CAS implementálása MPEG-2 TS-alapú hálózatokon

Unger Tamás István
ungert@maxwell.sze.hu

2014. április 16.

Tartalom

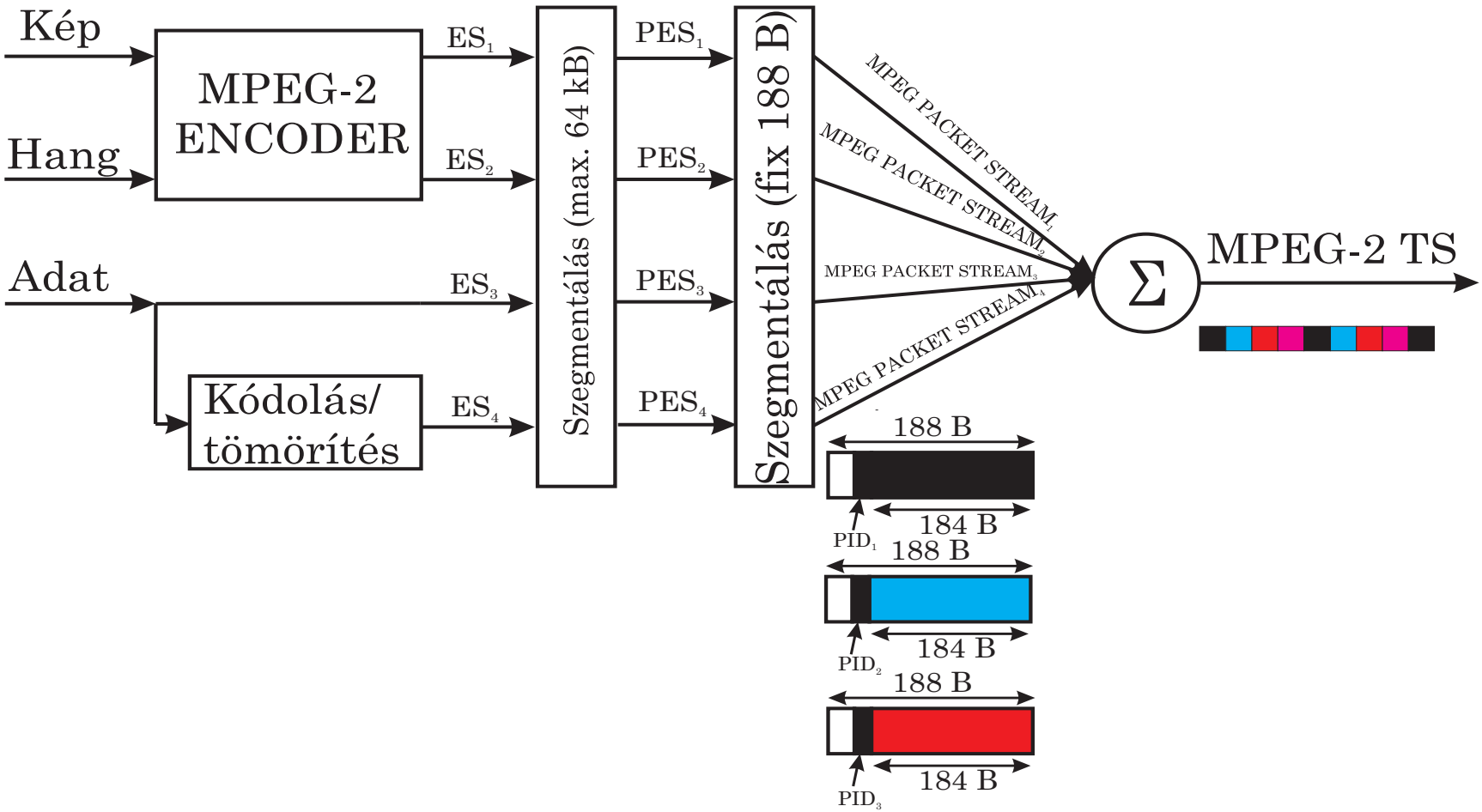
1. *Az MPEG-2 TS rövid áttekintése*
2. *Rendszeradminisztráció*
3. *A kiválasztott program felépítése*
4. *A titkosítás igénye*
5. *Szimmetrikus és aszimmetrikus titkosítás*
6. *A CAS lényege*
7. *Adó- és vevőoldali rendszertechnika*
8. *Scramblerezés*
9. *ECM, EMM, CAT*
10. *A rendszer, sávszélességek*

Az MPEG-2 TS

Az MPEG-2 TS **adatátvitelre** tervezett rendszer, amely képes hang és kép megbízható átvitelére is, így alkalmas műsorszórásra.

1. Tömörített hang és/vagy kép, adat $\rightarrow$ **E**lementary **S**tream
2. ***ES**-ek változó hosszúságú szegmentálása (max. 64 kB), header + payload struktúra* $\rightarrow$ **P**acketized **E**lementary **S**tream
3. **PES**-ek szegmentálása fix hosszúságú MPEG-2 csomagokra $\rightarrow$ 4 B header + 184 B payload = 188 B MPEG-2-packet
4. MPEG-2-packetek $\rightarrow$ MPEG-2 TS
5. 13 bit **P**acket **ID**entifier a headerben $\rightarrow$ mi van a payloadban?

Az MPEG-2 TS



1. ábra. Az MPEG-2 TS felépítése

Rendszeradminisztráció

Az MPEG-2 TS szerkezete rugalmas és nyílt, adott esetben rengeteg hang-, kép- és adatstreamet tartalmazhat. A streameket rendszerezni, adminisztrálni kell, televíziórendszerek esetén programokhoz, programcsomagokhoz kell rendelni, előfizetéses rendszer esetén **titkosítani** kell.

Megoldás:

Adminisztrációs táblák továbbítása a rendszeren TS-packetek formájában a hasznos adatot szállító streamek mellett.

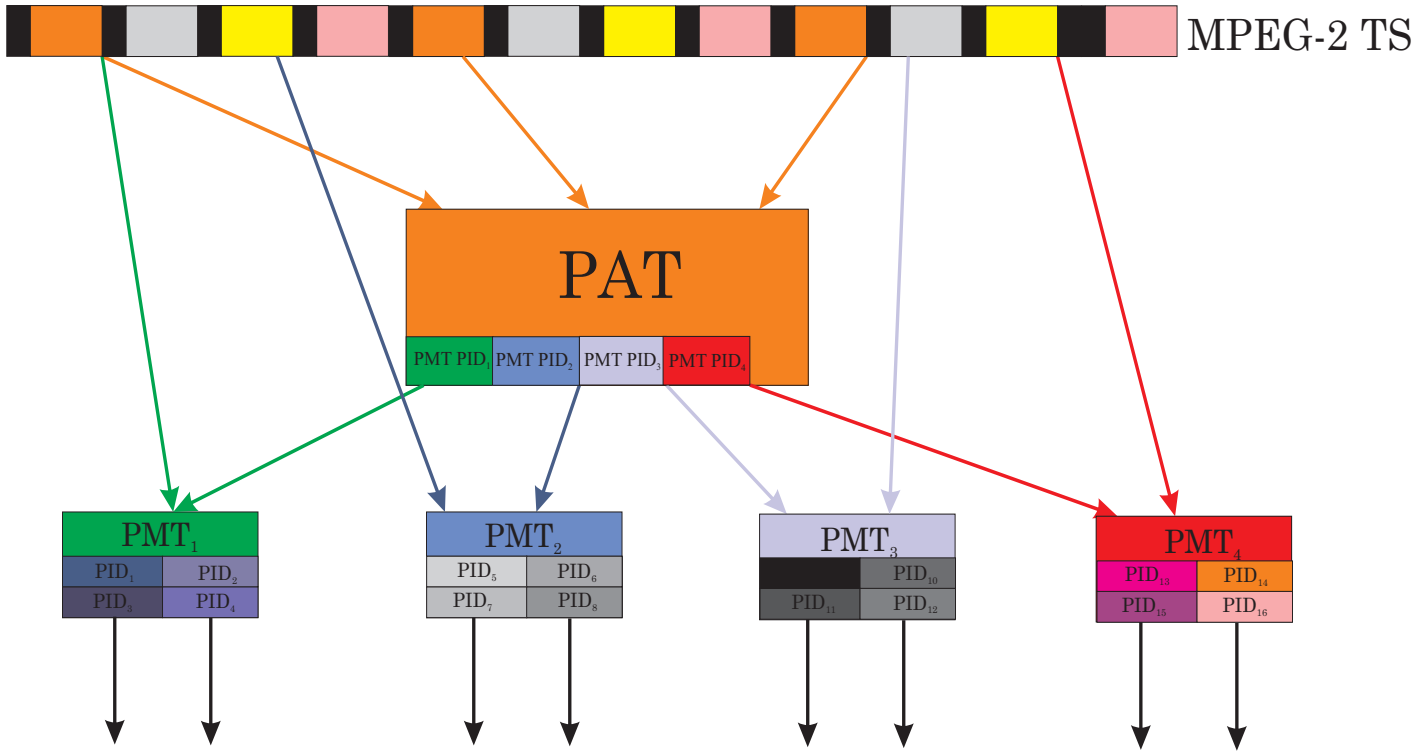
Hogyan zajlik egy program kiválasztása?

Rendszeradminisztráció

Program**S**pecifikus **I**nformációk továbbítása

1. Szinkron az adatfolyammal
   - Az MPEG-2-packetek elejét fix helyű és értékű flag jelzi ($0x47_H$)
2. Programszerkezet kiolvasása
   - **PAT**-tábla kiolvasása (*Program Association Table*). Szabványos packetek szállítják, PID-je mindig zérus, a rendszer $0,5$ s időközönként megismétli. 1 TS $\rightarrow$ 1 PAT. Megadja, hány program van a streamben. **A PAT-tábla PMT-táblák PID-jeit hordozza.**
   - A kiválasztott program **PMT**-táblájának kiolvasása (*Program Map Table*). Tartalom: adott programhoz tartozó PES-ek PID-jei. $\sum 2$ kerül általában kiválasztása (kép + hang).

Hogy is néz ez ki?



Hang + kép kiválasztása

Kiválasztott program

2. ábra. Egy program felépítése

Titkosított adatfolyam továbbítása MPEG-2 TS-alapú hálózaton

Igény:

Előfizetési díjhoz kötött szolgáltatások továbbítása során felmerül az igény a programok és a hozzájuk tartozó adatfolyamok titkosítására.

Megoldás:

MPEG-2 TS-alapon működő broadcast-hálózatok esetén fontos alapelv, hogy **kizárólag PES-ek kerülnek titkosításra**, maga az MPEG-2 stream nem, így a rendszeradminisztrációs táblák sem.

Ok:

Ha a packet stream kerülne titkosításra, a PAT-tábla sem lenne visszafejthető, így az ingyenes, kódolásmentes csatornák sem lennének dekódolhatóak a rendszer hierarchiájából fakadóan.

CAS - Conditional Access System

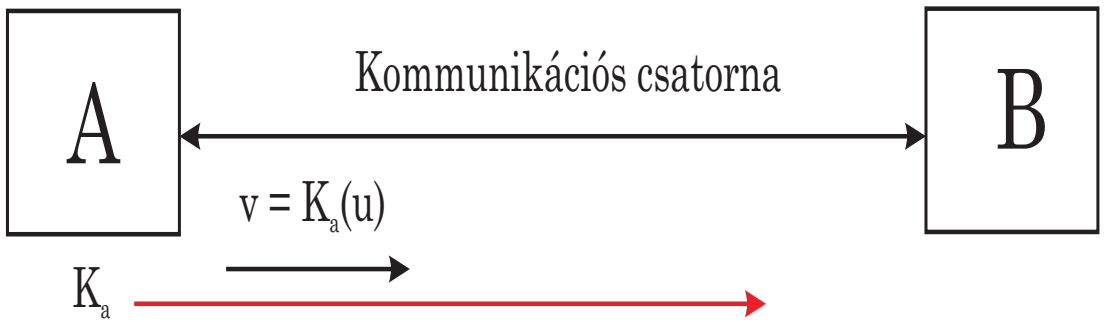
A vevőoldali dekódernek ki kell nyernie a transport streamből a titkosítás feloldásához szükséges adatokat.

Erre szolgál az MPEG-2 TS CAT-táblája (*Conditional Access Table*).

Alapelv:

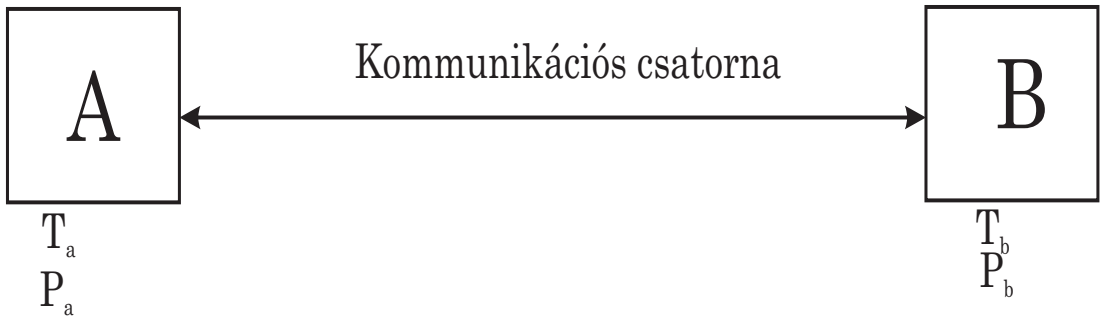
A szésztosztó jellegű hálózat struktúrájához igazított, kvázi-szimmetrikus, hierarchikus titkosítási rendszer és algoritmus.

Szimmetrikus titkosítás



Lényege, hogy mind a kódolás, mind a dekódolás ugyanazzal a kulccsal történik. Előnye az egyszerűségében rejlik, hátránya, hogy a kulcsot valamilyen úton át kell juttatni a generálási helyről a másik oldalra.

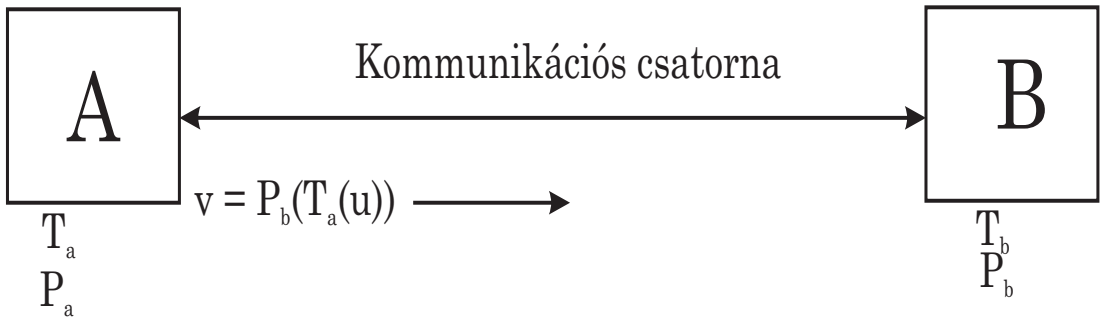
Aszimmetrikus titkosítás - 1.



Kulcsgenerálás

A és B oldalon egyaránt le kell generálni egy összetartozó nyilvános-titkos kulcspárt. A kommunikáció során P_a-t és P_b-t nyilvánosságra kell hozniuk a kommunikáló feleknek, míg T_a és T_b nem kerül átvitelre, a genenrálás helyén, a generáló oldalán marad. A nyilvános-titkos kulcspárok egymás inverzei.

Aszimmetrikus titkosítás - 2.



Az üzenet elkódolása:

Amennyiben A üzenni akar B-nek, úgy az eredeti *u* üzenet helyett egy *v* üzenetet fog elküldeni, amely az eredeti üzenet A titkos kulcsával elkódolt verziójának B nyilvános kulcsával elkódolt változata. Ezt a kétszeresen kódolt üzenetet küldi át A a kommunikációs csatornán.

Aszimmetrikus titkosítás - 3.

Visszafejtés:

B oldalon a visszafejtés a következőképpen történik:

$$u = P_a(T_b(v)) \tag{1}$$

Bizonyítás:

Mivel az elején kikötöttük, hogy $T_b^{-1} = P_b$:

$$T_b(v) = T_b(P_b(T_a(u))) = T_a(u) \tag{2}$$

A második lépcsőben pedig $P_a^{-1} = T_a$ felhasználásával:

$$P_a(T_b(v)) = P_a(T_a(u)) = u \tag{3}$$

A CAS lényege

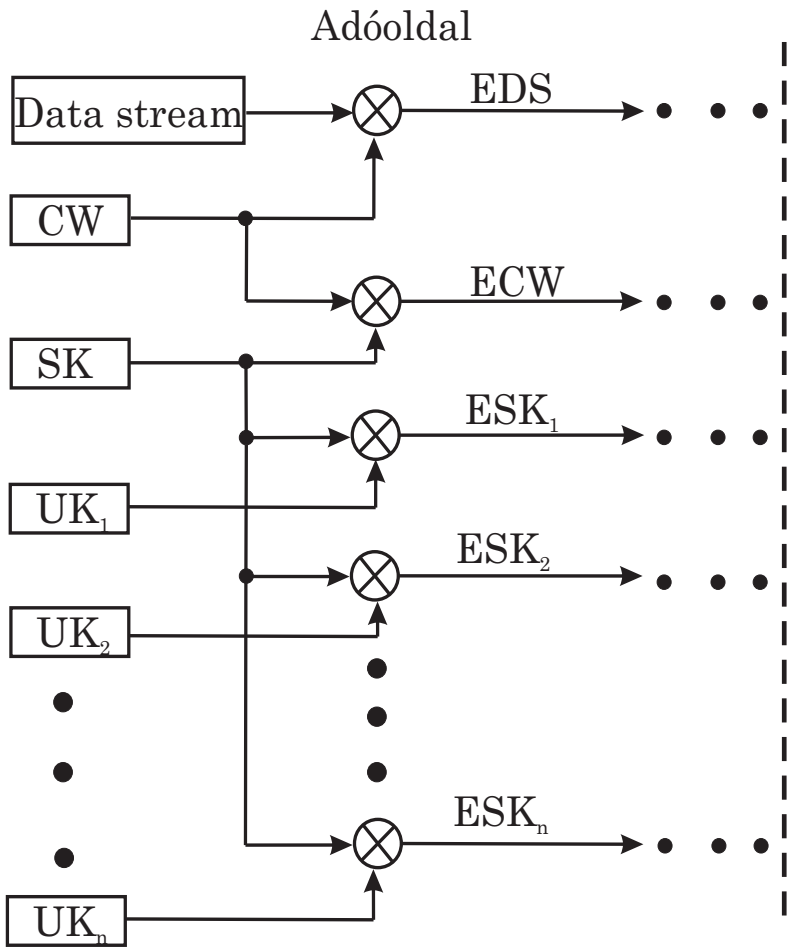
A rendszer három kulcsot definiál:

- **C**ontrol **W**ord (**CW**)
- **S**ervice **K**ey (**SK**)
- **U**ser **K**ey (**UK**)

Adóoldali rendszertechnika:

PES-alapú titkosítás a **CW**-vel. A rendszer a **CW**-t az **SK** segítségével titkosítja (**E**ncrypted **CW**,**ECW**), majd broadcastolja a hálózaton.
1 csatorna $\rightarrow$ *1* ***CW***
A közös **SK** az előfizetőnként individuális $\mathbf{UK}_n$ segítségével kerül titkosításra, majd előfizetőnként külön-külön átvitelre ($\mathbf{EUK}_n$).

Sematikus adóoldali rendszertechnika



3. ábra. Adóoldali rendszertechnika

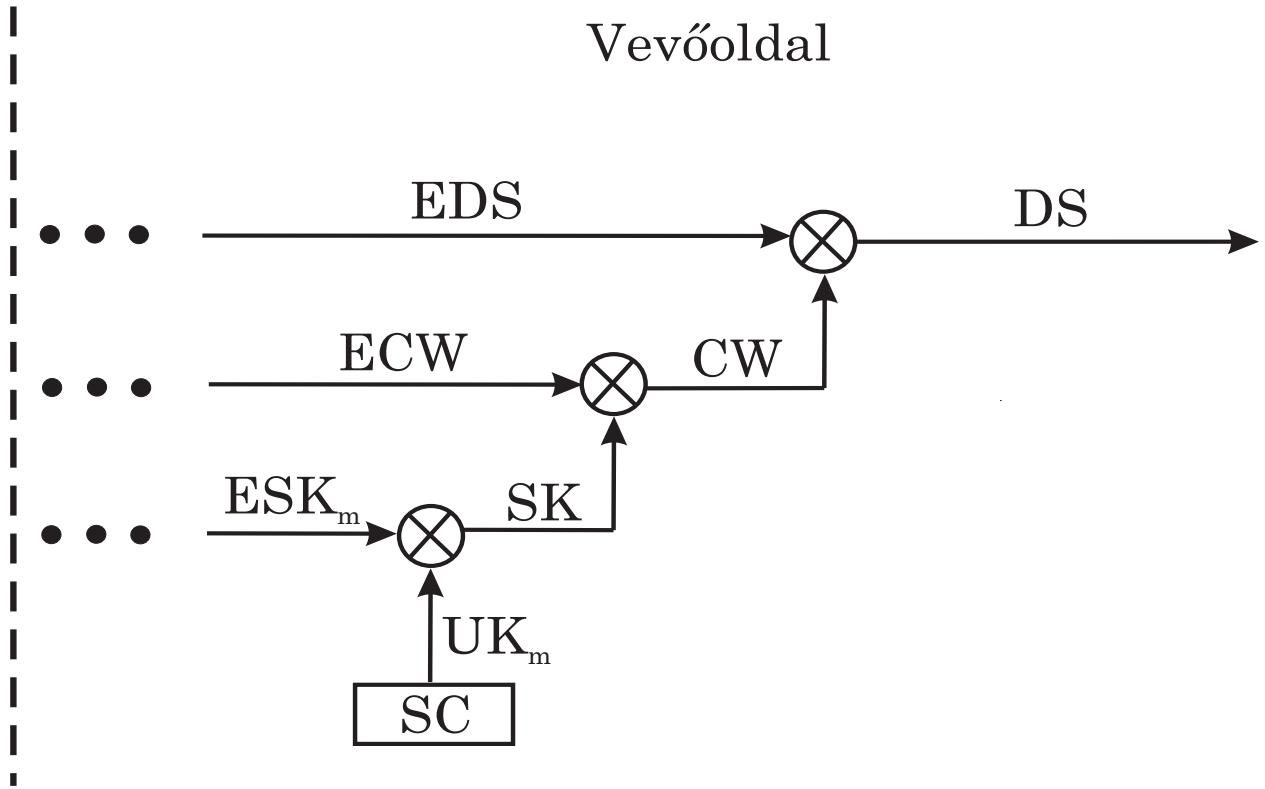
A CAS lényege

Vevőoldali rendszertechnika:

A vevőoldalon kezdetben kizárólag az individuális **UK** áll rendelkezésre a dekódoláshoz, tipikusan az előfizető **S**mart **C**ard-ján. A dekódolás általános lépései:

- **ESK** dekódolása **UK** segítségével $\rightarrow$ **SK**
- **ECW** dekódolása **SK** segítségével $\rightarrow$ **CW**
- **D**ata **S**tream dekódolása **CW** segítségével $\rightarrow$ ☺

Sematikus vevőoldali rendszertechnika



4. ábra. Vevőoldali rendszertechnika

Kvázi-szimmetrikus titkosítás

Szimmetrikus, mert:

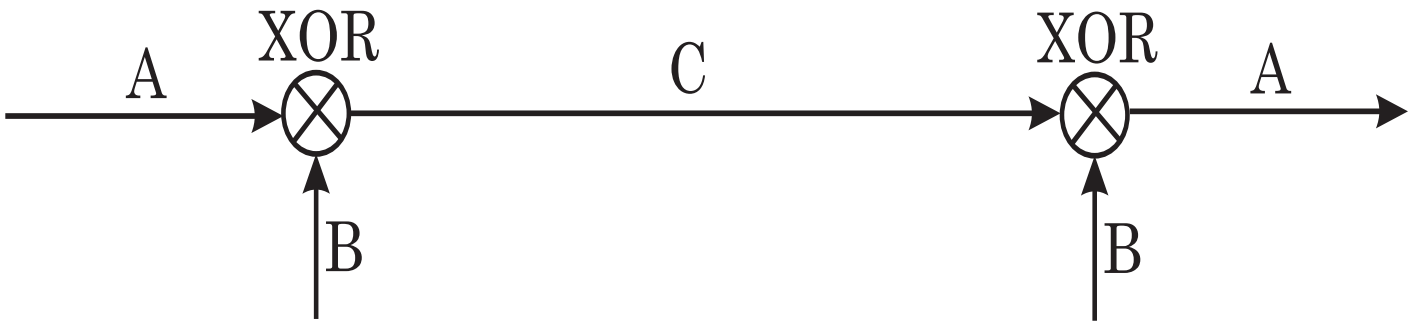
- Az adóoldali titkosító kulcs megegyezik a vevőoldali dekódoló kulccsal (**CW**)
- **CW** titkosító kulcsa adóoldalon megegyezik a vevőoldali dekódoló kulccsal (**SK**)
- **SK** titkosító kulcsa adóoldalon megegyezik a vevőoldali dekódoló kulccsal (**UK**)

Aszimetrikus, mert:

- **SK** felfogható az adó által generált nyilvános-, **UK** pedig titkos kulcsként
- Az MPEG-2 TS nem viszi át a hálózaton a titkos kulcsot

Scramblerezés

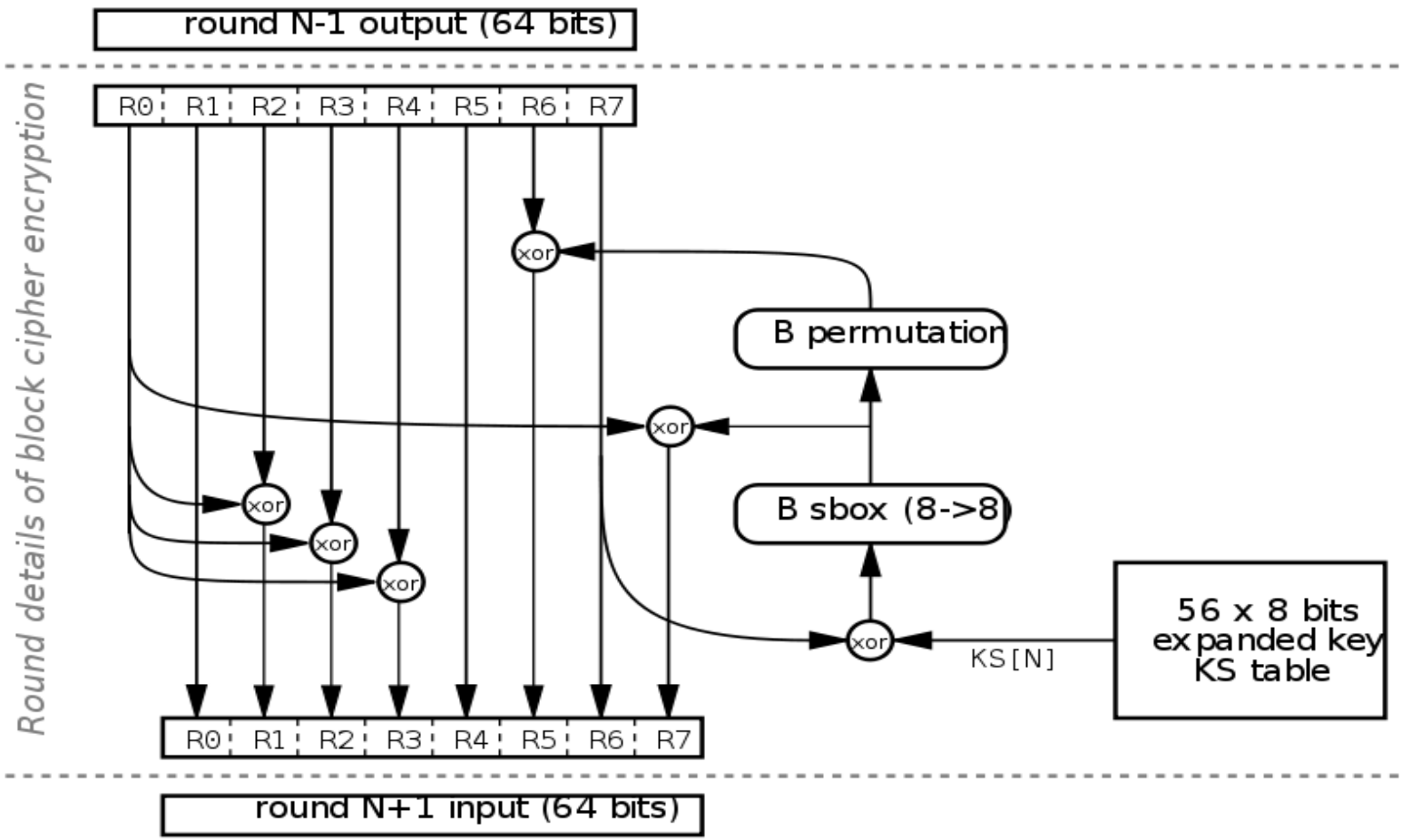
Alapelv:



A	B	C	B	A
0	1	1	1	0
1	1	0	1	1
0	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	0	1	0	1

Elvi demonstrációra kiváló, de a gyakorlat ennél jóval komplexebb...

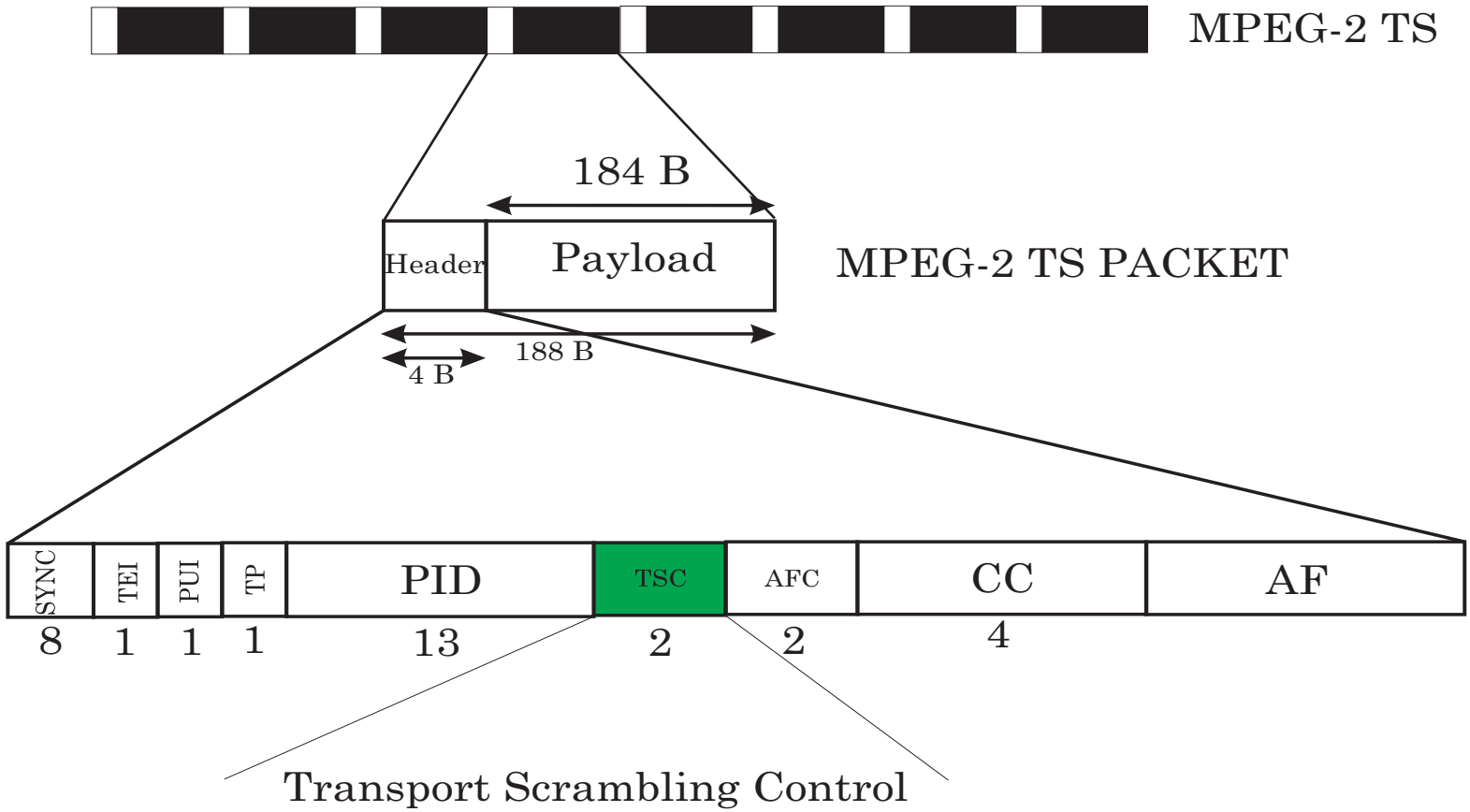
Gyakorlati megvalósítás: CSA (forrás: Wikipedia)



5. ábra. Blokk alapú CSA

Transport Scrambling Control - 1.

Biztonsági okokból a **CW**-t kb. 10 másodpercenként változtatják → a folytonos dekódolás érdekében két **CW** kerül továbbításra.



Transport Scrambling Control - 2.

Bitkombináció	Jelentése
00	Nem scramblerezett, nem titkosított adatfolyam
01	Nem használt, jövőbeli alkalmazásra fenntartva
10	Páros **CW**-vel titkosítva
11	Páratlan **CW**-vel titkosítva

Kérdések:

És hol visszük át a **CW**-t? Mi az, hogy páros, mi az, hogy páratlan?

ECM - Entitlement Control Message

Az első lépcső:

MPEG-2 TS-alapú rendszerek a CW-t az SK-val titkosítva viszik át ECM-üzenetek formájában. Ez még kevés, hiszen SK közös, nem subscriber-individual.

Tartalma:

Szolgáltatónként változó. Ami fix:

- Két **CW**
- Dátum, idő $\rightarrow$ él még az előfizetés?
- Csatornaazonosító $\rightarrow$ csatornánként eltérő, de csomagonként azonos is lehet

A rendszer az **ECM** üzeneteket kb. 100 ms időközönként ismétli $\rightarrow$ csatornaváltás gyors lekezelése

EMM - Entitlement Management Message

A második lépcső:

MPEG-2 TS-alapú rendszerek az SK-t a user-individual UK-val titkosítva viszik át EMM-üzenetek formájában. Ez a lépés garantálja, hogy csak az jut hozzá az aktuális CW-hez, aki rendelkezik élő, hiteles előfizetéssel.

Tartalma:

- Titkosítatlan hosszmező
- Titkosítatlan címmező. Címzési típusok:
  - Egyedi: Egy set-top-boxnak / **SC**-nek szól (UNICAST)
  - Csoport: Set-top-boxok / **SC**-k csoportjának szól (MULTICAST)
  - Mindenki: Mindenkinek szól (BROADCAST)
- **UK**-val titkosított **SK**

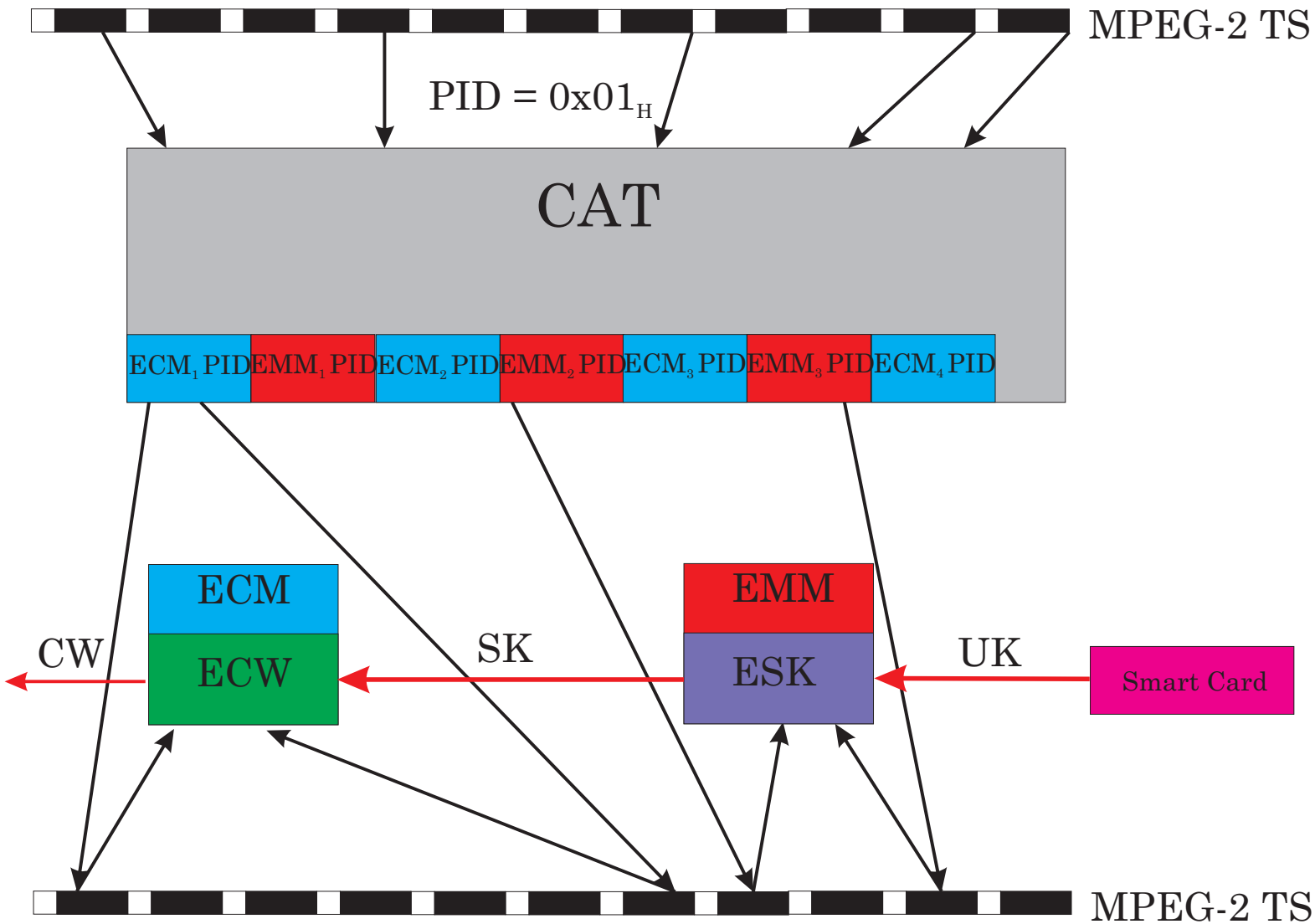
Mivel a hálózat az **ECM**-ek sűrű broadcastolásával már így is "túlterhelt", ezért az **EMM**-eket a rendszer kb. 10 másodpercenként ismétli.

Jó-jó, de honnan tudjuk, hogy mely packetek hordoznak ECM és EMM információkat?

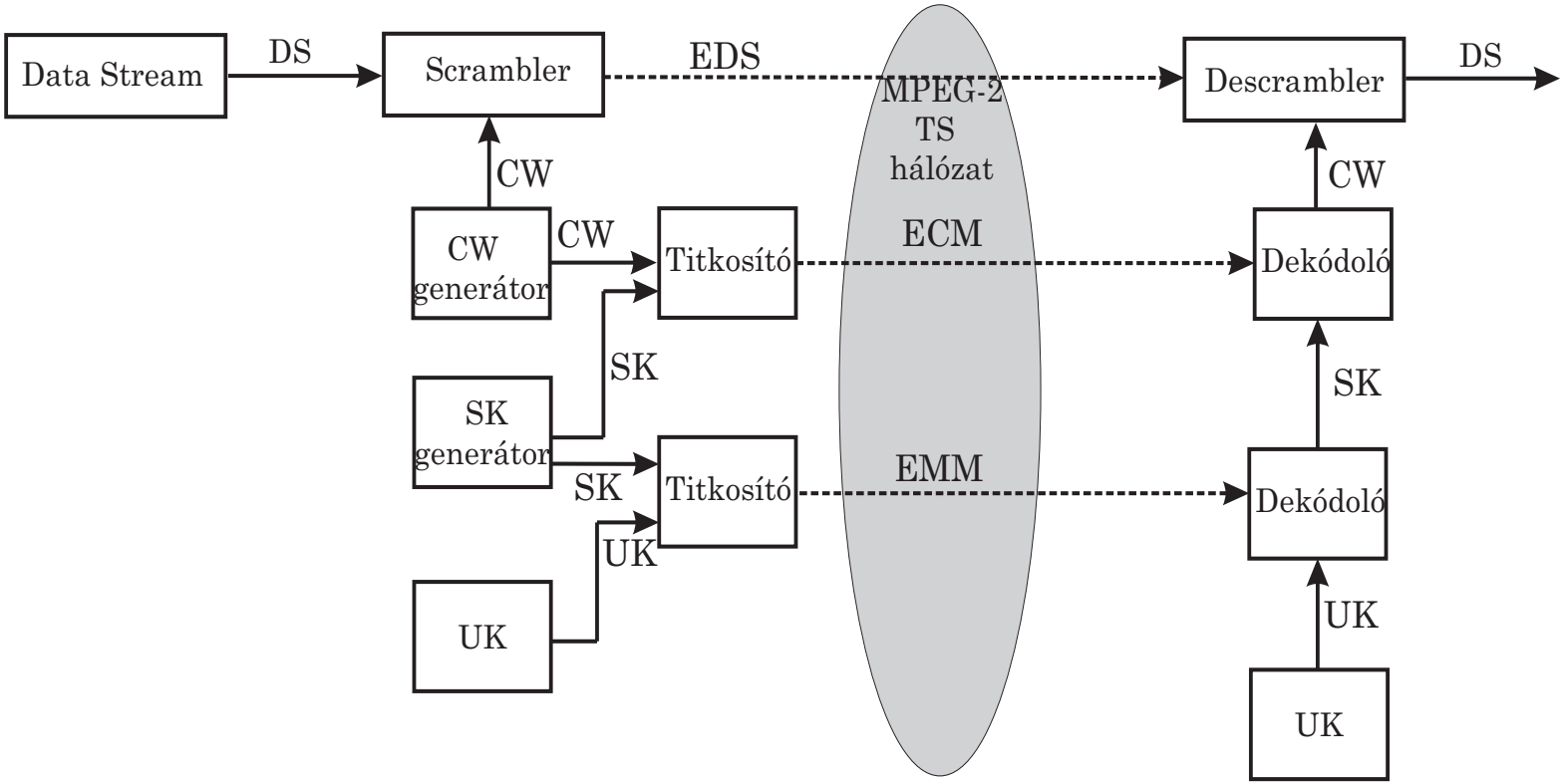
Megoldás:

Feltételes hozzáférési tábla használata (Conditional Access Table - CAT).

CW kinyerése a CAT-tábla segítségével



MPEG-2 TS CAS madártávlatból



6. ábra. CAS madártávlatból

Kitekintés: CAS és a sávszélesség - 1.

ECM/EMM sávszélesség:

$$B = (N \cdot M)\,\frac{L}{F} \tag{4}$$

Ahol:

- B: sávszélesség [bps]
- N: csatornák száma
- M: előfizetők száma
- L: **ECM/EMM** üzenet hossza [bit]
- F: **ECM/EMM** üzenet ismétlődési periódusa [s]

Kitekintés: CAS és a sávszélesség - 2.

1 000 000 előfizetővel és 30 csatornával számolva, feltéve, hogy az **ECM** üzenet legrövidebb hossza kb. $168bit$, az **EMM** üzenet legrövidebb hossza kb. $488bit$, továbbá **ECM**-üzenetek csak **CW**-frissítéskor kerülnek továbbításra, míg **EMM** üzenetek kizárólag óránként:

ECM sávszélesség:

$$B_{ECM} = (1 \cdot 30)\frac{168bit}{10s} = 504bps \quad (5)$$

EMM sávszélesség:

$$B_{EMM} = (1 \cdot 10^6 \cdot 30)\frac{488bit}{3600s} \approx 4,07\ Mbps \quad (6)$$

Az **EMM** a szűk keresztmetszet!

Kérdések?

Köszönöm a figyelmet!