



# GSM

## Global System for Mobile Communication

April 2001 Patrick Röder

# Überblick

- ◆ Geschichte der GSM Entwicklung
- ◆ Technische Grundlagen
- ◆ Funk und Zellulartechnik
- ◆ Netzorganisation
- ◆ Logische und physikalische Kanäle
- ◆ Authentifizierung, Kompression, Codierung, Verschlüsselung

# Geschichte der GSM Entwicklung

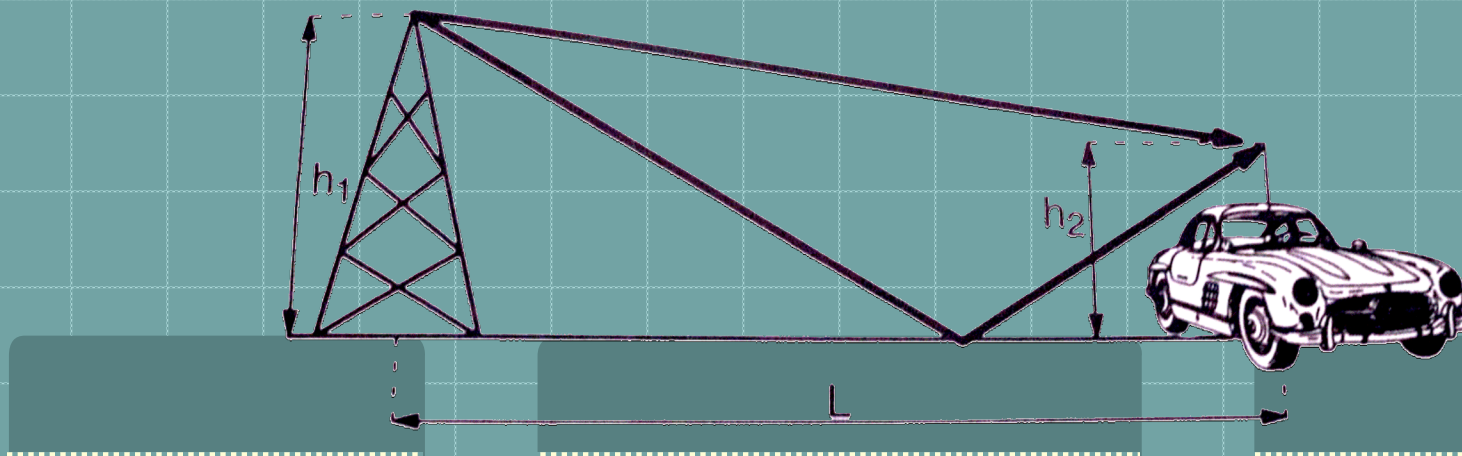
- ◆ 1982 Groupe Spécial Mobile gegründet
- ◆ 1987 Funktechnik festgelegt
- ◆ 1989 GSM Teil der ETSI (European Telecommunication Standards Institute)
- ◆ 1991 Erste GSM900-Netze (D-Netze) in Betrieb
- ◆ DCS1800 (E-Netze) Specs festgelegt
- ◆ 1994 Datendienste werden angeboten
- ◆ 1995 Erste PCS1900-Netz in USA geht in Betrieb
- ◆ Heute ?

# Technische Grundlagen

## Funkwellenausbreitung

Idealfall:  $P_{\text{ef}} \sim 1 / L^2$

- Realität:  $P_{\text{ef}} \sim 1 / L^\mu$  ( $2 \leq \mu \leq 5$ )
  - Ausbreitungskoeffizient  $\mu$
  - Bedingt durch Hindernisse und *Mehrwegeausbreitung*





# Technische Grundlagen

- ◆ Fading (Signaldämpfung)
  - ◆ Fast Fading (Durch Mehrwegeausbreitung)
  - ◆ Slow Fading (Durch Hindernisse)
- ◆ Typisch im periodischen Abstand etwa einer halben Wellenlänge
  - ◆ Frequenzselektives Fading
- ◆ Stärkstes Signal der Mehrwegeausbreitung: Rice-Kanal ( Rice-Fading)
- ◆ Alle Signal gleich stark gedämpft: Rayleigh-Fading

# Technische Grundlagen

## Fazit

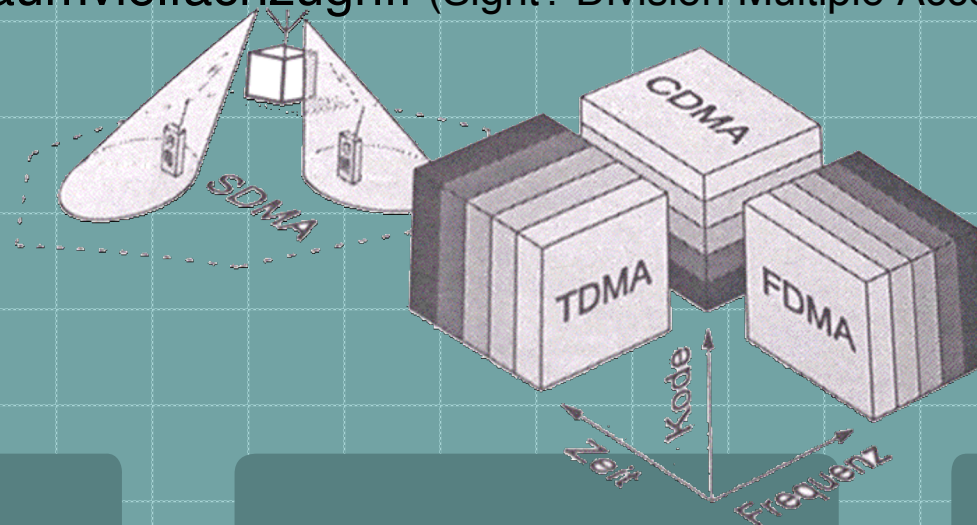
- ◆ Mobilfunkkanal schlechtes Medium
- ◆ Teilweise tiefe Fadinglöcher mit typischen Bitfehlerraten von 1% bis 10% ( $10^{-2}$  bis  $10^{-1}$ )
- ◆ Aufwändige Maßnahmen gegen Mehrfachausbreitung:
  - Equalizer* wird mit Trainingssequenzen trainiert und trennt damit *Rice-Kanal* von störendem Rest
  - Vorwärtsfehlerkorrektur mit fehlerkorrigierenden Codes
    - Fehlerrate kann dadurch auf etwa  $10^{-5}$  bis  $10^{-6}$  reduziert werden
  - Algorithmen zur Sendleistungsregelung

# Duplexübertragung

- ◆ Frequency Division Duplex **FDD**
  - ◆ Je eine Frequenz für uplink und downlink
  - ◆ Im analogen Mobilfunk eingesetzt, braucht große Hardwarefilter zur Frequenztrennung
- ◆ Time Division Duplex **TDD**
  - ◆ Abwechselnd senden und empfangen
  - ◆ In GSM verwendet, braucht keine Filter
  - ◆ Max. mögliche Bitrate dadurch halbiert

# Vielfachzugriffstechniken

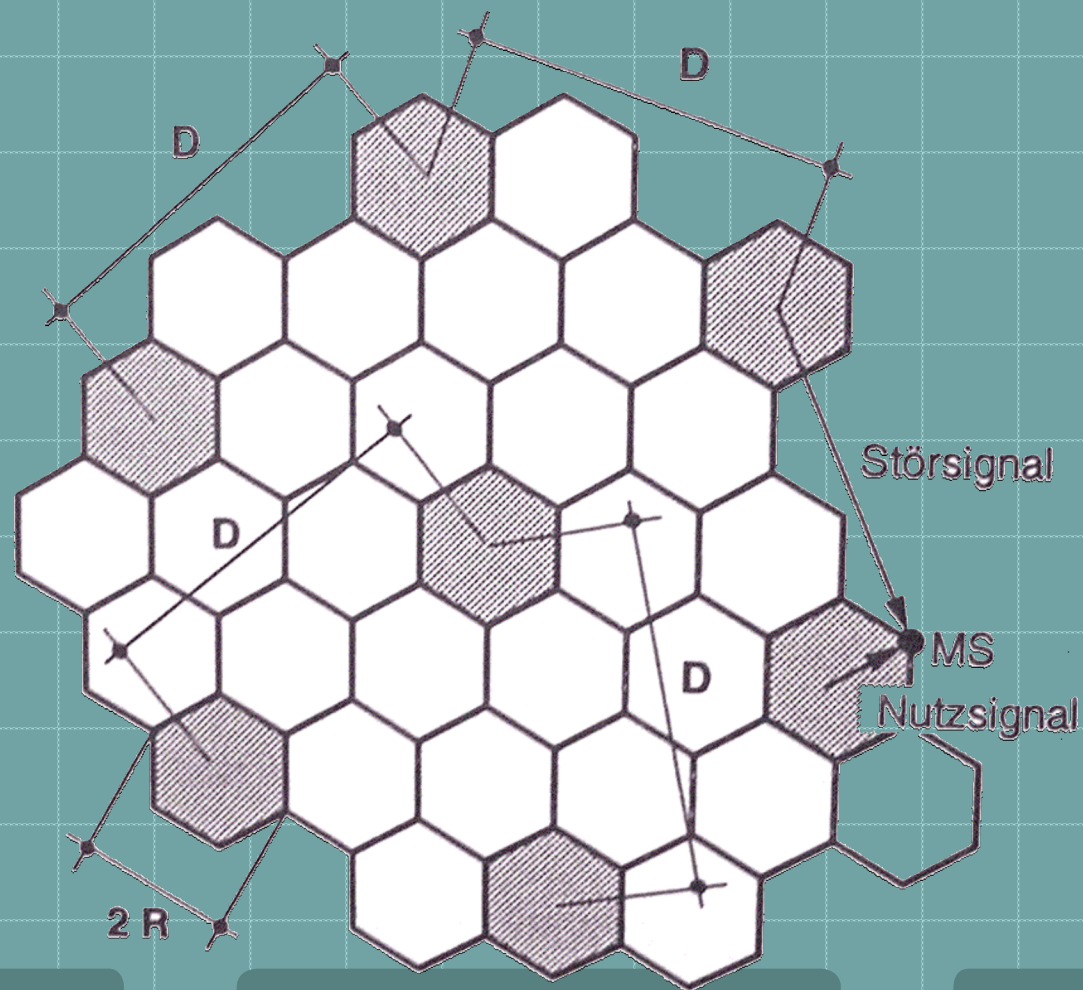
- ◆ Funkmedium knapp, effiziente Nutzung sehr wichtig
- 1. Frequenzmehrfachzugriff (Frequency Division Multiple Access **FDMA**)
- 2. Zeitvielfachzugriff (Time Division Multiple Access **TDMA**)
- 3. Codevielfachzugriff (Code Division Multiple Access **CDMA**)
- 4. Raumvielfachzugriff (Space Division Multiple Access **SDMA**)



# Zellulartechnik

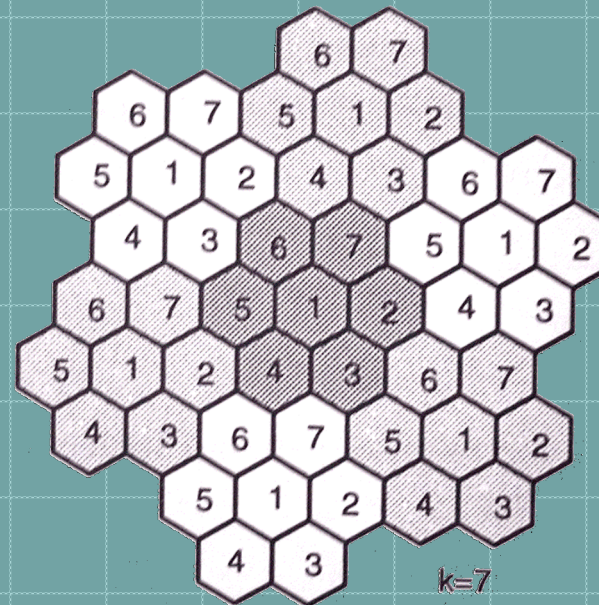
- ◆ GSM 900 nur 25 MHz Bandbreite
- ◆ 125 Kanäle á 200 kHz mit je 8 Timeslots (TDMA)
- ◆ = 1000 Sprachkanäle -> zu wenig für alle in der BRD
- ◆ Netz in Zellen aufteilen
- ◆ Jede Zelle erhält eigene Frequenzmenge
- ◆ Im Abstand **D** (Frequenzwiederholabstand) Frequenzen wieder benutzen
- ◆ Beim Übergang von eine Zelle zur nächsten während eines Gesprächs erfolgt *Handover*, d. h. automatischer Frequenzwechsel auf (freie) Frequenz der nächsten Zelle

# Zellulares Netz



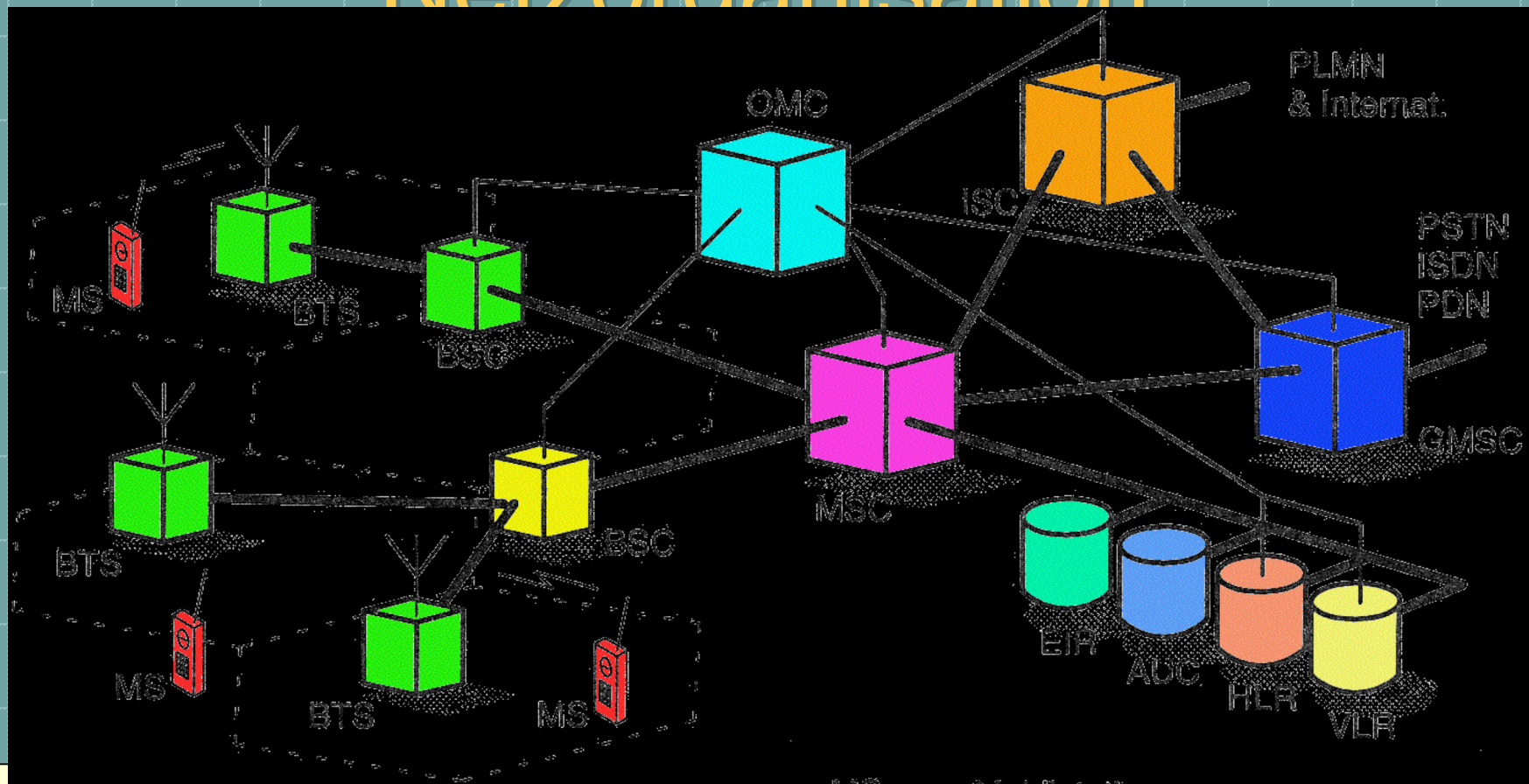
# Clusterbildung

- ◆ Gruppenbildung durch Frequenzzuteilung -> Cluster
- ◆ Im Cluster kommen alle Frequenzen vor
- ◆ Je größer ein Cluster ( $k$  groß), desto größer der Frequenzwiederholabstand  $D$





# Netzorganisation



BTS Base Transceiving Station  
 BSC Base Station Controller  
 MSC Mobile Switching Center  
 GMSC Gateway MSC  
 ISC International Switching Center

MS Mobilisation  
 HLR Home Location Register  
 VLR Visited Location Register  
 EIR Equipment Identity Register  
 AUC Authentication Center  
 OMC Operation and Maintenance Center



# Identifikation

- ◆ Country Code **CC** (3 Dezimalstellen)
  - ◆ Internat. eindeutiger Code für ein Land (BRD=262)
- ◆ Mobile Network Code **NC** (2 Dezimalstellen)
  - ◆ Code für das Netz (01 = D1; 02 = D2; 03 = E+; 07 = Viag)
- ◆ International Mobile Station Equipment Identity **IMEI** (15 Dez.-Stellen)
  - ◆ Geräte ID im Handy und im EIR gespeichert
  - ◆ Betreiber führen White- / Grey- und Black-List
- ◆ International Mobile Subscriber Identity **IMSI** (15 Dez.-Stellen)
  - ◆ Teilnehmer ID im SIM gespeichert
  - ◆ Enthält u. a. NC und CC
- ◆ Location Area Code (16 Bit)
  - ◆ ID des Aufenthaltsbereich im Netz
  - ◆ Wird im Broadcast Control Channel jeder BTS regelmäßig gesendet
  - ◆ Wechsel der LAC muß das Handy ein Location Update machen

# Identifikation

- ◆ Cell ID **CID** (max. 16 Bit)
  - ◆ ID einer Zelle zusammen mit LAC national eindeutig
- ◆ Bases Station Identity Code **BSIC**
  - ◆ ID eine BTS
  - ◆ Auf Broadcast und Synchronisation Channel gesendet

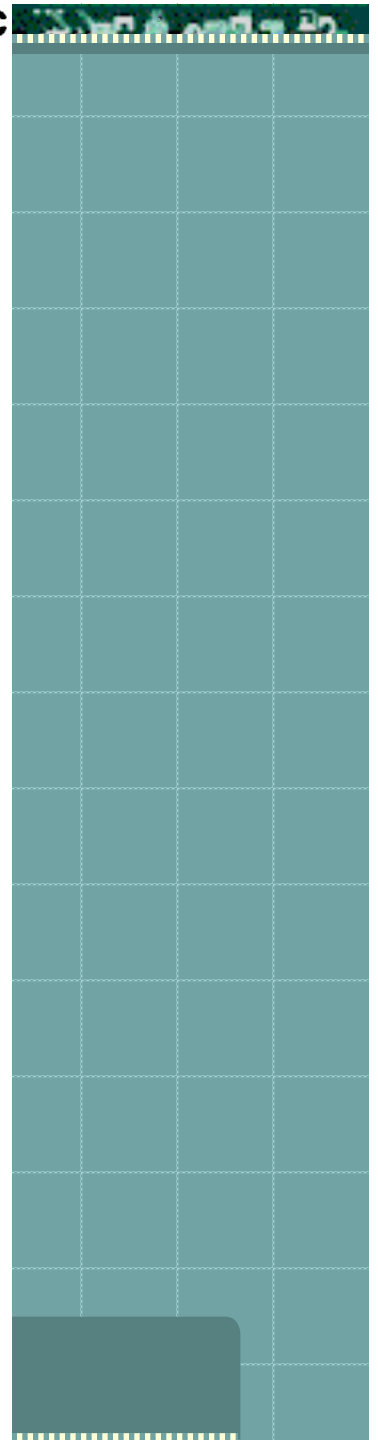
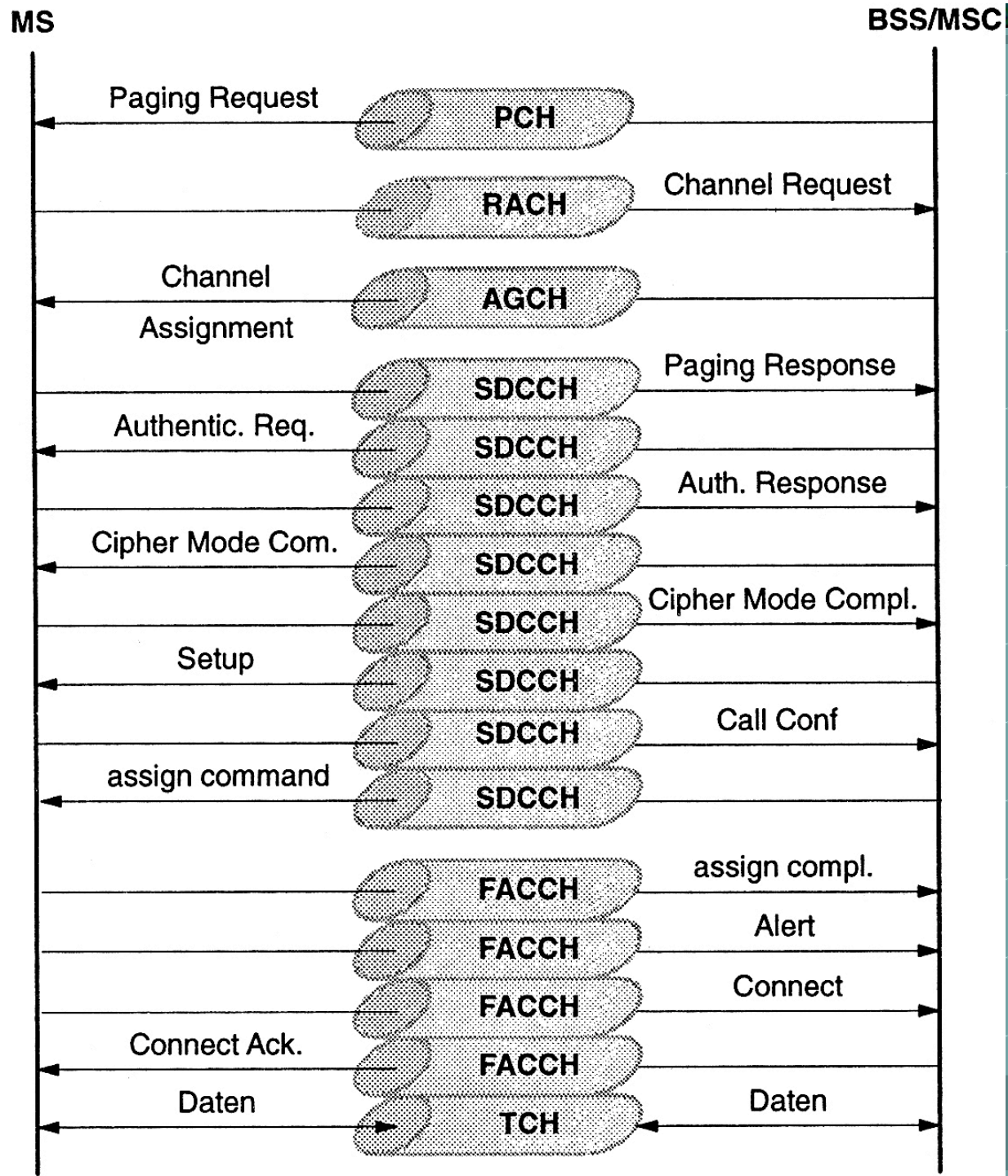
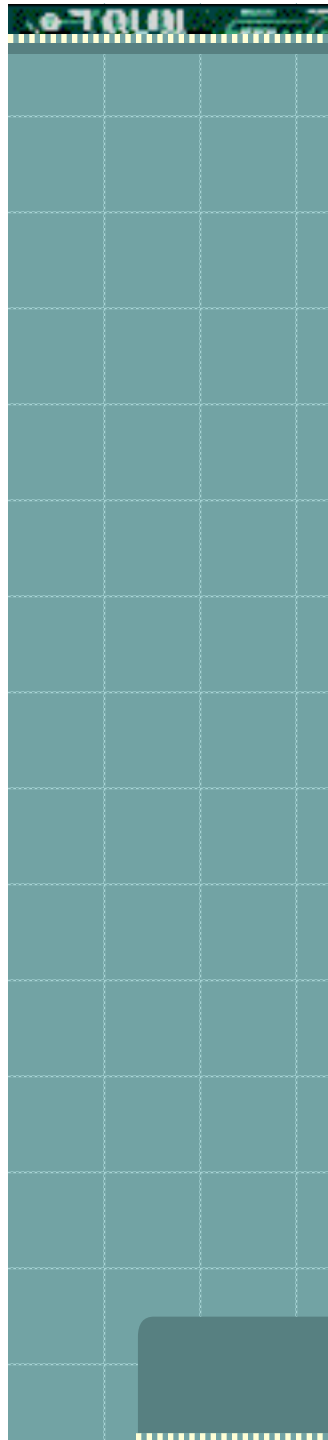
# Logische Kanäle

- ◆ **Traffic Channel TCH**
  - ◆ Für Sprache, Fax oder Daten
  - ◆ mobiler B-Kanal
  - ◆ Half Rate (halber Kanal)
  - ◆ Full Rate (Voller Kanal)
  - ◆ Enhanced Full Rate (besserer Codec)
  - ◆ Daten mit 2.4, 4.8, 9.6, und 14.4 kbit/s

# Logische Kanäle

- ◆ Signalisierungskanäle (mobiler D-Kanal)
  - ◆ Broadcast Channel
    - ◆ Broadcast Control Channel **BCCH** (Verwaltungsdaten)
    - ◆ Frequency Correction Channel **FCCH**
    - ◆ Synchronization Channel **SCH**
  - ◆ Common Control Channel **CCCH**
    - ◆ Random Access Channel **RACH**
    - ◆ Access Grant Channel **AGCH**
    - ◆ Paging Channel **PCH**
  - ◆ Dedicated/Associated Control Channel DCCH/ACCH
    - ◆ Stand-alone Dedicated Control Channel **SDCCH**
    - ◆ Fast/Slow Associated Control Channel **SACCH/FACCH**

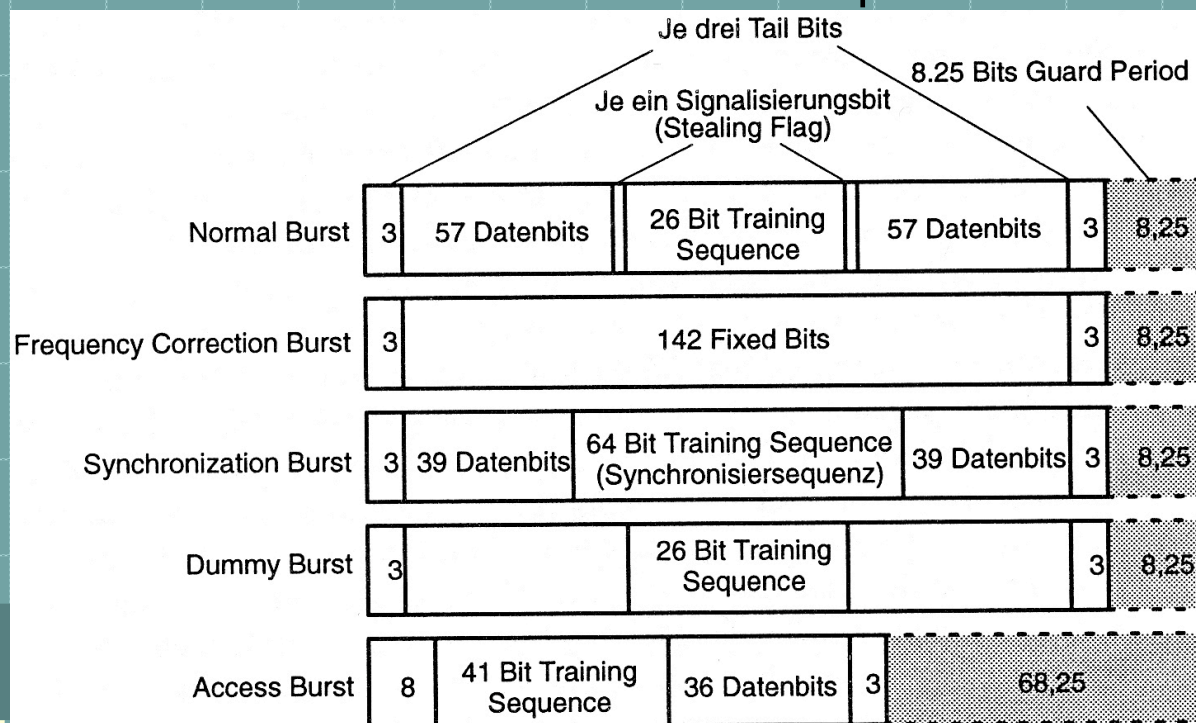
Kanaltyp	Nettodaten- rate [kbit/s]	Block- länge [Bit]	Blockabstand [ms]
TCH (Full-Rate Sprache)	13.0	182+78	20
TCH (Half-Rate Sprache)	wird standardi- siert	wird stan- dardisiert	wird standardi- siert
TCH (Daten, 9.6 kbit/s)	12.0	60	5
TCH (Daten, 4.8 kbit/s)	6.0	60	10
TCH (Daten, $\leq 2.4$ kbit/s)	3.6	72	20
Full-Rate FACCH	9.2	184	20
Half-Rate FACCH	4.6	184	40
SDCCH	598/765	184	3060/13
SACCH (mit TCH)	115/300	168+16	480
SACCH (mit SDCCH)	299/765	168+16	6120/13
BCCH	598/765	184	3060/13
AGCH	n*598/765	184	3060/13
PCH	p*598/765	184	3060/13
RACH	r*27/765	8	3060/13





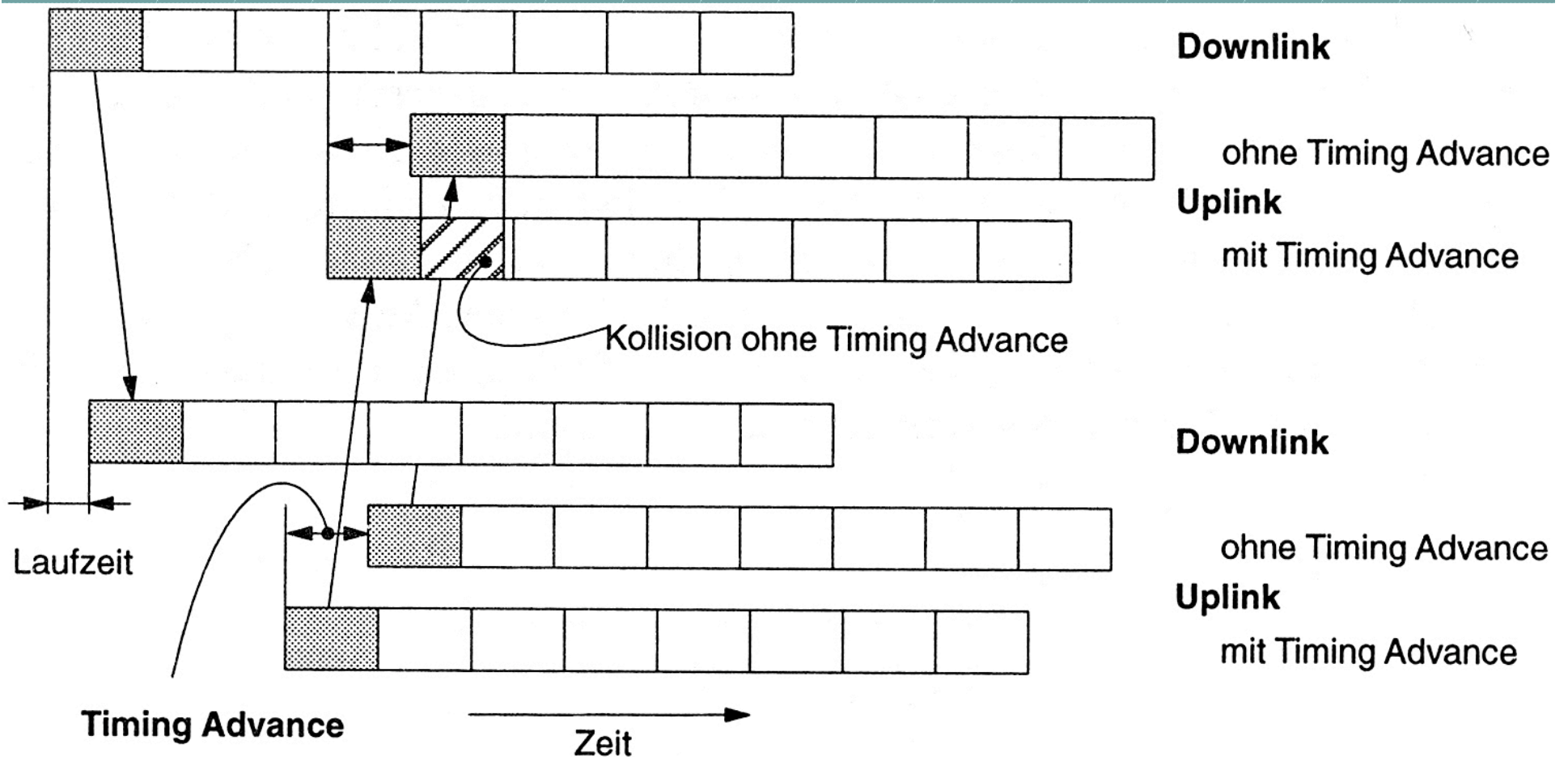
# Physikalische Kanäle

- ♦ Jeder Kanal in 8 Time-Slots geteilt **TDMA**
- ♦ Uplink 3 Slots später als Downlink **TDD**
- ♦ Eigene Frequenz für Up/Downlink (45 MHz Abstand) **FDD**
- ♦ Jeder Timeslot enthält Burst von 156.25 Bitperioden = 576.9  $\mu\text{s}$



# Timing Advance

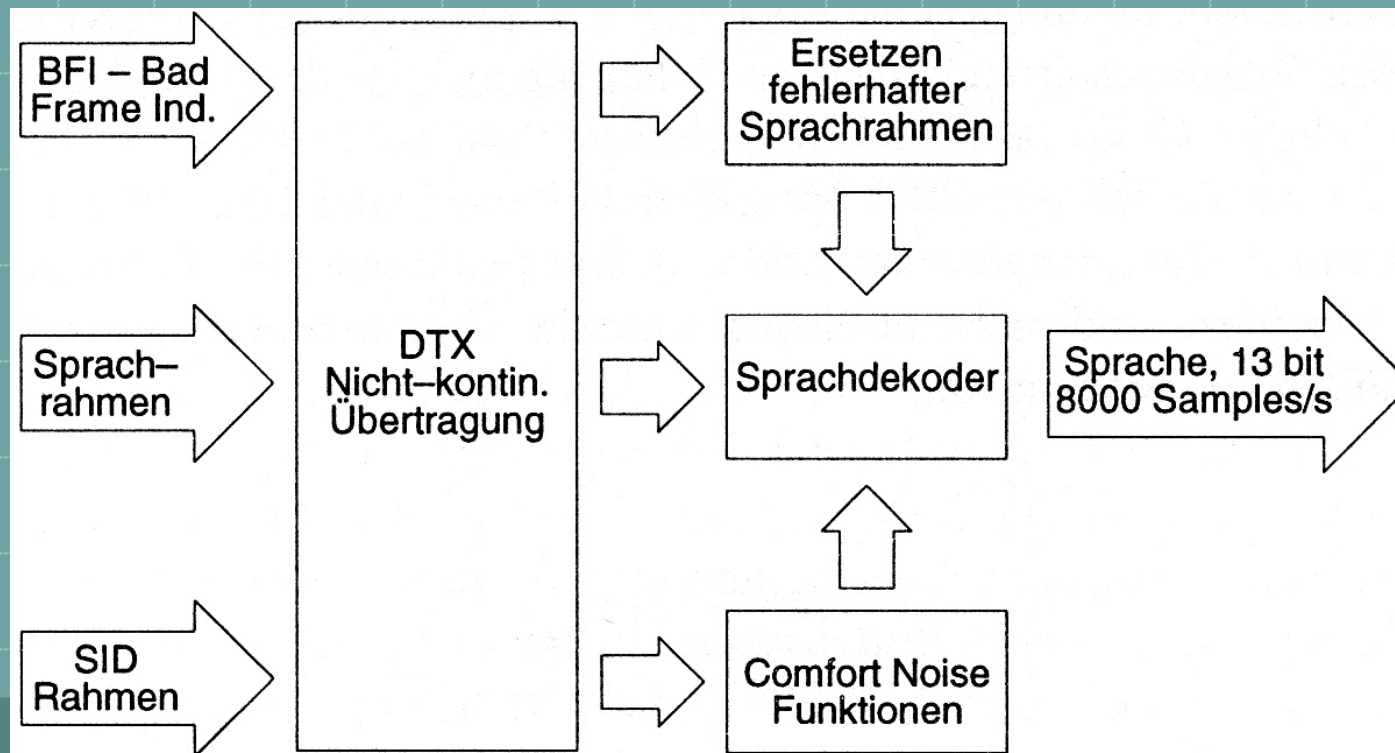
- ◆ Signallaufzeit - **TDMA** Slots müssen präzise getroffen werden!!





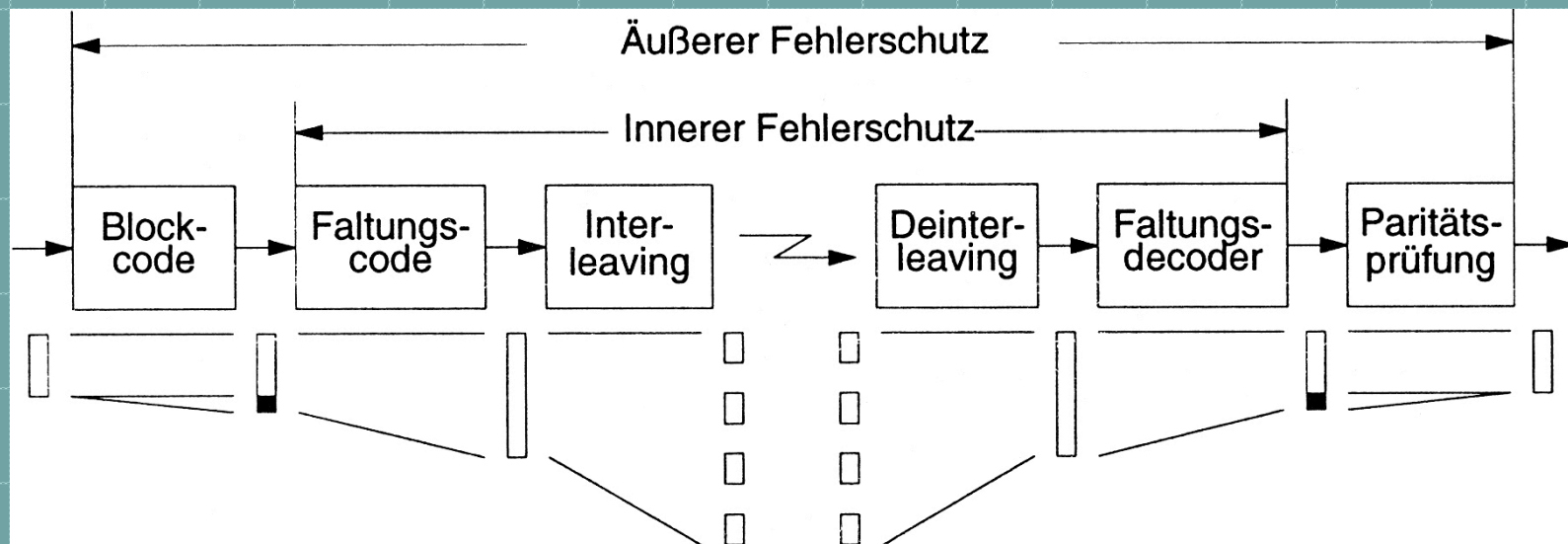
# Audio Codec

- ◆ Regular Pulse Excitation - Long term Prediction **RPE-LPT**
- ◆ Grobe Hüllkurve + Klangparameter -> Sprachsynthese



# Fehlerkorrektur

- ♦ Daten hoch komprimiert - sehr fehleranfällig



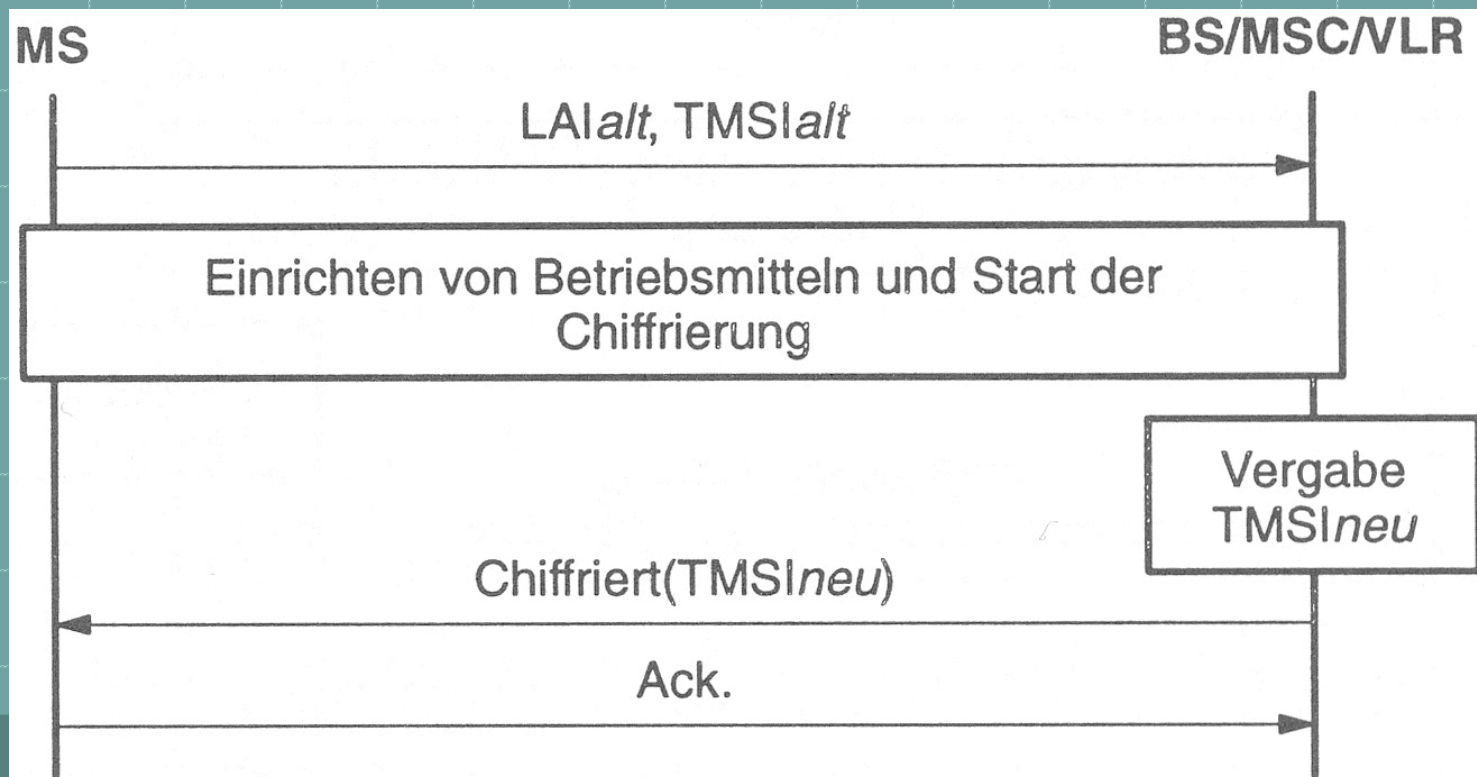
Blockcode: Fehlererkennung; Faltungscode: zusätzliche Redundanz

Interleaving: Schutz vor Bündelfehlern

Klasse 1 Daten: Hohe Sicherheit; Klasse 2: weniger Sicherheit

# Schutz der Teilnehmeridentität

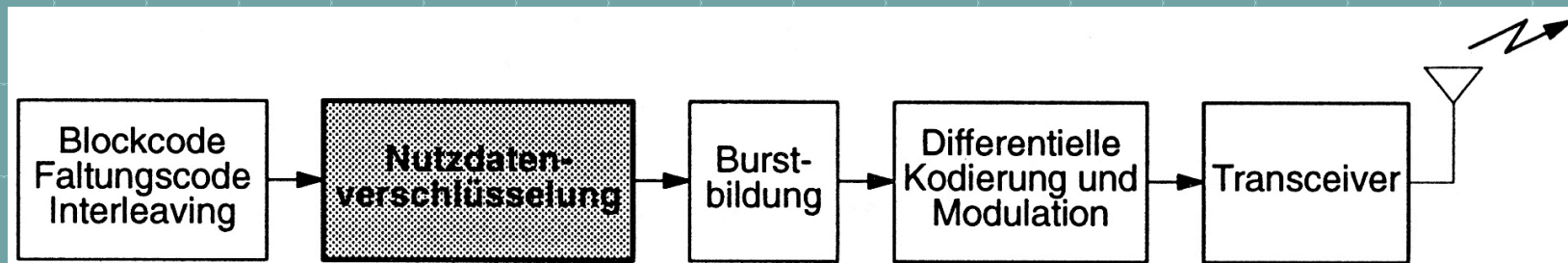
- ♦ Verwendung von **TMSI** statt **IMSI**
- ♦ **TMSI** bei jedem *Location Update* neu vergeben



# Teilnehmerauthentifizierung

- ◆ Geheimer Schlüssel **Ki** (128 Bit)
  - ◆ Im **AUC** des Heimat Netz und im **SIM** gespeichert
- ◆ Netz schickt Zufallszahl (**RAND** 128 Bit) an **MS**
- ◆ Diese wird von der **MS** irreversibel mit der **Ki** verrechnet (**SRES**)
- ◆ Netz berechnet **SRES** ebenfalls und vergleicht mit der der **MS**
- ◆ **Ki** wird immer im **AUC** des Heimat-Netz behalten
- ◆ Zur besseren Performance wird ein Satz von (**RAND**, **SRES**) Tupeln im voraus berechnet und an das jeweilige **VLR** gesendet

# Verschlüsselung



- ♦ Mittels **RAND** wird beidseitig (Netz und **MS**) aus **Ki** der **Kc** (*Cipher Key* 64 Bit) berechnet
- ♦ Symmetrische Verschlüsselung nach Algorithmus A5
- ♦ Zusätzlich wird noch die Frame-Nr mit in die Verschlüsselung codiert, diese wiederholt sich alle 3,5 Stunden
- ♦ Uplink und Downlink eigene **Kcs**

# Hürden beim GSM-Sniffen

- ◆ Radio-Scanner
  - ◆ Muß GMSK-Modulation (Gauss-Minimum-Shift-Keying ) können -> sehr, sehr teuer, ca. 150.000 DM
  - ◆ Zwei davon: Uplink/ Downlink !!!
- ◆ Optimale Lage
  - ◆ Gerichteter Funk von **BS** zur **MS**; Interferenzen
  - ◆ Sendeleistungsregulierung, bewegte **MS**
- ◆ Frequency-Hopping (Verfahren zur Reduz. des Rayleigh-Fading)
- ◆ Synchronisation, Timing-Advance, Interleaving, Faltungskodes
- ◆ Sprachkodierung, Signalisierung (Kanalwechsel...)
- ◆ 64 Bit-Verschlüsselung (einzige Hoffnung: Selten mal inaktiv)

# Buchtipps

- ♦ **M. Mouly / M.-B. Pautet: The GSM System for Mobile Communications**
  - ♦ Das absolute Muß für alle, die es wirklich wissen wollen. Informativ, detailliert und in Englisch.
  - ♦ Nur bei den Autoren [direkt erhältlich](#),
  - ♦ Faxbestellungen +33 1 69 310338      ISBN 2-950-71900-7      770 FFR
  - ♦ 130 EUR
- ♦ **K. David / T. Benkner: Digitale Mobilfunksysteme**
  - ♦ Viele wichtige Grundlagen sowie ein gutteil GSM, aber auch ein kurzer Abstecher zu anderen zellularen Netzen.
  - ♦ Verlag Teubner, Stuttgart      ISBN 3-519-06181-3      76,00 DEM
  - ♦ 38,86 EUR ( ICH HABE DIESES BUCH )
- ♦ **G. Heine: GSM-Signalisierung verstehen und praktisch anwenden**
  - ♦ Ausführliche und verständliche Darstellung aller, aber auch wirklich aller Aspekte dieses Themas. Unbedingt lesen.
  - ♦ Verlag Franzis', Poing      ISBN 3-7723-5773-3      178,00 DEM