

Konzepte von Betriebssystem-Komponenten: Schwerpunkt Sicherheit (KVBK)

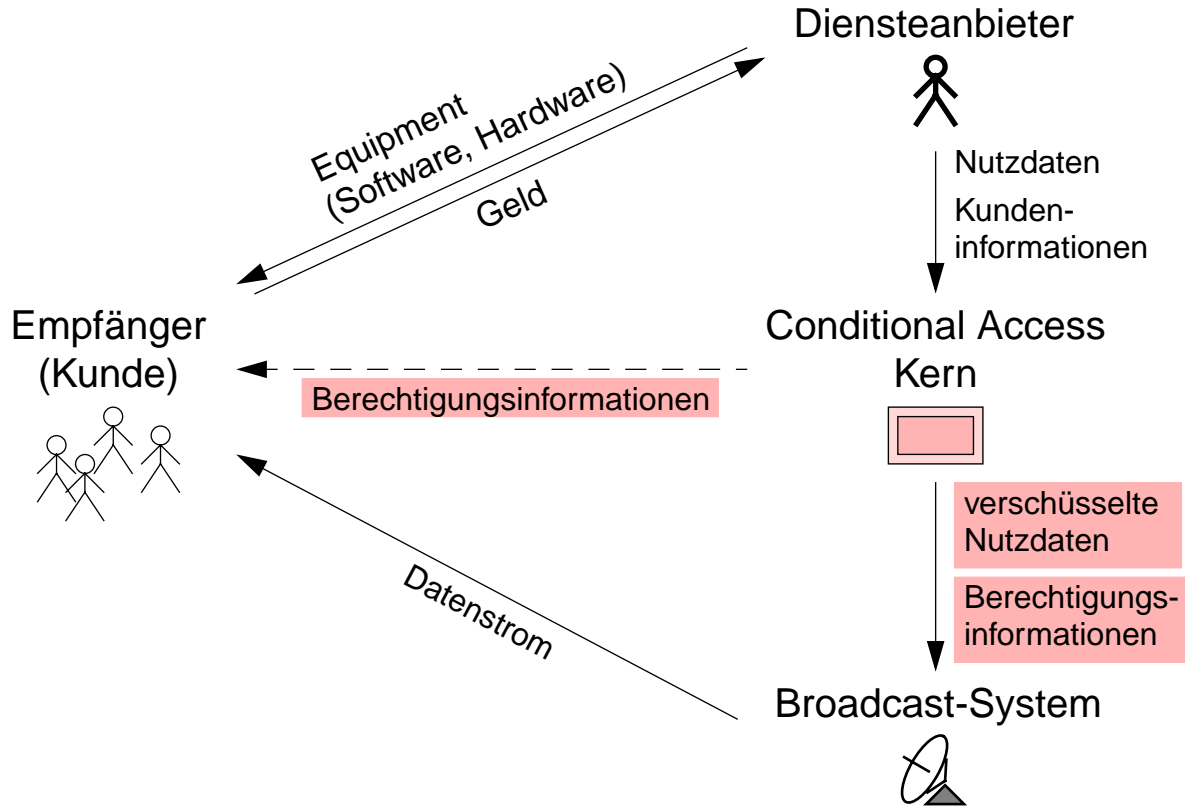
Adaption eines Conditional Access Systems für Eureka 147 DAB (Diplomarbeitsvortrag)

Andreas Weißel

Überblick

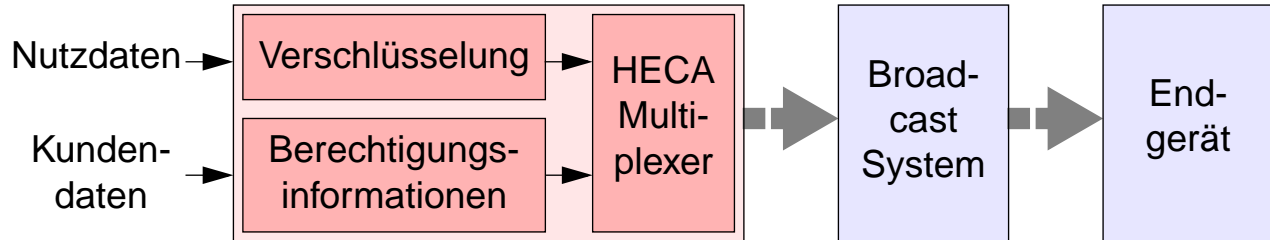
- Conditional Access Systeme
- HECA - High Efficient Conditional Access
- Decodermodul
- Stromchiffrierungen
- Lineare rückgekoppelte Schieberegister
- Implementierungen

Conditional Access Systeme



HECA - High Efficient Conditional Access (1)

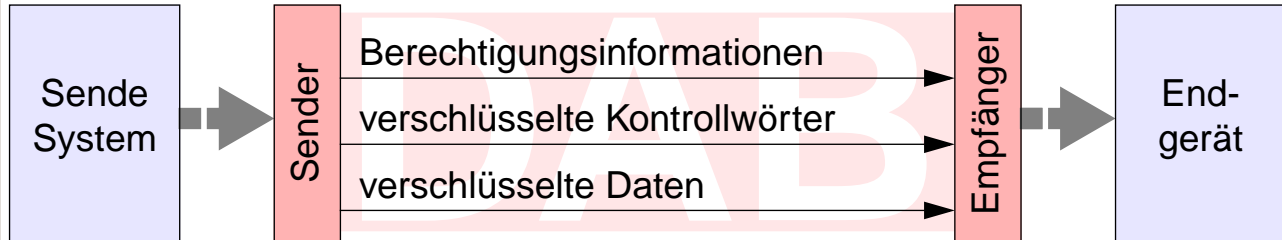
■ Sendeseite (Conditional Access Kern)



- Verschlüsselung der Daten mit schnell wechselnden "Kontrollwörtern"
- Kundendaten umfassen Art des Abonnements und Gültigkeitszeitraum
→ Generierung von Berechtigungsinformationen:
Freischaltungen, Verlängerungen
- passive Kündigung

HECA - High Efficient Conditional Access (2)

■ Broadcast-System



■ Drei Nachrichtentypen:

- ◆ Berechtigungsinformationen (Entitlement Management Message - EMM)
- ◆ verschlüsselte Kontrollwörter (Entitlement Control Message - ECM)
- ◆ verschlüsselte Daten

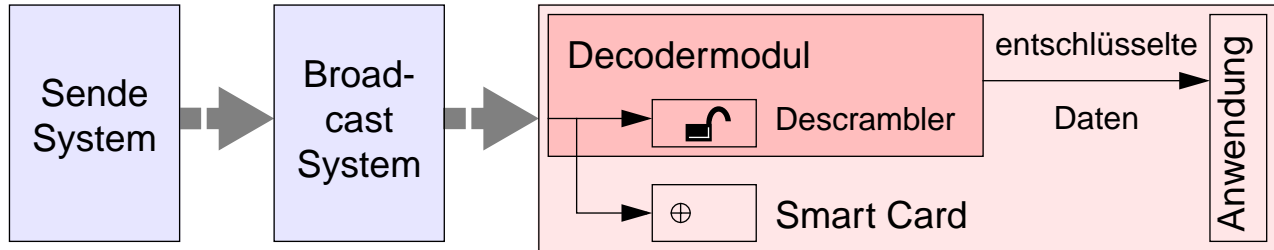
■ Einheitliches Format: SCDL - Smart Card Description Language

EUREKA 147 DAB

- Adaption von HECA an Eureka 147 DAB
- Digital Audio Broadcasting
 - ◆ digitales terrestrisches Rundfunksystem
 - ◆ fehlerkorrigierende Übertragung
 - ◆ digitale Audioprogramme mit unterschiedlicher Bitrate
 - ◆ Datendienste (HTML-Seiten, Bilder, Filme ...)
 - ◆ vorbereitet für den Einsatz von Conditional Access
 - ◆ Nettodatenrate max. 1.8 MBit/s
- Regelbetrieb seit 1998 (u. a. Deutschland)

HECA - High Efficient Conditional Access (3)

■ Endgerät (Decodermodul)



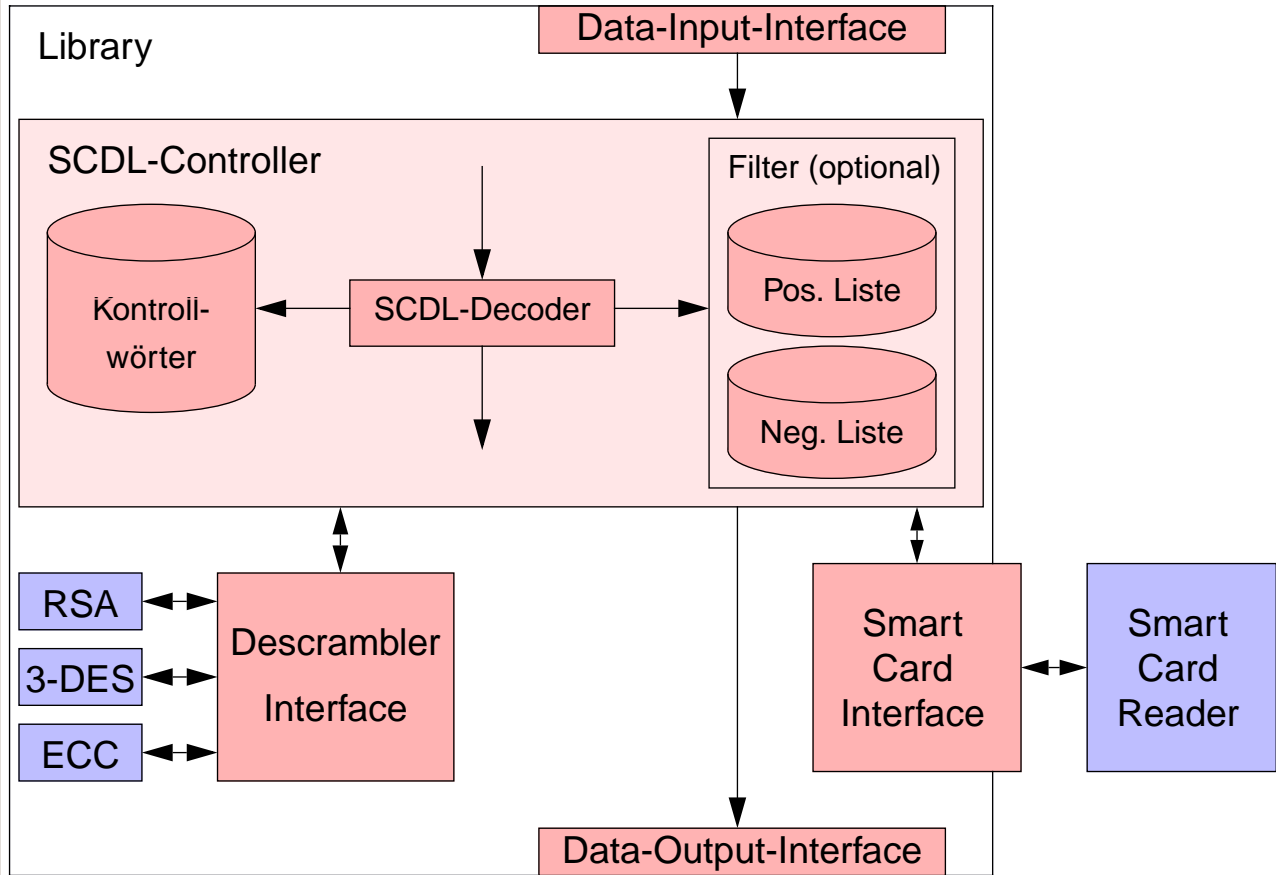
■ Verarbeitung der drei Nachrichtentypen

■ Smart Card als Sicherheitsmodul

- ◆ überprüft und verwaltet Berechtigungsinformationen
- ◆ decodiert bzw. erzeugt Kontrollwörter

■ Descrambler zur Entschlüsselung der Daten

Decodermodul



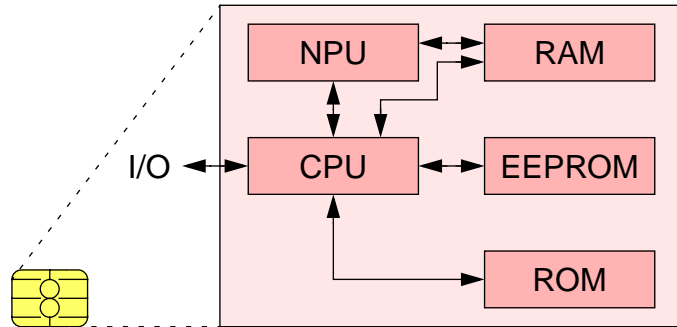
Filter

- Smart Card ist der Flaschenhals des Systems (niedrige Verarbeitungsgeschwindigkeit und Datenübertragungsrate)
- Filterung von Nachrichten
 - ◆ Nachrichten, die nicht für diese Smart Card codiert sind
 - ◆ Nachrichten, die bereits erfolgreich verarbeitet wurden
 - ◆ in Abhängigkeit vom erfolgreichen Verarbeiten anderer Nachrichten
- Realisiert durch
 - ◆ Smart Card Id
 - ◆ eindeutige Nachrichten-Ids
 - ◆ Positiv-Liste (Ids erfolgreich verarbeiteter Nachrichten)
 - ◆ Negativ-Liste (Ids nicht erfolgreich verarbeiteter Nachrichten)

Smart Cards

■ Chipkarte mit Sicherheitslogik

- ◆ Mikrocontroller mit (Krypto-)Coprozessor
- ◆ Speicherplatz 8 - 64 KBit



■ Sicherheit

- ◆ Einsatz kryptographischer Verfahren (Authentisierung, Verschlüsselung)
- ◆ Interne Daten nur über Befehlssatz erreichbar, Zugriffsrechte

■ Schutz vor Angriffen auf die Hardware

- ◆ Messen des Stromverbrauchs (Leistungsanalyse)
- ◆ Speicherdesign (optische Analyse)
- ◆ Ausführungszeit von Kryptoalgorithmen

Überblick

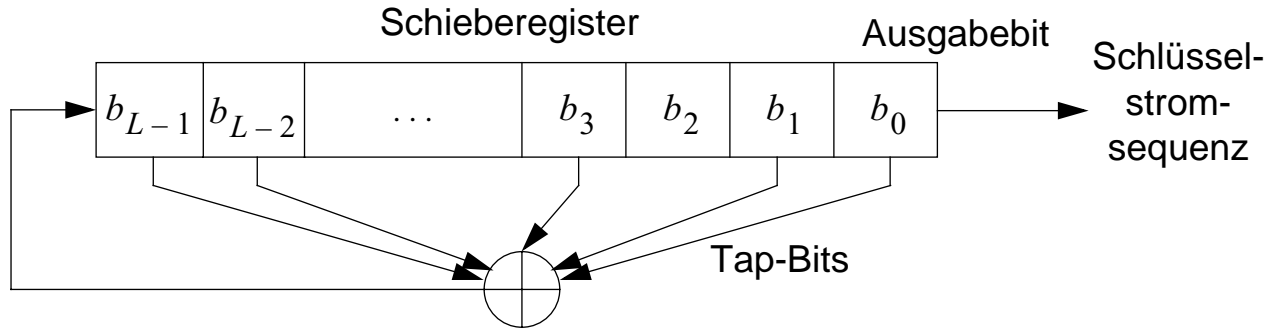
- Conditional Access Systeme
- HECA - High Efficient Conditional Access
- Decodermodul
- Stromchiffrierungen
- Lineare rückgekoppelte Schieberegister
- Implementierungen

Stromchiffrierungen

- Blockchiffrierungen (z.B. DES) verschlüsseln Datenblöcke fester Länge
- Stromchiffrierungen (*stream ciphers*) verschlüsseln Bit für Bit:
 - ◆ Erzeugen pseudo-zufällige Bitsequenzen mit großer Periode (z.B. 2^{128} Bit)
 - "Schlüsselstromsequenz"
 - ◆ Klartext \oplus Schlüsselstromsequenz = Chiffretext
 - ◆ Der Schlüssel initialisiert den Generator
 - ◆ Meist einfacheres Design und damit höhere Geschwindigkeit als Blockalgorithmen
- Bekannte Algorithmen: A5 (GSM), RC4 (SSH), Seal, Wake
- Häufigste Realisierung: lineare rückgekoppelte Schieberegister
 - ◆ Intensiv analysiert; Eigenschaften genau bekannt
 - ◆ Effizient in Soft- und Hardware realisierbar

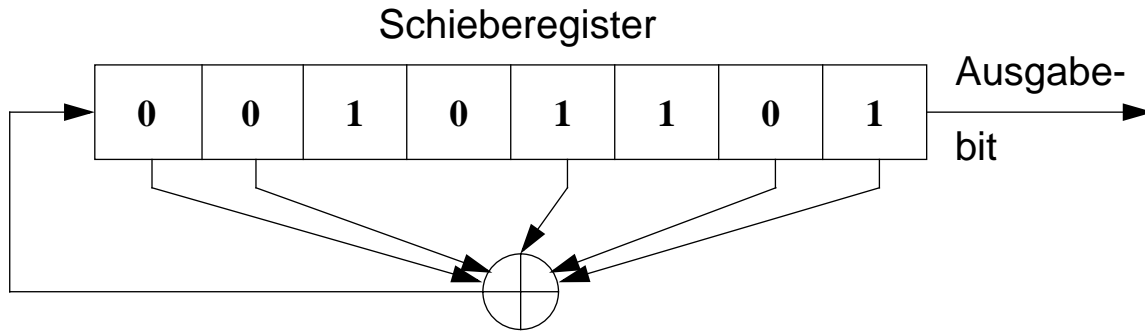
Lineare rückgekoppelte Schieberegister (1)

- Aufbau (Register der Länge L)



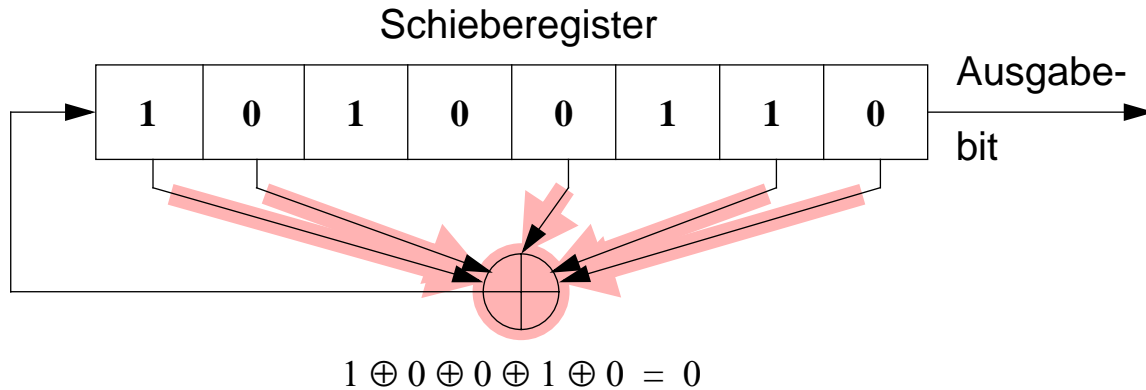
- Bei jeder Taktung:
 - ◆ XOR-Verknüpfung der Tap-Bits
 - ◆ Shift um 1 nach rechts, dabei Ausgabe des niederwertigsten Bits b_0
 - ◆ Ergebnis der XOR-Verknüpfung in b_{L-1} speichern
- Periode abhängig von Tap-Konfiguration (max. $2^L - 1$)

Lineare rückgekoppelte Schieberegister (2)

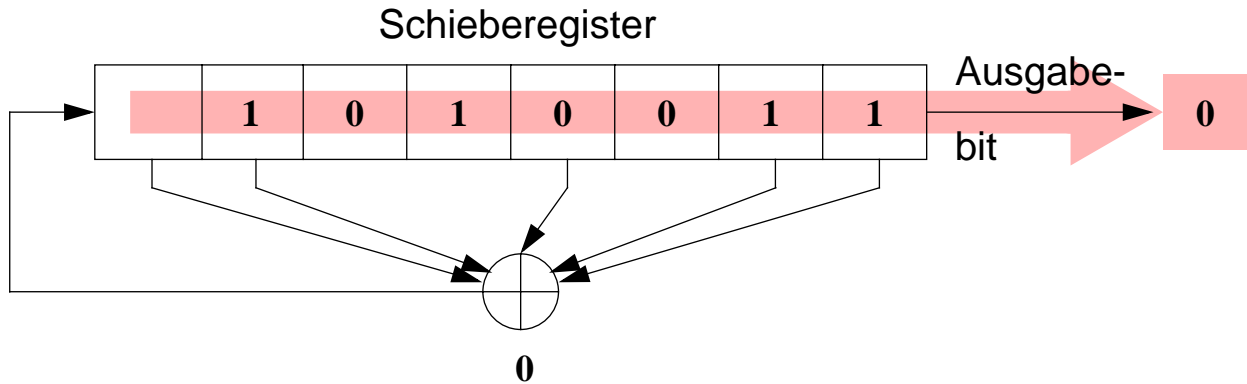


- Taps: b_7 , b_6 , b_3 , b_1 und b_0

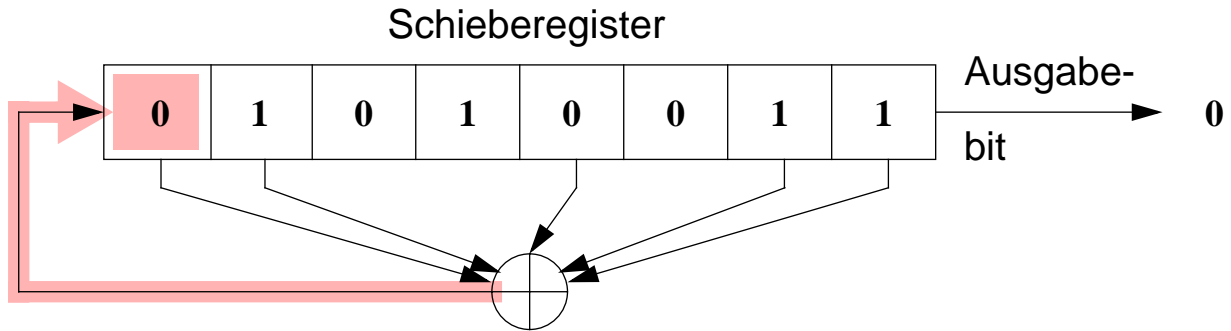
Lineare rückgekoppelte Schieberegister (3)



Lineare rückgekoppelte Schieberegister (4)



Lineare rückgekoppelte Schieberegister (5)



Lineare rückgekoppelte Schieberegister (6)

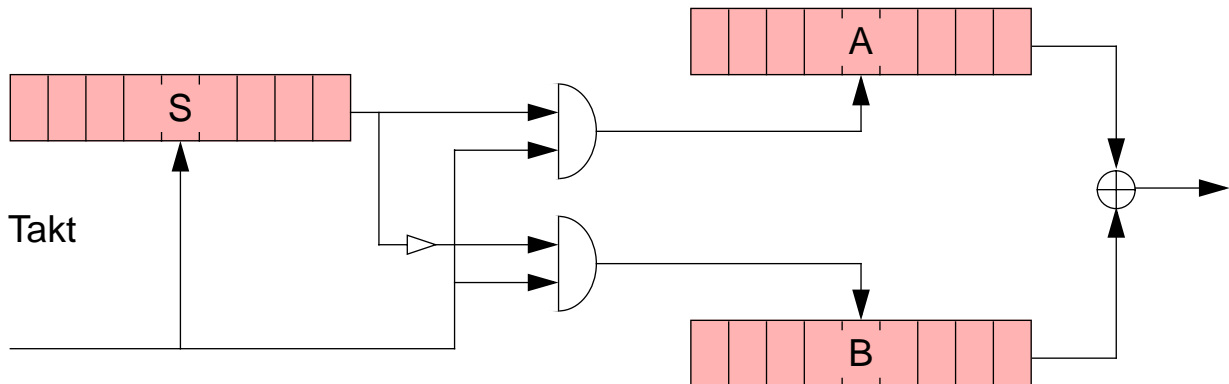
- Schlüssel bestimmt Anfangszustand (Inhalt) und evtl. Tap-Konfiguration
- Effizienter Algorithmus zur Bestimmung der Tap-Konfiguration
 - ◆ Ein einzelnes lineares rückgekoppeltes Schieberegister ist nicht sicher!
 - ◆ Kombinationsgeneratoren:
 - Die Ausgabe des Generators ist eine nichtlineare Funktion der Ausgaben eines oder mehrerer Register.
 - ◆ taktgesteuerte Generatoren (unregelmäßige Taktung)
- Korrelationsattacken
 - ◆ Gesucht wird eine Korrelation zwischen dem Schlüsselstrom und der Ausgabesequenz mindestens eines Registers.
 - ◆ Anfangszustand dieses Registers rekonstruieren
 - ◆ Weitere Register untersuchen, bis der gesamte interne Aufbau des Generators offenliegt (*divide-and-conquer-Attacke*).

Implementierungen

■ Alternating Step Generator

◆ unregelmäßige Taktung der Register A und B

◆ Attacke auf das Steuerregister möglich; zeitliche Komplexität $O(2^{L_S})$



■ Länge der Schieberegister konfigurierbar

■ Tap-Konfigurationen (maximale Periode) abhängig vom Schlüssel

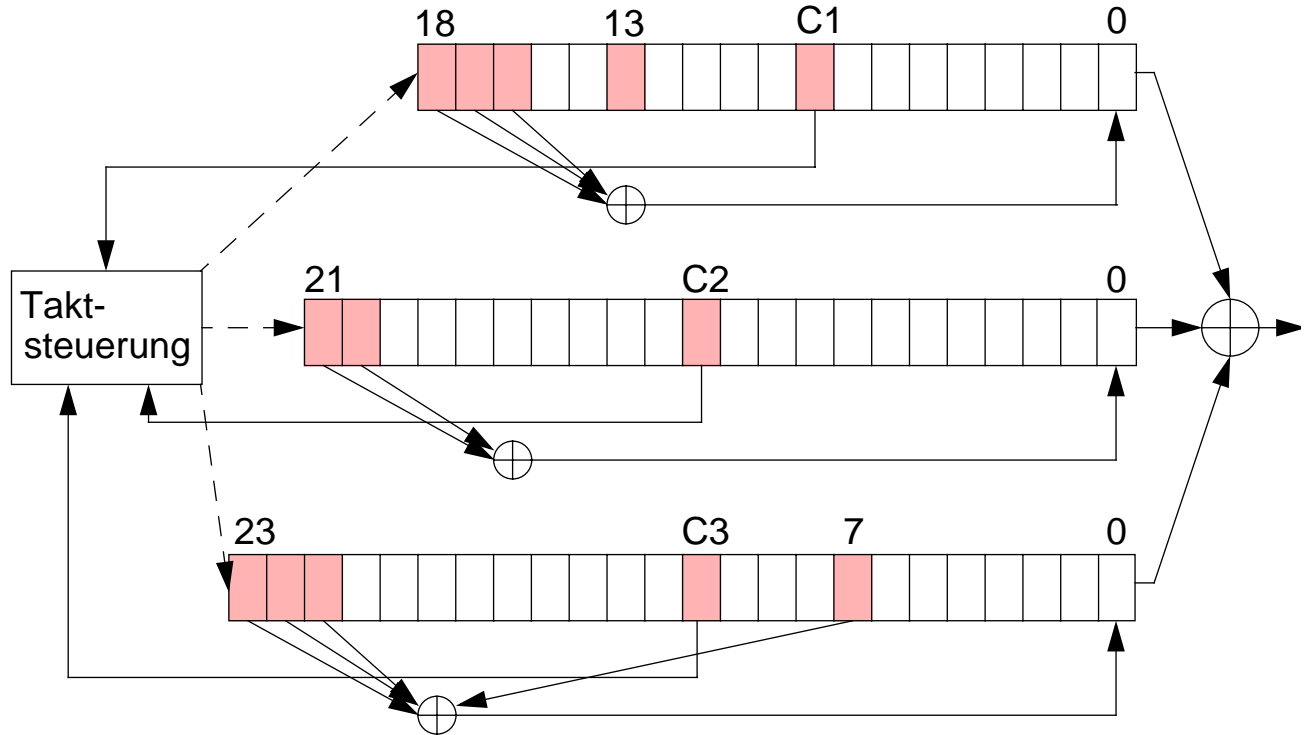
■ Weitere Algorithmen: A5, RC4, Self-Shrinking- und Shrinking-Generator

A5 (GSM-Verschlüsselungsalgorithmus)

- Variante A5/1 (USA, Teile Europas)
 - ◆ 3 kurze Register (insgesamt 64 Bit)
 - ◆ Über eine Mehrheitsfunktion der drei mittleren Register-Bits wird die Taktung der einzelnen Register gesteuert.
 - ◆ geheimer Schlüssel auf SIM-Karte (Smart Card) im Handy + Framenummer

- Effizienteste Attacke (Biryukov, Shamir und Wagner 1999)
 - ◆ handelsüblicher PC mit 128 MByte RAM und 4*73 GB Plattenplatz
 - ◆ Ermittelt geheimen Schlüssel innerhalb von zwei Minuten.
 - Mithören eines Gesprächs (fast) in Echtzeit möglich!
 - ◆ Algorithmus ausreichend sicher ab 128 Bit Gesamt-Registerlänge

A5 (GSM-Verschlüsselungsalgorithmus)



Ausblick

- Conditional Access System "VIACCESS" der France Telecom nicht erfolgreich.
- Pilottest für HECA/DAB (200 Zuhörer)
- Deutsche Telekom AG plant Mitte 2002 Einsatz für DVB ("Digital Video Broadcasting") Datendienste.
- Integration der Stromchiffrierungen in HECA
- Realisierung des Decodermoduls in Hardware (ASIC)

GSM-Verschlüsselung

- SIM-Karte enthält:
 - ◆ K_A : geheimer Schlüssel zur Authentisierung und Schlüsselgenerierung
 - ◆ A8: Algorithmus zur Erzeugung des Schlüssels
 - ◆ A3: Authentisierungsalgorithmus

