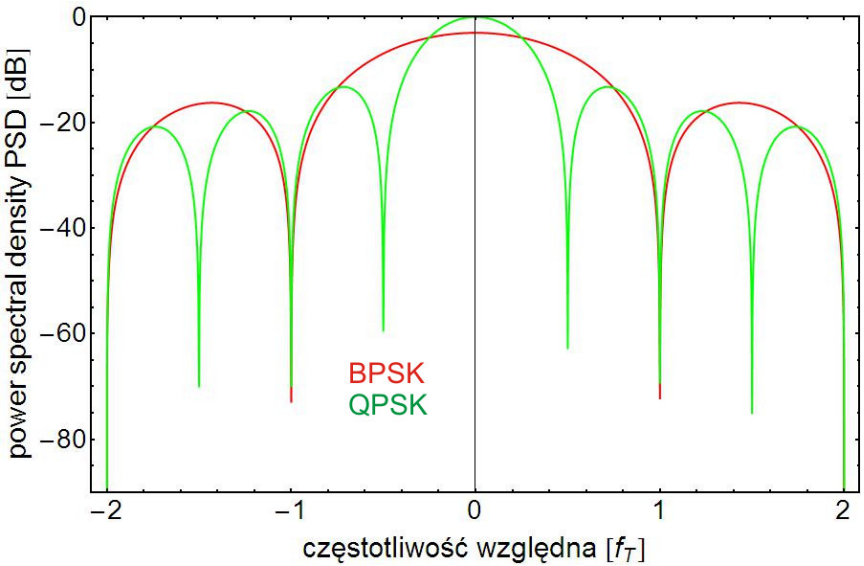


diagram konstelacyjny QPSK







Modulacje cyfrowe — OQPSK

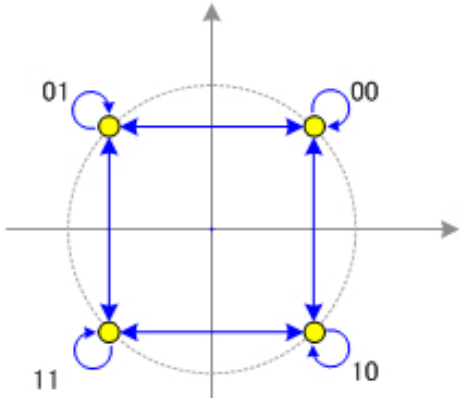
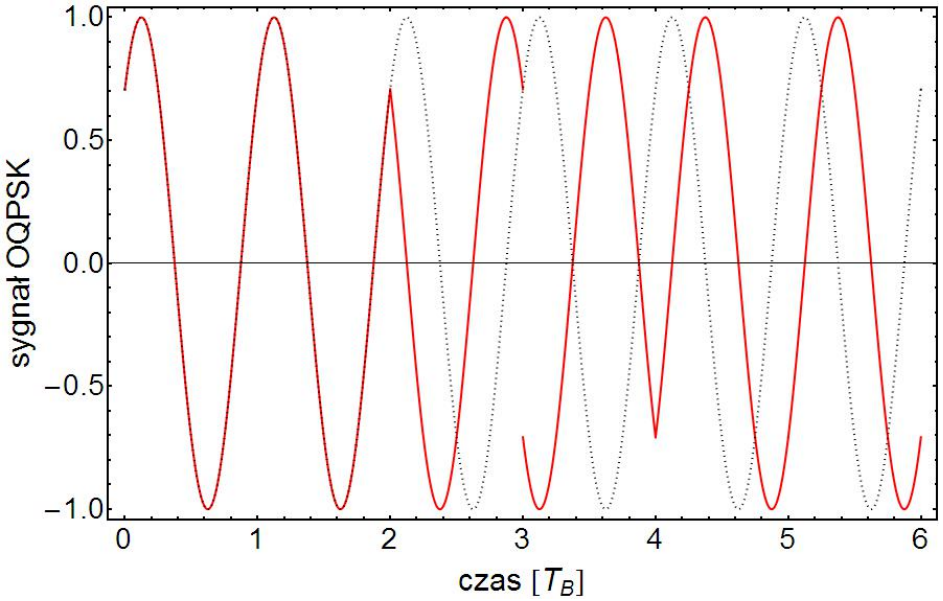
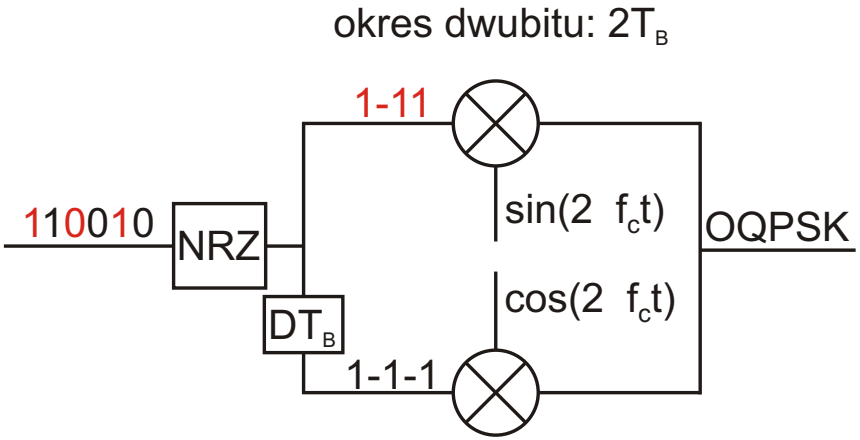
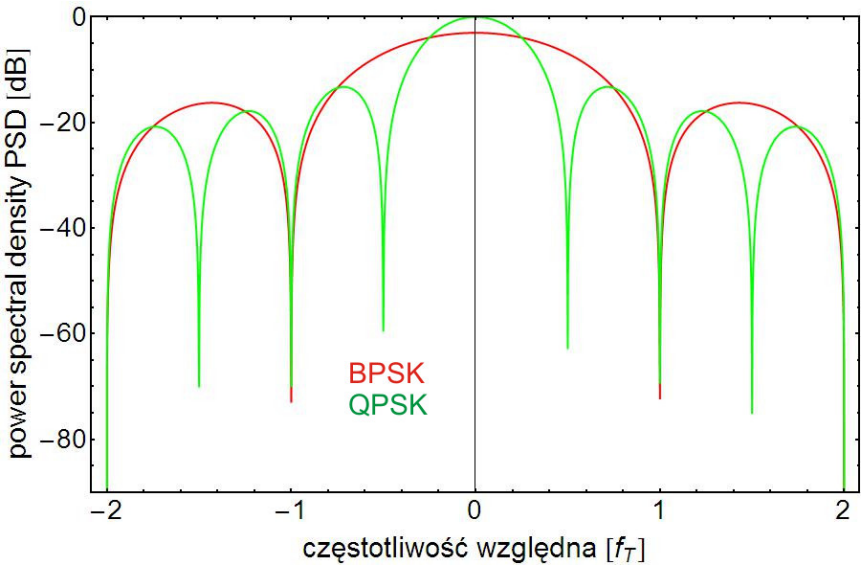


diagram konstelacyjny OQPSK





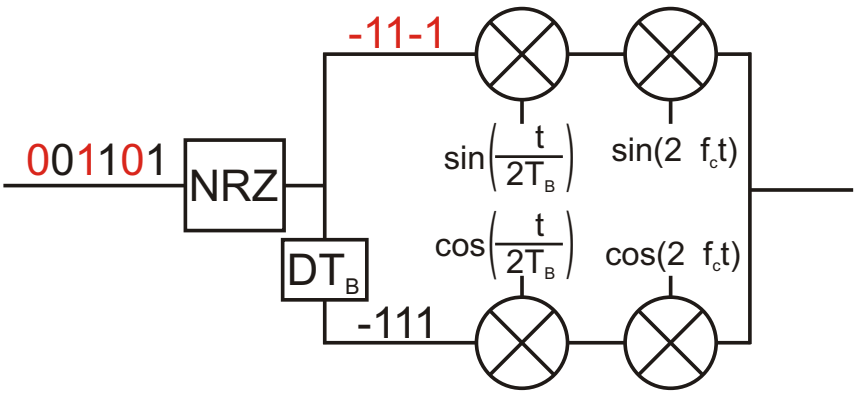


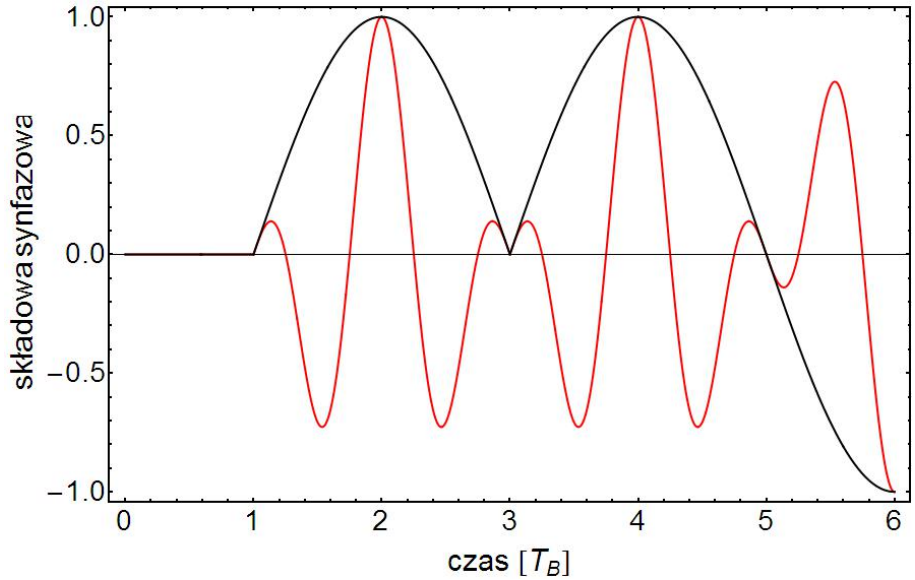
Modulacje cyfrowe — MSK

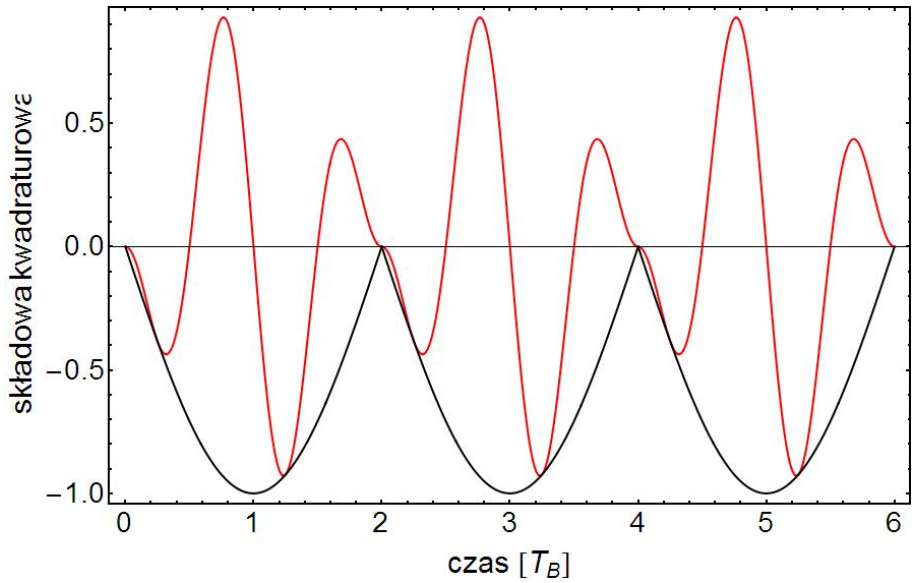
$$S_{MSK}(t) = A_0 x_S \cos\left(\frac{\pi t}{2T_B}\right)\cos(2\pi f_c t)$$

$$+A_0 x_Q \sin\left(\frac{\pi t}{2T_B}\right)\sin(2\pi f_c t)$$

$$x_S,\ x_Q = 1,\ -1$$





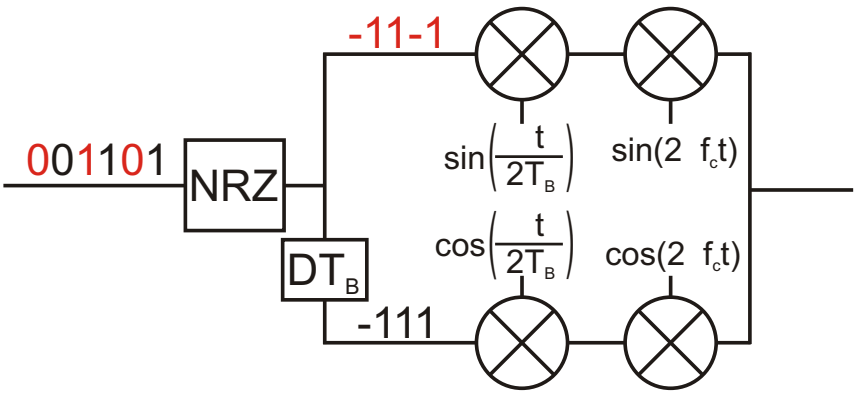


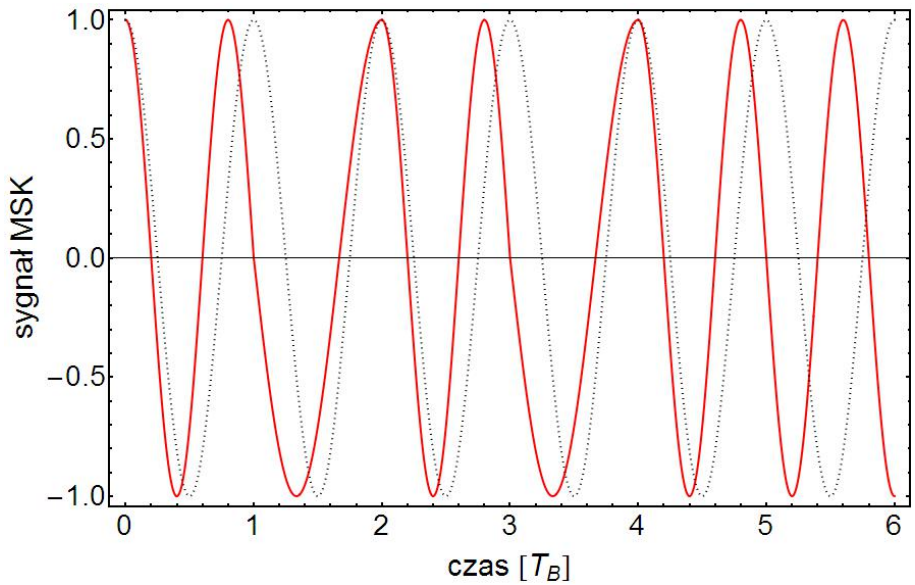
Modulacje cyfrowe — MSK

$$S_{MSK}(t) = A_0 x_S \cos\left(\frac{\pi t}{2T_B}\right)\cos(2\pi f_c t)$$

$$+A_0 x_Q \sin\left(\frac{\pi t}{2T_B}\right)\sin(2\pi f_c t)$$

$$x_S,\ x_Q = 1,\ -1$$





Modulacje cyfrowe — MSK

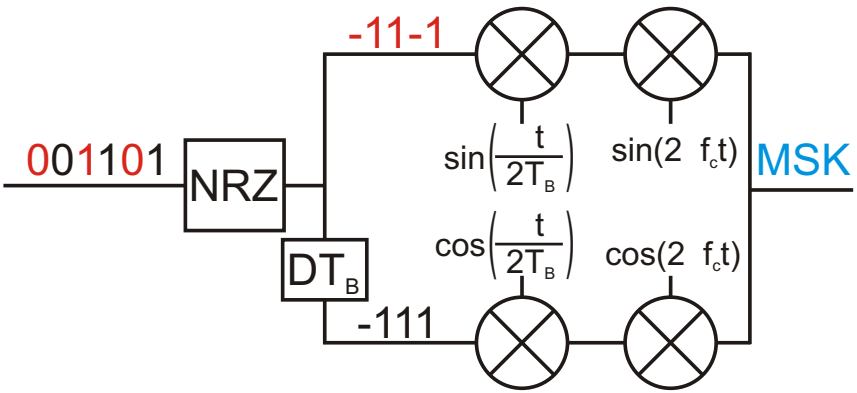
$$S_{MSK}(t) = A_0 x_S \cos\left(\frac{\pi t}{2T_B}\right)\cos(2\pi f_c t)$$

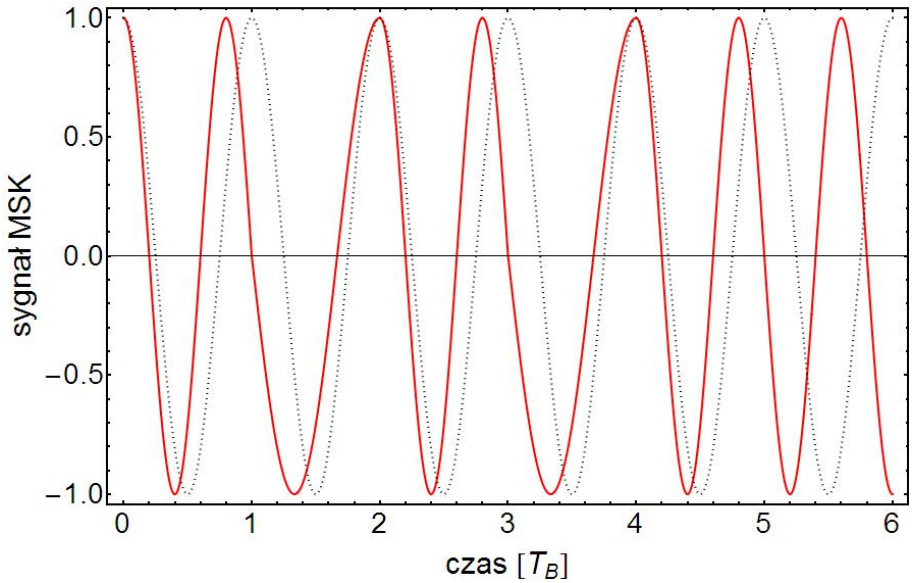
$$+A_0 x_Q \sin\left(\frac{\pi t}{2T_B}\right)\sin(2\pi f_c t)$$

$$x_S,\ x_Q = 1,\ -1$$

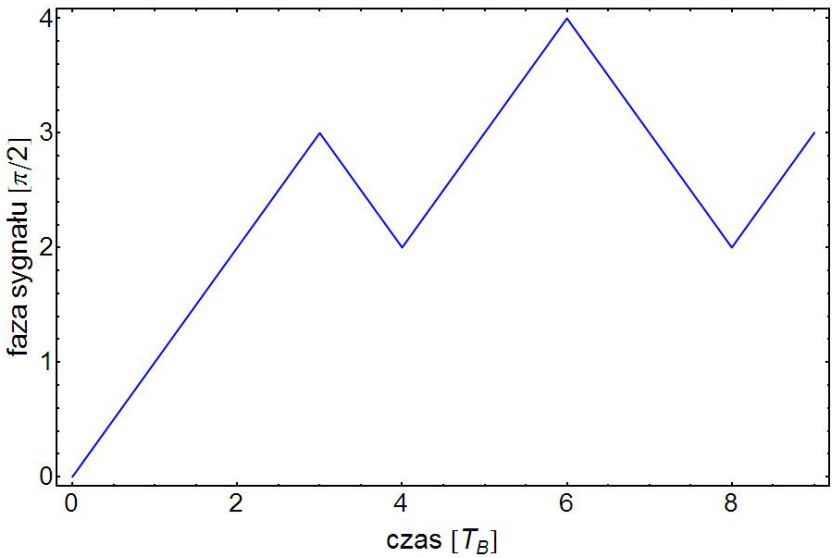
$$S_{MSK}(t) = A_0 x_S \cos\left(2\pi f_c t - \frac{x_Q}{x_S}\frac{\pi t}{2T_B}\right)$$

indeks modulacji: $h = 0.5$

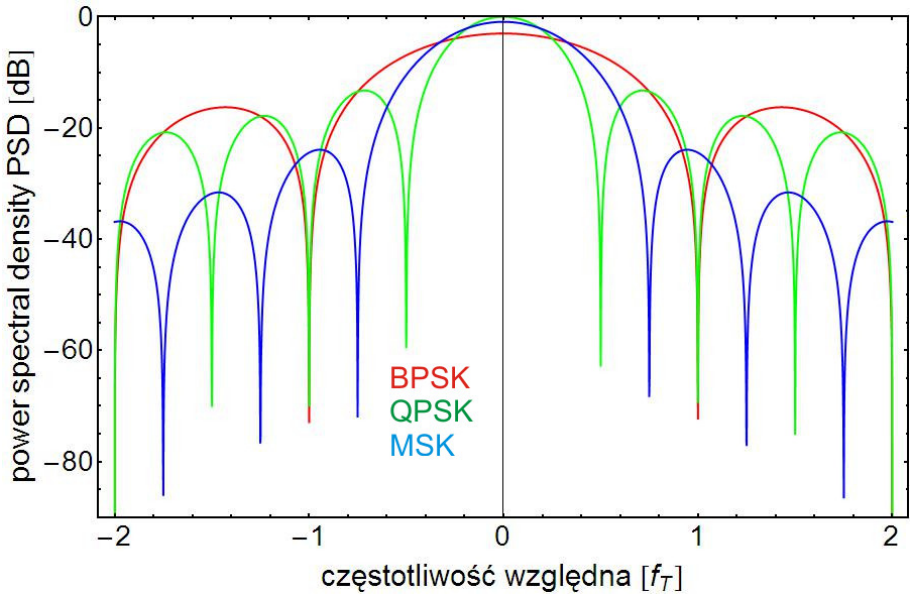




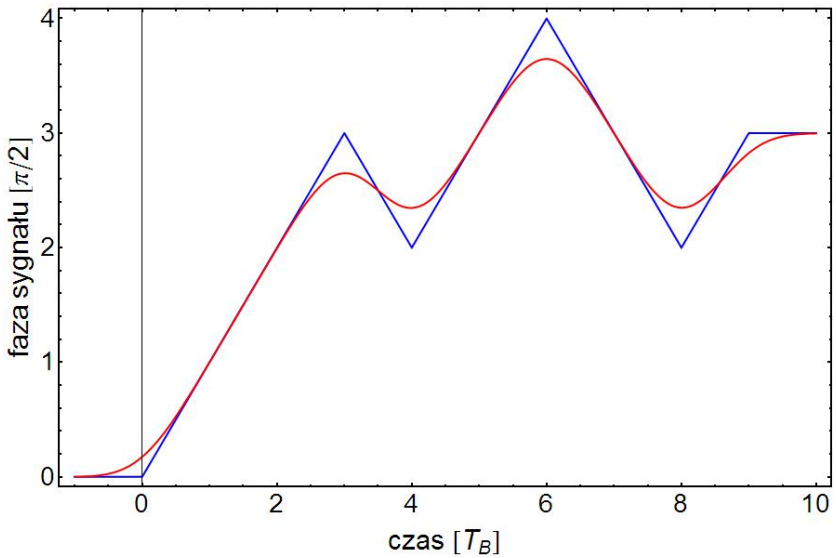
Modulacje cyfrowe — MSK i GMSK



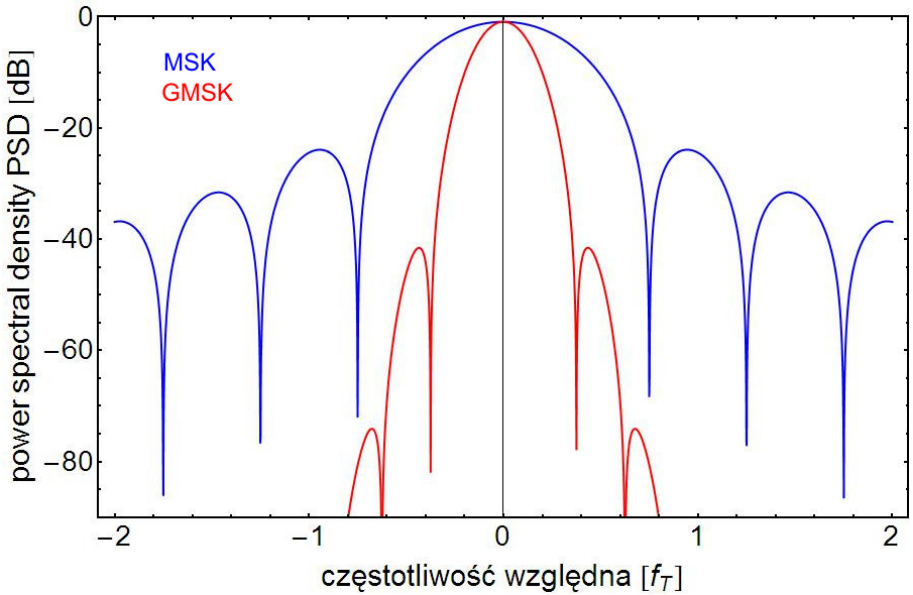
wykres kratowy fazy



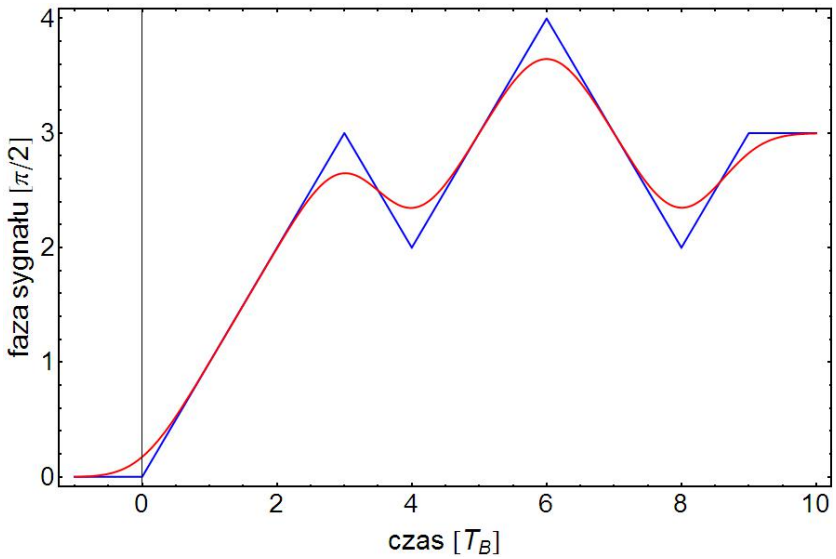
Modulacje cyfrowe — MSK i GMSK



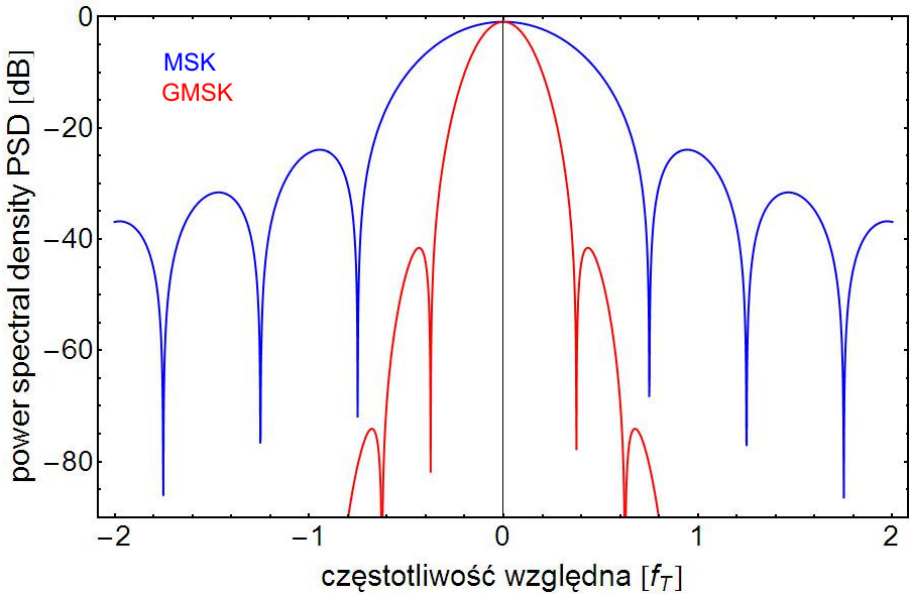
wykres kratowy fazy

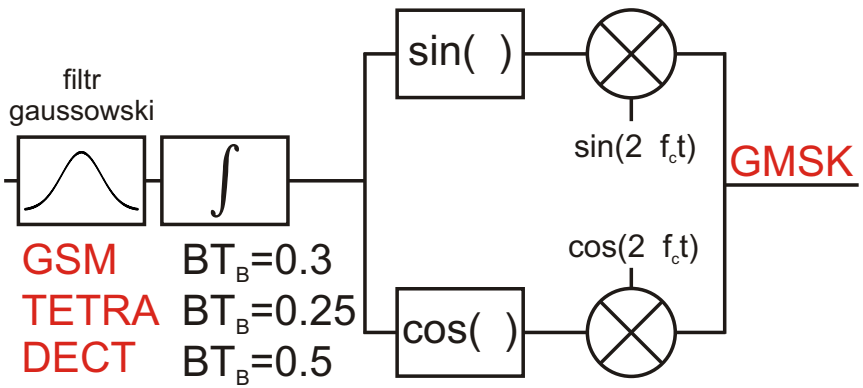


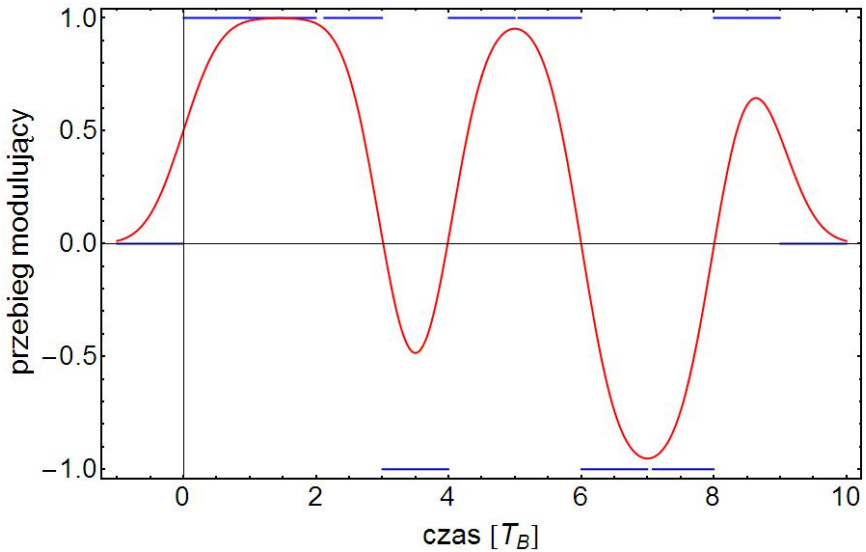
Modulacje cyfrowe — MSK i GMSK



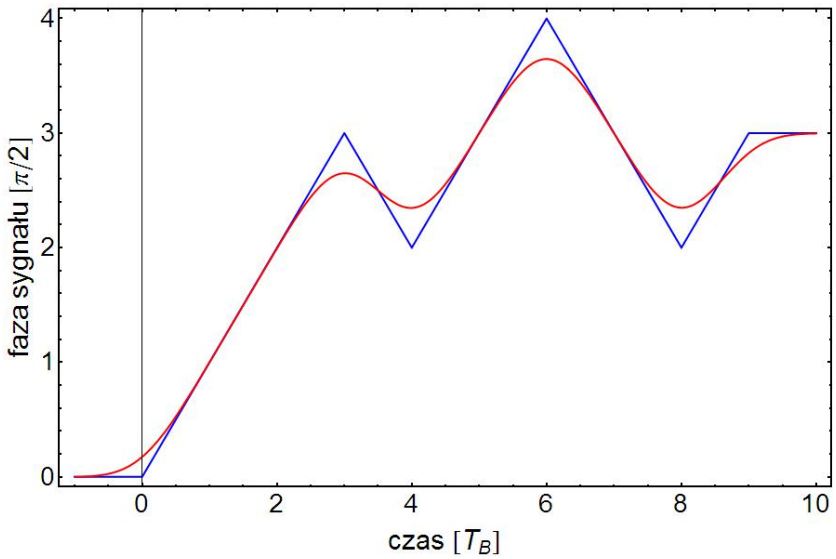
wykres kratowy fazy



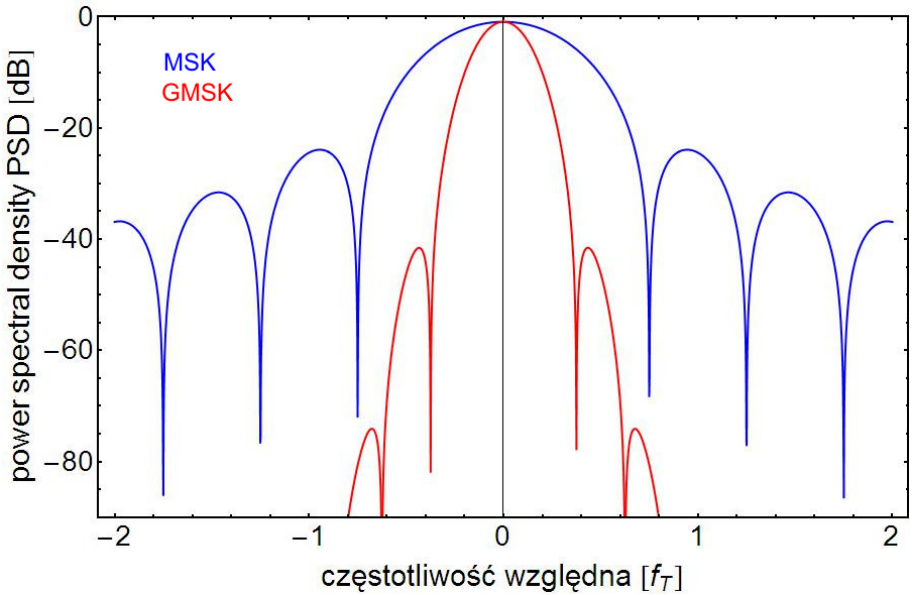


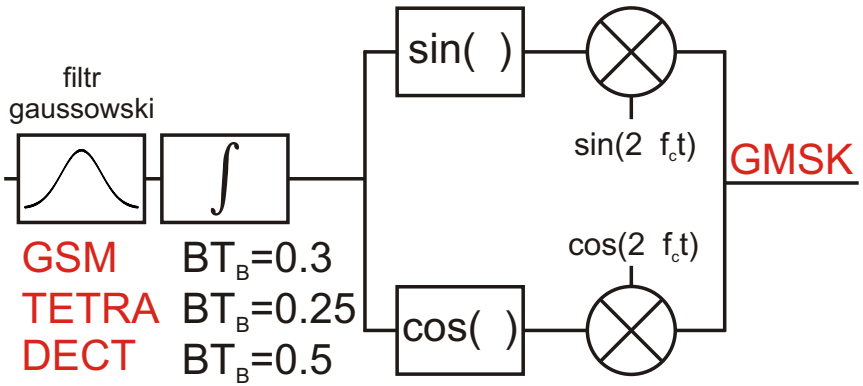


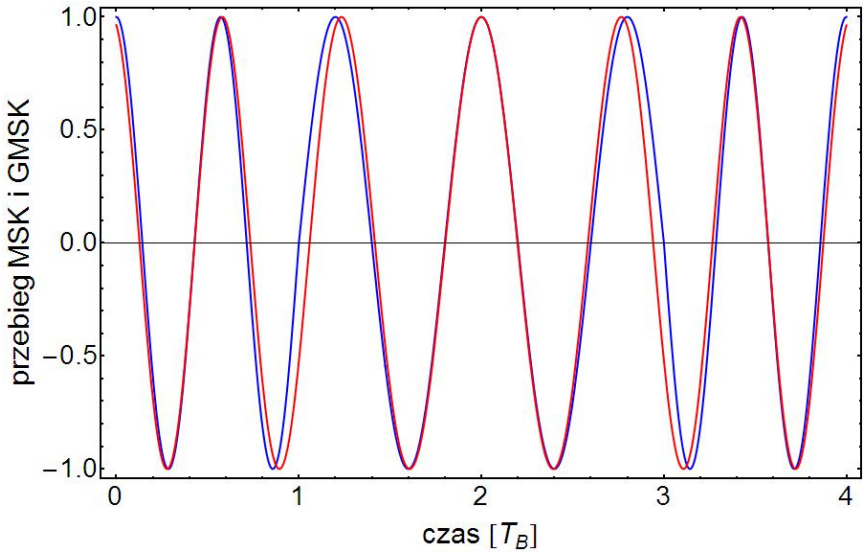
Modulacje cyfrowe — MSK i GMSK



wykres kratowy fazy

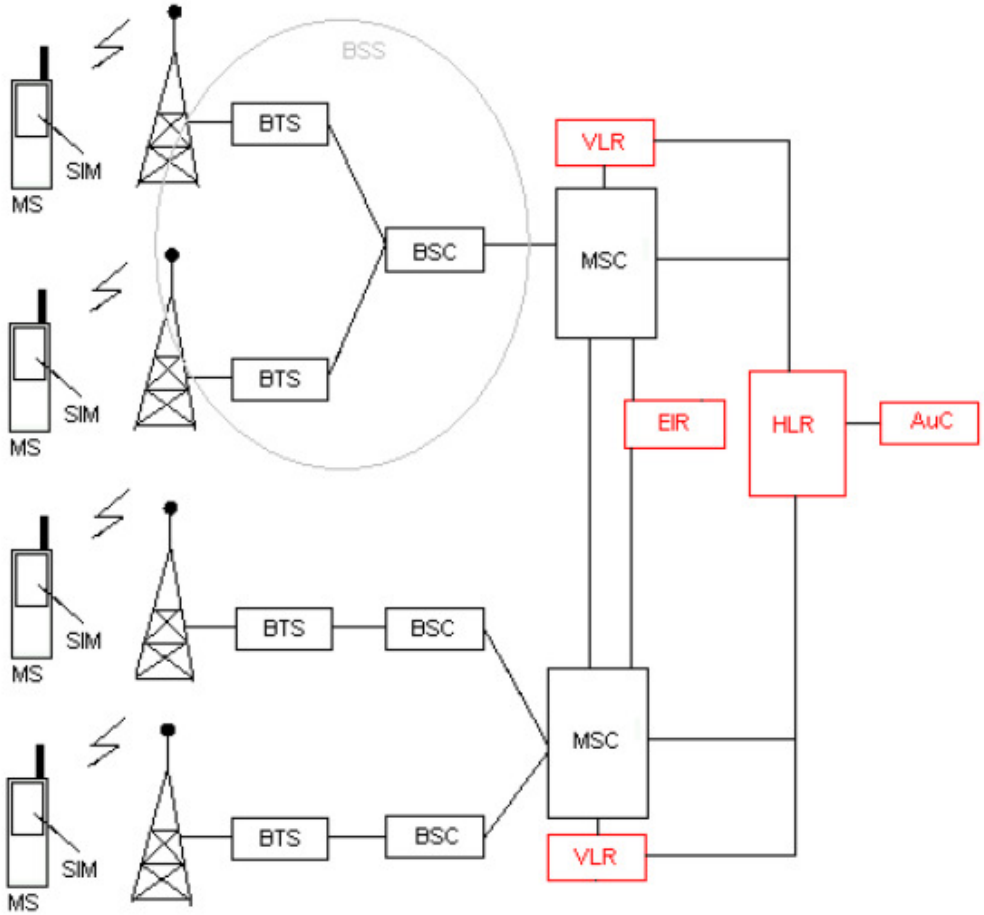






Struktura sieci GSM

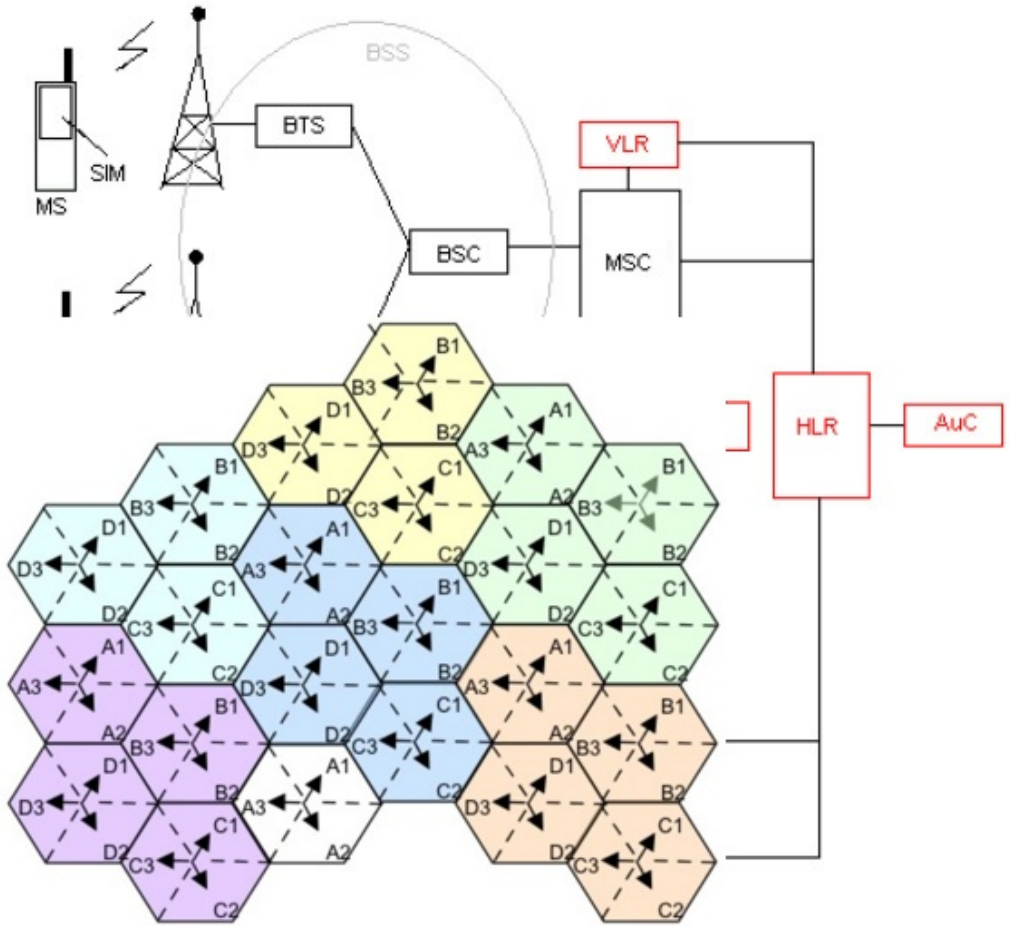
- BSC — kontroler stacji bazowych
- MSC — centrala telefoniczna
- HLR, VLR, EIR — rejestry abonentów i telefonów



Krzysztof Liszewski, Porównanie bezpieczeństwa systemów GSM i UMTS, 2007

Struktura sieci GSM

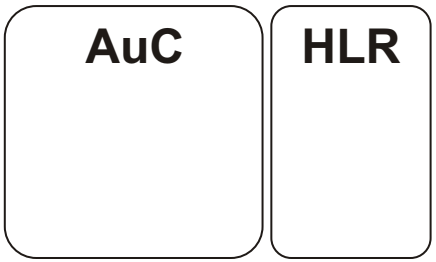
- BSC — kontroler stacji bazowych
- MSC — centrala telefoniczna
- HLR, VLR, EIR — rejestry abonentów i telefonów



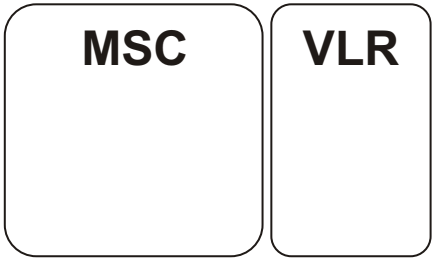
Krzysztof Liszewski, Porównanie bezpieczeństwa systemów GSM i UMTS, 2007

Karta SIM i szyfrowanie

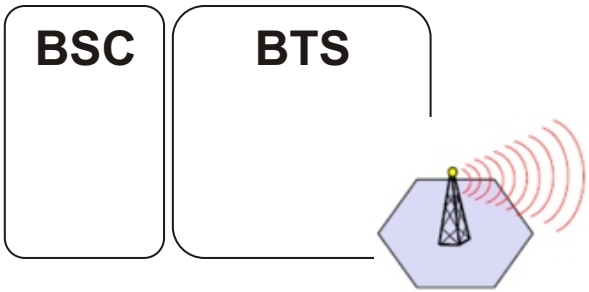
centrum autentykacji + rejestr abonentów

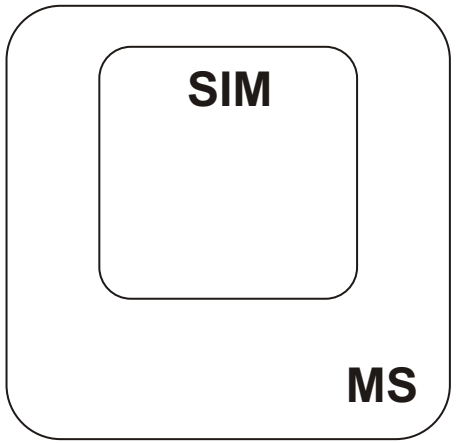


centrala +rejestr użytkowników



obsługa łącza radiowego





Karta SIM i szyfrowanie

centrum autentykacji + rejestr abonentów

AuC
A3, A8
IMSI, Ki

HLR

centrala +rejestr użytkowników

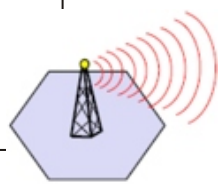
MSC

VLR

obsługa łącza radiowego

BSC

BTS
A5

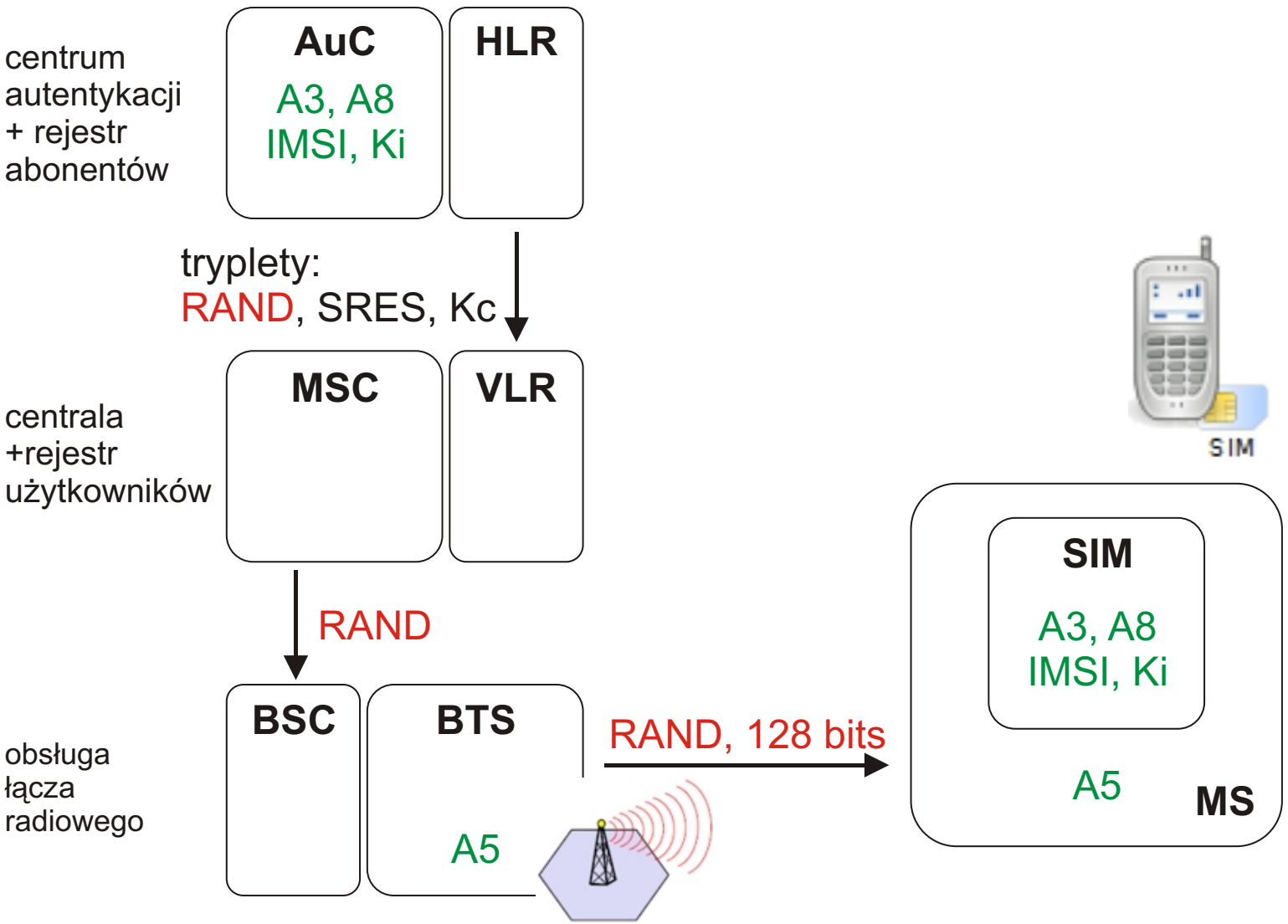


SIM
A3, A8
IMSI, Ki

A5

MS

Karta SIM i szyfrowanie

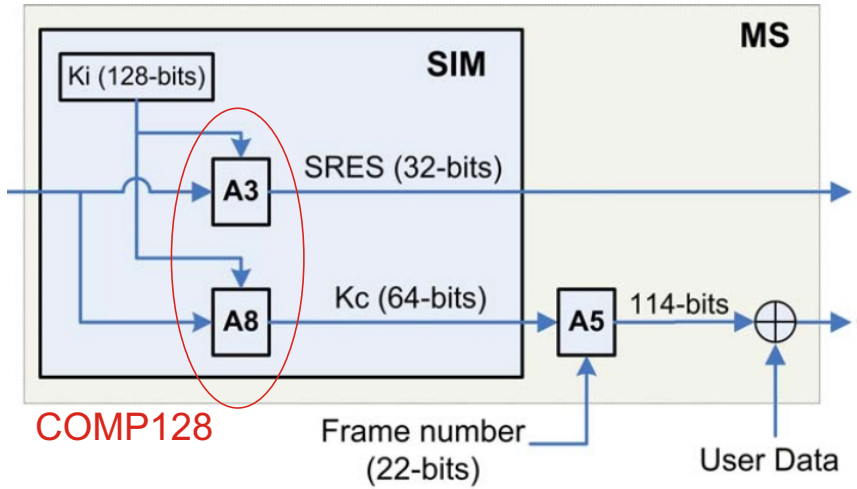


Karta SIM i szyfrowanie

centrum autentykacji + rejestr abonentów

AuC
A3, A8
IMSI, Ki

HLR



centrala +rejestr użytkowników

MSC
RAND
SRES?SRES
Kc

VLR

SRES

obsługa łącza radiowego

BSC

BTS
A5

SRES, 32 bits

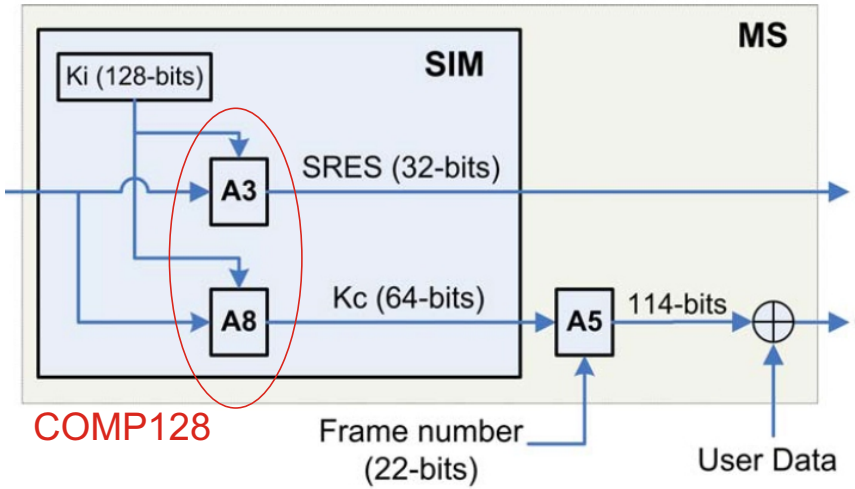
SIM
A3, A8
IMSI, Ki
A5
MS

Karta SIM i szyfrowanie

centrum autentykacji + rejestr abonentów

AuC
A3, A8
IMSI, Ki

HLR



centrala +rejestr użytkowników

MSC
RAND
SRES
Kc

VLR

połączenie nieszyfrowane

obsługa łącza radiowego

BSC

BTS
A5, Kc

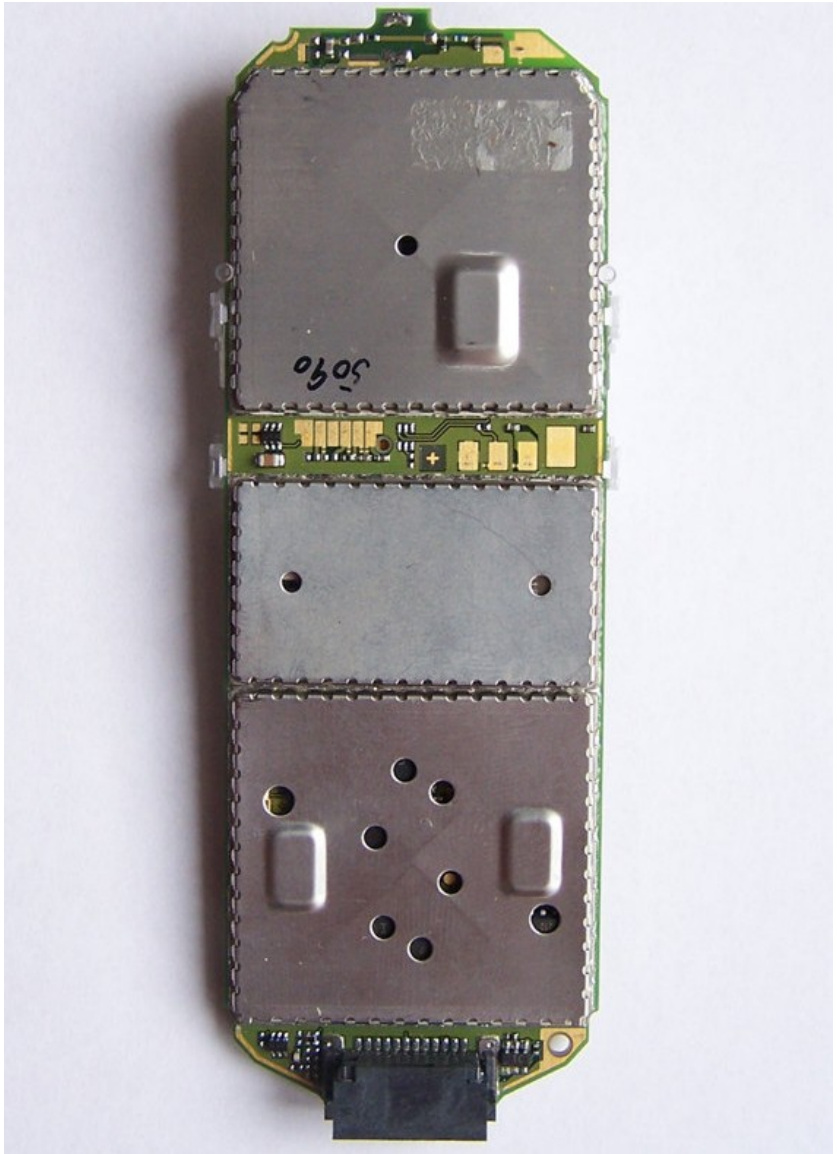
połączenie szyfrowane

SIM
A3, A8
IMSI, Ki

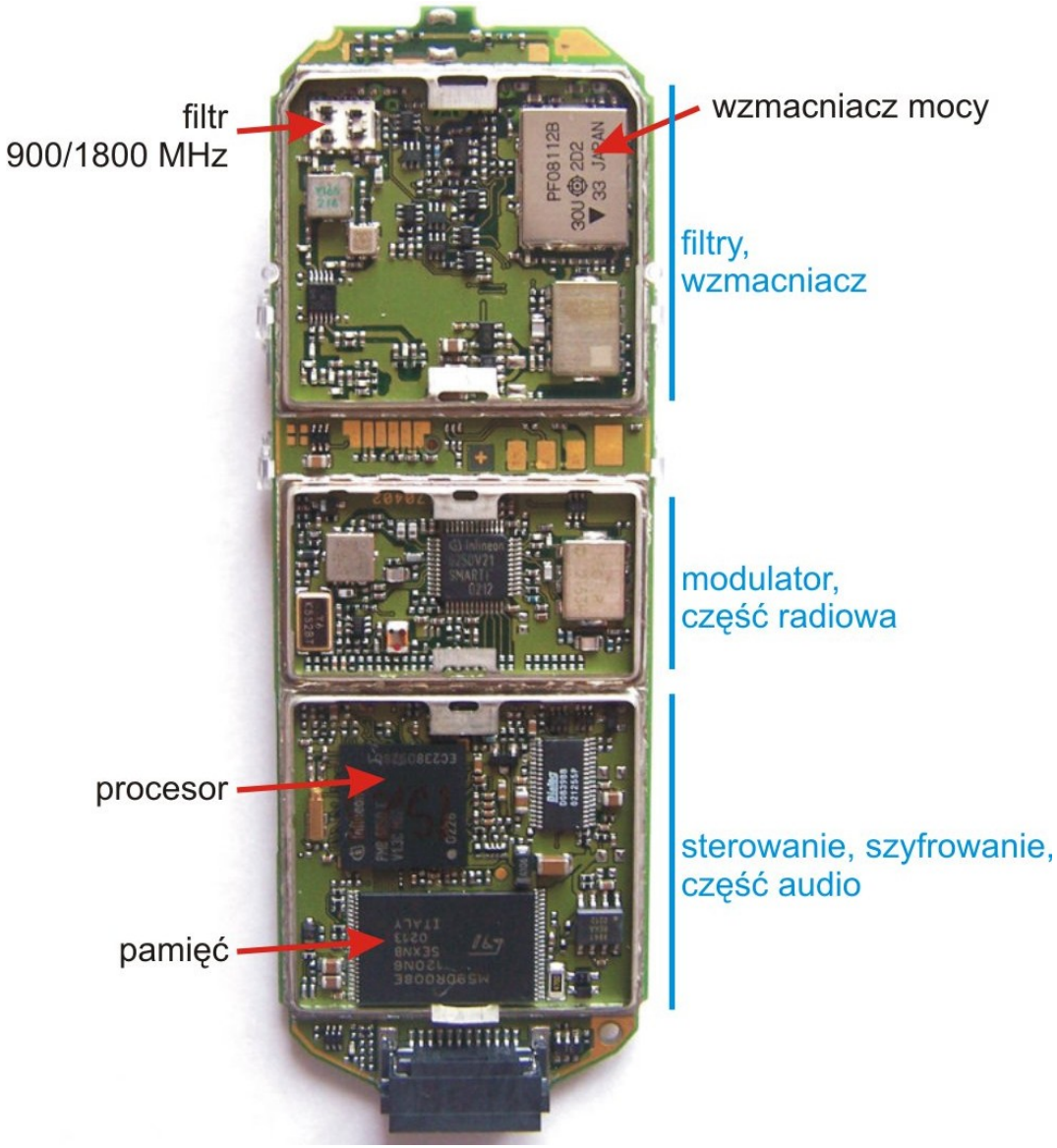
A5, Kc

MS

GSM — budowa telefonu (Siemens A36)



GSM — budowa telefonu (Siemens A36)



Bezpieczeństwo, szyfrowanie, ataki

- anonimowość — częściowo zapewniona (numery IMSI, TMSI), ale: Internet + analiza ruchu w sieci komórkowej
- autentyczność — autentykacja telefonu, ale brak kontroli autentyczności sieci przez telefon
- poufność — szyfrowanie rozmów i SMSów, trudności techniczne podsłuchu (np. frequency hopping, TDMA)
- integralność danych

Bezpieczeństwo, szyfrowanie, ataki

- anonimowość — częściowo zapewniona (numery IMSI, TMSI), ale: Internet + analiza ruchu w sieci komórkowej
- autentyczność — autentykacja telefonu, ale brak kontroli autentyczności sieci przez telefon
- poufność — szyfrowanie rozmów i SMSów, trudności techniczne podsłuchu (np. frequency hopping, TDMA)
- integralność danych — brak...

Bezpieczeństwo, szyfrowanie, ataki

- anonimowość — częściowo zapewniona (numery IMSI, TMSI), ale: Internet + analiza ruchu w sieci komórkowej
- autentyczność — autentykacja telefonu, ale brak kontroli autentyczności sieci przez telefon
- poufność — szyfrowanie rozmów i SMSów, trudności techniczne podsłuchu (np. frequency hopping, TDMA)
- integralność danych — brak...

Błędy protokołów:

- używanie tego samego klucza sesyjnego Kc do kilku rozmów oraz w różnych algorytmach szyfrujących
- używanie zbyt słabego algorytmu szyfrującego A5/1, a wcześniej bardzo słabego A5/2 lub brak szyfrowania A5/0
- zbyt słaby algorytm A3/A8 w karcie SIM (poprawione)
- szyfrowanie transmisji po dodaniu bitów nadmiarowych
- *security by obscurity*
- brak szyfrowania numeru ramki

Ataki na A3/A8 (COMP128)

- 1997 — wyciek fragmentów notatek
- 1998 — uzupełnienie kodu i podanie ataku (2^{17} RANDs), Goldberg, Wagner (Berkeley)
- możliwe poznanie klucza Ki, także bez fizycznego dostępu do karty
- ulepszenie ataków, ale też wprowadzenie poprawek do COMP128

Ataki na A5

- 1999 — inżynieria wsteczna z telefonu i ujawnienie algorytmu
- po 2000 — realne propozycje ataków na A5/1 (bez dużych ilości tekstu jawnego)
- 2003 — złamanie A5/2 w czasie rzeczywistym, tylko z szyfrogramem
- 2003–2010 — ataki *time memory tradeoff* na A5/1, tablice tęczowe
- 2010 — gotowy kompletny przepis na atak na A5/1 oraz rozwiązanie komercyjne

Ataki na A5

- 1999 — inżynieria wsteczna z telefonu i ujawnienie algorytmu
- po 2000 — realne propozycje ataków na A5/1 (bez dużych ilości tekstu jawnego)
- 2003 — złamanie A5/2 w czasie rzeczywistym, tylko z szyfrogramem
- 2003–2010 — ataki *time memory tradeoff* na A5/1, tablice tęczowe
- 2010 — gotowy kompletny przepis na atak na A5/1 oraz rozwiązanie komercyjne

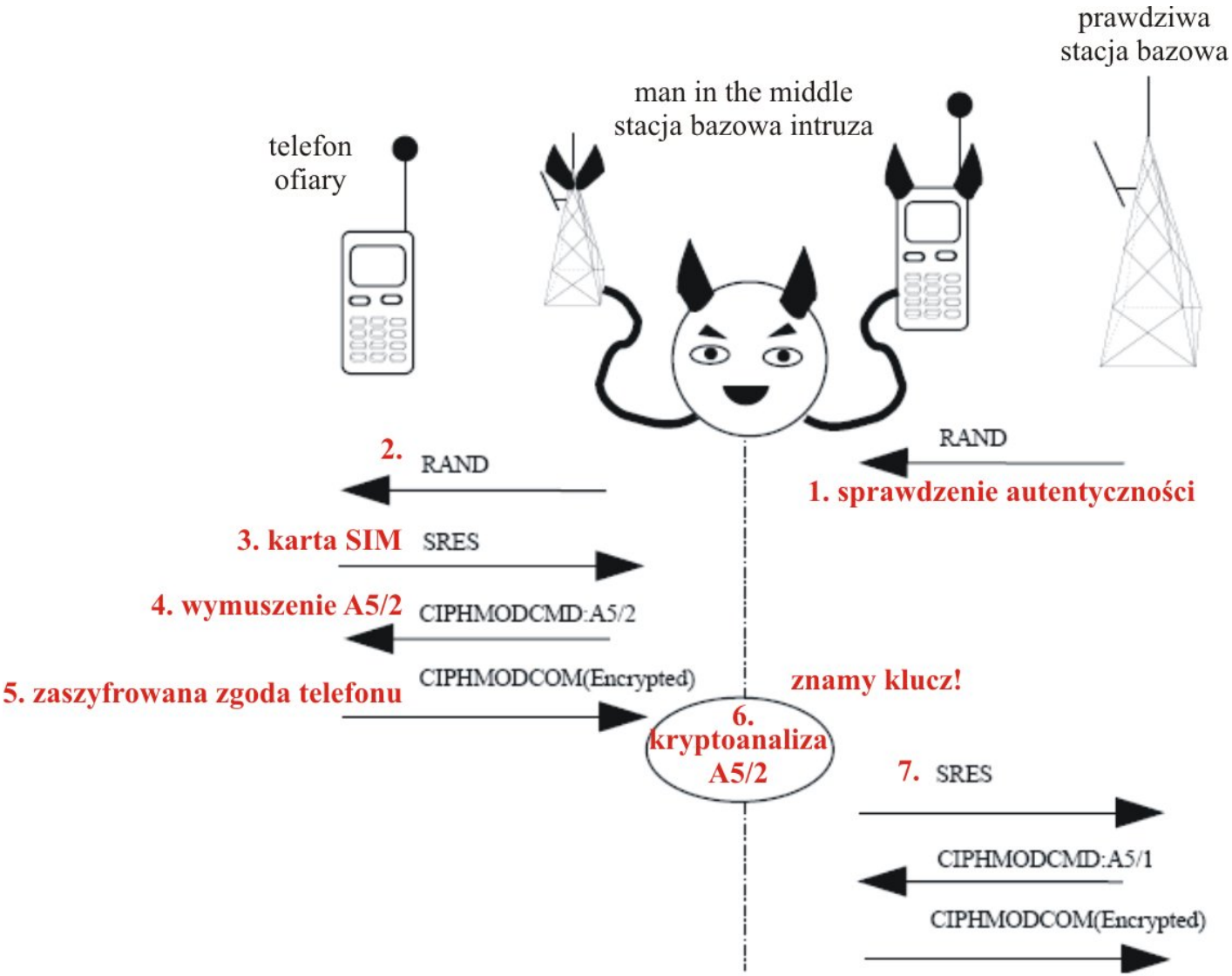
$\Rightarrow$ potencjalna możliwość:

- podsłuchiwania rozmów i przechwytywania SMSów
- fałszowania rozmów i SMSów oraz rozmów na czyjś koszt

Rodzaje ataków:

- pasywne — tylko podsłuch
- aktywne — podsłuch i nadawanie (udawanie stacji bazowej)

Przykładowy scenariusz ataku...



Journal of Cryptology, **21**, 392 (2008)

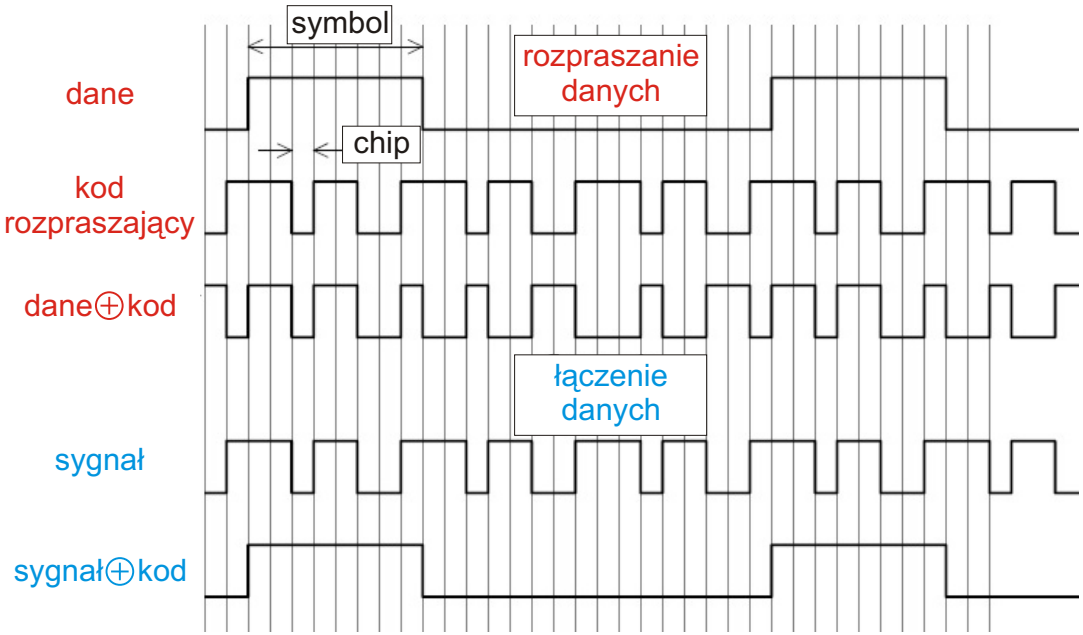
Rozwiązanie komercyjne — 2010

- podsłuch aktywny i pasywny
- A5/1 i A5/2 w czasie rzeczywistym

Meganet Corporation, USA

System 3G UMTS — Universal Mobile Telecommunications System

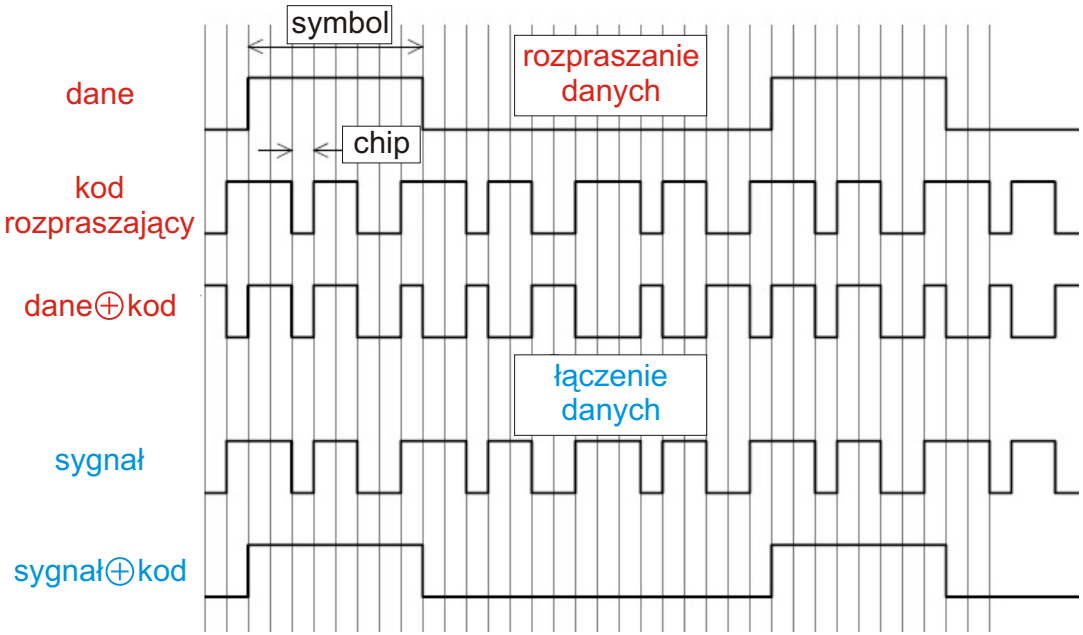
- wielodostęp dzięki (W)CDMA — (Wideband) Code Division Multiple Access
- rozpraszanie widma sygnału do prawie 5 MHz przez tzw. ciągi ortogonalne
- rozpoznawanie transmisji z różnych telefonów dzięki ciągom skramblującym
- transmisje wielu telefonów — w tym samym kanale jednocześnie
- odporność na zakłócenia, sąsiednie Node B mogą współdzielić częstotliwość
- konieczna budowa nowej infrastruktury radiowej względem BTS GSM



Ryszard Witkowski, Telefonia komórkowa UMTS, analiza transmisji i modulacji sygnałów, 2006

System 3G UMTS — Universal Mobile Telecommunications System

- wielodostęp dzięki (W)CDMA — (Wideband) Code Division Multiple Access
- rozpraszanie widma sygnału do prawie 5 MHz przez tzw. ciągi ortogonalne
- rozpoznawanie transmisji z różnych telefonów dzięki ciągom skramblującym
- transmisje wielu telefonów — w tym samym kanale jednocześnie
- odporność na zakłócenia, sąsiednie Node B mogą współdzielić częstotliwość
- konieczna budowa nowej infrastruktury radiowej względem BTS GSM
- większe bezpieczeństwo — weryfikacja sieci, lepsze algorytmy szyfrujące, ale nadal problemy, np. w dla współpracujących sieci GSM i UMTS



Ryszard Witkowski, Telefonia komórkowa UMTS, analiza transmisji i modulacji sygnałów, 2006