DVB – Digital Video Broadcasting

Sicurezza su Reti II

Umberto Palo matr. 0521000836
Prof. Alfredo De Santis

Sommario

CAPITOLO 1: Lo standard DVB per la televisione digitale terrestre

1.1 Introduzione

In questo primo capitolo, parleremo dei vantaggi dello standard digitale rispetto alla trasmissione analogica, vedremo un analisi relativa all'introduzione e allo sviluppo della televisione digitale terrestre in Italia guardando i servizi e le applicazioni offerte con il DVB. Verranno descritti in modo generico il ricevitore – decodificatore integrato e i sistemi riceventi di utente, si parle del decoder integrato, del decoder unico dei sistemi simulcript e multycript e saranno introdotto termini che saranno specializzati e approfonditi nel capitolo 4. Nella parte finale del capitolo si parlerà degli standard DVB più utilizzati e verranno visti in modo generico, poi specializzati in alcune loro parti nei capitoli successivi, gli standard trasmissivi quelli interattivi e le codifiche video utilizzate. Ora verrà effettuata una breve storia sulla nascita e sviluppo del DVB.

Il rapido progresso delle tecnologie digitali, già a partire dagli anni '90, nei campi della produzione, distribuzione e diffusione televisiva e le nuove prospettive offerte agli operatori del settore e all'industria di consumo, hanno portato alla costituzione nel 1993 del Progetto europeo DVB (Digital Video Broadcasting). Il Progetto, che ora raccoglie oltre 300 Membri europei ed extraeuropei, ha l'obiettivo di armonizzare le strategie volte all'introduzione della televisione digitale e dei nuovi servizi multimediali e interattivi sui vari mezzi trasmissivi e definire le relative specifiche tecniche. Il primo significativo risultato è stato raggiunto con la definizione della specifica del sistema DVB-S per la diffusione diretta da satellite di TV multi - programma, alla quale ha contribuito direttamente il Centro Ricerche Rai; subito dopo sono state definite le specifiche del sistema DVB-C per la distribuzione dei segnali televisivi attraverso le reti via cavo e, successivamente, una intera "famiglia" di specifiche che, partendo dal mondo della televisione, si sono progressivamente allargate a interessare lo scenario delle tecnologie emergenti e dei nuovi media. Le specifiche tecniche approvate dal DVB vengono ratificate dall'ETSI (European Telecommunications Standards Institute) (1) che ne attribuisce la veste di standard europei. All'interno della famiglia DVB le specifiche per la televisione digitale terrestre (DVB-T) assumono una importanza rilevante data la valenza "universale" del servizio televisivo che, nel nostro Paese, raccoglie quasi il 100% dell'utenza. La definizione della specifica DVB-T risale al novembre 1995, con approvazione come standard ETSI nel febbraio 1997; il processo di normalizzazione, piuttosto lungo e complesso, è stato influenzato da vari fattori: la complessità tecnica del problema, dovuta anche alla maggiore ostilità della propagazione del segnale elettromagnetico nelle bande terrestri VHF/UHF rispetto alla diffusione via satellite, la congestione dello spettro di frequenza per la diffusione televisiva terrestre in gran parte dell'Europa ed in particolare nel nostro Paese, l'interesse di soddisfare nuove modalità operative su reti isofrequenziali (SFN) anche a grande copertura, i diversi piani di introduzione dei servizi digitali terrestri formulati dalle varie Amministrazioni europee.

Un contributo decisivo alla definizione delle specifiche DVB-T è stato dato dall'attività condotta dai maggiori radiodiffusori in ambito al progetto europeo RACE dTTb ed a progetti nazionali (HD-DIVINE e HDTV-T), che hanno successivamente adeguato i rispettivi piani di ricerca e sviluppo per soddisfare i requisiti di servizio definiti dal Modulo Commerciale del DVB.
Fra questi:

- la necessità di mantenere la maggior comunanza possibile con i sistemi DVB-S (Digital Video Broadcasting - Satellite) e DVB-C (Digital Video Broadcasting – Cable), al fine di consentire la produzione di ricevitori commerciali multi-standard a basso costo;
- la possibilità di ricezione fissa con terminali portatili, dotati di antenna omni-direzionale, in aggiunta alla ricezione con antenna direttiva posta sul tetto degli edifici;
- la possibilità di introdurre reti SFN (Single Frequency Network) a larga copertura (regionale e nazionale) impiegando trasmettitori sincronizzati operanti sullo stesso canale a radiofrequenza (RF), al fine di sfruttare i significativi vantaggi in termini di efficienza spettrale rispetto alle reti convenzionali multi-frequenza (MFN).

1.2 I vantaggi dello standard digitale

I vantaggi dello standard digitale si riassumono in tre principali ordini di fattori:

1. **il potenziamento del servizio televisivo in termini di quantità e di qualità**.
   A parità di frequenze utilizzate per le reti televisive analogiche, il numero dei programmi digitali irradiabili potrebbe quadruplicarsi o quintuplicarsi. La trasmissione digitale offre una migliore qualità delle immagini e dei suoni e permette di utilizzare schermi televisivi di grande formato (dagli schermi 16:9 a quelli piatti a grandi dimensioni).
   Inoltre il *broadcaster* può usare le risorse di trasmissione con maggior flessibilità: in una determinata area di copertura può ridurre il numero di programmi trasmessi, privilegiando una migliore qualità delle immagini, da diffondere eventualmente anche in alta definizione.
2. **l'offerta di una serie di servizi aggiuntivi di tipo interattivo accessibili tramite il televisore**.
   L'adattatore digitale (detto in seguito: *set - top - box)* da applicare al normale televisore, o il televisore digitale integrato nelle versioni più evolute, hanno capacità di memoria e di elaborazione tali da trattare e immagazzinare le informazioni: l'utente le può acquisire in forma interattiva semplicemente collegando l'apparecchio alla linea telefonica domestica. Ciò significa che anche nelle case prive di personal computer sarà possibile accedere all'insieme dei servizi associati a Internet. Attraverso il televisore i servizi interattivi potranno essere utilizzati da soli o abbinati alle trasmissioni televisive per arricchire i programmi di informazione a richiesta.
3. **la progressiva sostituzione degli attuali mezzi analogici** di produzione, trasmissione e ricezione televisiva con una nuova generazione di mezzi digitali. Sul fronte della produzione dei contenuti televisivi il processo di sostituzione è in corso già da qualche tempo. Sul fronte degli apparati e delle reti di trasmissione i mezzi satellitari si sono aggiornati con grande rapidità per diventare oggi il supporto più usato per la televisione digitale. È lecito supporre che nell'arco dei prossimi 10-15 anni, nella

maggior parte dei paesi europei, le reti di trasmissione televisiva, via terra, via cavo o via satellite, saranno completamente digitali.

La televisione digitale può essere trasmessa via satellite, via cavo e via etere terrestre. Ciascun supporto ha caratteri propri che si riflettono in specifici vantaggi e limiti. La diffusione analogica televisiva terrestre assicura da tempo in Europa una copertura capillare del territorio, essendo disponibile nella quasi totalità (oltre il 95%) delle abitazioni tramite antenne poco costose e semplici da installare. Essa presenta quindi potenzialità superiori rispetto a quelle offerte dalla televisione via cavo e via satellite e rappresenta la soluzione ottimale per chi voglia diffondere programmi in un numero elevato di famiglie e voglia perseguire, anche con il digitale, quegli obiettivi di *servizio universale* che da sempre in Europa hanno caratterizzato l'attività televisiva.
Le reti terrestri presentano tuttavia altri vantaggi essenziali, quali:

1. **la portabilità** del servizio, la possibilità cioè,di ricevere i programmi ovunque, grazie a un'antenna mobile, senza predisporre punti di allacciamento alla rete in ognuno dei luoghi deputati, anche temporaneamente, al consumo televisivo.
2. **la regionalità.** Il territorio regionale è troppo esteso per essere coperto capillarmente da una rete di trasmissione via cavo a costi non elevati, laddove il satellite ha una copertura geografica molto ampia, non circoscrivibile su scala regionale.

Sotto il profilo strettamente economico le trasmissioni digitali terrestri rappresentano una risorsa per lo Stato, i consumatori e l'industria dei prodotti elettronici di largo consumo.
Nel decidere il passaggio alle trasmissioni digitali terrestri il Governo genera effetti economici di lungo termine. Vengono infatti poste le condizioni per un uso più efficiente dello spettro hertziano, con la liberazione di una parte delle frequenze da destinare, secondo le scelte, a ulteriori canali televisivi terrestri, ad altri servizi diffusivi (*data broadcasting*) o di telecomunicazione (servizi interattivi mobili) o da ripartire tra le diverse funzioni. I vantaggi del digitale terrestre, tuttavia, sono innegabili anche per i consumatori e l'industria. I consumatori non solo disporranno, sul televisore domestico e senza significativi aggravi di spesa, di una assai più ampia gamma di programmi fra i quali scegliere, ma potranno anche compiere da casa operazioni che oggi richiedono l'utilizzo del computer o implicano spostamenti in luoghi specifici (e-*commerce, home banking*, persino adempimenti amministrativi).
Per le attività svolte attraverso i servizi interattivi che passano per il televisore, vi sarà dunque una drastica riduzione dei costi di transazione (*home banking*, *e-finance*) e di informazione (*e-commerce*) .
Per l'industria elettronica di largo consumo si apriranno ottime prospettive, determinate dal necessario rinnovo degli apparecchi televisivi e dalla maggiore produzione di *set-top-box .*
In una fase transitoria, i consumatori che non vorranno sostituire il proprio apparecchio dovranno aggiungere al televisore tradizionale una "scatola" esterna, il *set-top box*, in grado di convertire i segnali analogici in segnali digitali. La tecnologia contenuta in tali apparati, la cui produzione già in alcuni Paesi ha dato vita a un autonomo e fiorente segmento produttivo, può essere più o meno complessa: in alcuni casi i *set-top-box* possono convertire i segnali trasmessi da una sola piattaforma di trasmissione, in altri sono compatibili con due o più piattaforme, in altri ancora possono fornire l'accesso non solo ai canali televisivi digitali, ma anche a vari servizi di tipo interattivo.
Questa evoluzione è particolarmente rilevante per l'industria italiana che, nell'ultimo quindicennio, ha vissuto una fase di progressivo declino.

In futuro le componenti elettroniche necessarie a ricevere le trasmissioni digitali saranno incorporate nel televisore che diventerà in tal modo un apparato integrato per la ricezione di servizi digitali domestici. Già oggi si registra un aumento nella produzione di televisori digitali con funzioni interattive e una netta diminuzione dei prezzi.

I vantaggi di sistema derivanti dalla rapida adozione della televisione digitale terrestre sono dunque:

- l'uso efficiente delle risorse frequenziali destinate alla diffusione terrestre;
- un'offerta di programmi e servizi più ampia e meglio rispondente alle richieste del pubblico;
- un incremento dei consumi e degli introiti dell'industria produttrice (in ambito software e *hardware*) ;
- l'accelerazione alla diffusione, presso il grande pubblico, dell'uso di Internet e dei servizi interattivi sofisticati;
- un impulso all'adozione di nuove tecnologie e relativi guadagni di posizione nella competizione internazionale.

1.3 Analisi relativa all'introduzione e allo sviluppo della televisione digitale terrestre in Italia

1.3.1 Servizi e applicazioni

Gli standard digitali, sviluppati in seno al Consorzio europeo DVB e ratificati dall'ETSI (*European Telecommunications Standard Institute*), offrono nuove opportunità per i fornitori dei servizi, i gestori di rete e l'industria del settore, in un mercato caratterizzato dalla convergenza fra radiodiffusione, telecomunicazioni e information technology (2). Gli standard DVB forniscono la soluzione globale alla domanda crescente di nuovi servizi generalisti e tematici, free-to-air e a pagamento, multimediali e interattivi e consentono un sensibile miglioramento della qualità del servizio.
I nuovi servizi resi disponibili possono essere suddivisi in tre classi:

- enhanced broadcasting;
- televisione interattiva;
- accesso a Internet.

L'enhanced broadcasting si caratterizza per:

- il formato delle immagini in 16:9 (HDTV – *HighDefinition Television*), particolarmente adatto alla visione di film ed eventi sportivi;
- l'audio con qualità CD (Compact Disk) e la possibilità di avere più canali audio per un programma multilingue;
- l'EPG (*Electronic Programme Guide*), in grado di fornire informazioni sulla programmazione aggiornate in tempo reale.
- il super-Teletext, che può fornire contenuti graficamente arricchiti, immagini, ipertesti, clip audio e video, ecc.

La *televisione interattiva* consente una "interattività locale" e una "interattività con canale di ritorno". L'**interattività locale** consiste nella trasmissione ciclica di contenuti (*data carousel*) che vengono memorizzati nel ricevitore e utilizzati successivamente da parte dell'utente.

L**'interattività con canale di ritorno** risulta fondamentale per promuovere lo sviluppo di nuovi servizi di specifico interesse per il singolo utente. Ne sono un esempio la *pay-tv* e la *pay per view*, l'acquisto di prodotti e di servizi tramite televisore e così via.

L'accesso ad Internet tramite televisore offre all'utente tutte le potenzialità offerte da un personal computer. Il ricevitore-decodificatore integrato diventerà nel tempo un terminale d'utente multimediale e rappresenterà uno degli elementi propulsivi della cosiddetta "nuova economia".

1.4 Il ricevitore-decodificatore integrato e i sistemi riceventi di utente

1.4.1 Il ricevitore-decodificatore integrato

Per i ricevitori-decodificatori integrati il Comitato ha studiato alcune soluzioni tecniche e di regolamentazione in linea col dettato della legge (la n. 78 del 29 marzo 1999).
Le raccomandazioni tecniche sono state formulate sulla base di un'analisi del "modello funzionale" del decoder e sulla base di previsioni sui costi di produzione e sui prezzi al consumatore dei decoder digitali. Gran parte delle considerazioni di seguito riportate sono state recepite dalla recente delibera 216/00 che l'Autorità per le garanzie nelle comunicazioni ha emanato il 5 aprile 2000, dopo aver ottenuto il parere positivo delle Commissione europea e del Ministero delle comunicazioni.

1.4.2 Il decoder unico

La possibilità per gli utenti di fruire del maggior numero possibile di offerte di servizi di televisione numerica tramite un decoder unico si confronta con due realtà di mercato che presentano una dinamica differente :

- il mercato della televisione via satellite e via cavo, che sperimenta un notevole incremento nella vendita dei decoder, grazie soprattutto a una ricca offerta di programmi in chiaro ed a pagamento;
- il mercato della televisione digitale terrestre, che farà il suo debutto commerciale in Italia non prima del prossimo anno (2007-2008).

Nella fase di avviamento del servizio, secondo il Comitato, è necessario prevedere una normativa il più possibile aperta, capace di favorire il servizio stesso senza ostacolare le molteplici possibilità offerte dalla rapida evoluzione tecnologica e in grado di dare stabilità al sistema.
Usufruire dei servizi di televisione digitale con un decoder unico può significare:

- ricevere con lo stesso decoder le offerte dei differenti operatori sia in chiaro sia cifrate;
- ricevere con lo stesso decoder le offerte di televisione digitale (in chiaro e cifrate) su differenti mezzi trasmissivi (cavo, satellite, terrestre).

La prima interpretazione è quella che al momento riveste maggior rilevanza commerciale, essendo l'offerta dei servizi di televisione digitale attualmente limitata al satellite o al cavo. Anche se ancora non sono disponibili moduli multi standard per ricevere con lo stesso decoder la televisione digitale terrestre, via cavo e via satellite, è lecito prevedere che il decoder terrestre, con l'aggiunta di opportuni moduli, sarà compatibile con la ricezione via satellite e/o via cavo. Si ritiene tuttavia, in considerazione dell'elevato costo e dell'attuale assenza sul mercato di questi moduli, che tale ricezione multistandard debba per ora rimanere opzionale.

La ricezione delle offerte dei differenti operatori di *pay-tv* dovrebbe, in un decoder unico ideale, essere possibile semplicemente tramite l'attivazione dell'apposita *smart-card*, in maniera del tutto simile a quanto accade nei servizi di telefonia mobile GSM (*Global Standard for Mobile Telephony*). Il principale ostacolo a questa modalità di funzionamento, alla base del sistema *Eurocrypt*, è costituito dal fatto che tutti i sistemi d'accesso condizionato oggi esistenti in Europa sono proprietari, e ciò essenzialmente in ragione del dilagare del fenomeno delle *smart-card* illecite.
La sicurezza del sistema di cifratura è d'altronde condizione essenziale per il successo commerciale di un operatore di televisione a pagamento. La normativa europea vigente fissa nell'algoritmo comune europeo il sistema obbligatorio di **descrambling** per tutti i ricevitori, ma lascia piena libertà ai fornitori di sistemi di accesso condizionato di elaborare algoritmi proprietari per la protezione delle chiavi di accesso.
La stessa normativa tuttavia obbliga i depositari di algoritmi proprietari a fornire, su licenza, la tecnologia a condizioni eque e non discriminatorie.

1.4.3 I sistemi simulcrypt e multicrypt

Anche nel caso di decoder proprietario, dunque, la tecnologia deve essere accessibile a tutti coloro che ne facciano richiesta. Per consentire all'utente di abbonarsi alle offerte di differenti *providers* esistono attualmente due tecniche distinte, così come stabilite dal DVB:

- **SIMULCRYPT**: nella sua forma più semplice consiste nel trasmettere la stessa offerta digitale cifrata con differenti sistemi d'accesso condizionato.
  A differenza di quanto comunemente ritenuto, il *simulcrypt* non richiede un accordo fra operatori, ma un semplice accordo di licenza fra i fornitori dei sistemi d'accesso condizionato utilizzati e il *broadcaster*. Accordi più complessi possono avvenire per ragioni d'opportunità commerciale, (come ad esempio la condivisione della stessa *smart-card* che dà all'abbonato accesso a servizi differenti).
- **MULTICRYPT** : consiste nell'avere nel decoder uno o più *slot* ad interfaccia comune in grado di ospitare un modulo d'accesso condizionato fornito da un altro *provider*. Il modello *multicrypt* è per il momento scarsamente applicato. Sul totale dei ricevitori circolanti in Europa, solo una minima parte ha uno *slot* d'interfaccia comune, mentre in Italia sono da poco disponibili sul mercato.
  Si potrebbe tuttavia valutare l'opportunità di inserire il *multicrypt* sul mercato della televisione digitale terrestre. Nel caso di televisore con decoder integrato la *slot* ad interfaccia comune è obbligatoria per legge ed il Comitato raccomanda che tutti i *set-top-box* utilizzati per servizi di televisione digitale terrestre a pagamento siano dotati di almeno una *slot* di tale tipo.

Anche se non deve essere sottovalutata l'importanza del *multicrypt*, il *simulcrypt* rappresenta indubbiamente, a breve termine, la soluzione meno onerosa in relazione allo sviluppo del mercato satellitare e al numero assai rilevante di decoder circolanti.

1.5 Standard

1.5.1 Standard trasmissivi

I principali standard usati per la trasmissione della televisione digitale terrestre (3) sono:

- **DVB-T** (in blu nella mappa): è lo standard più diffuso e quello adottato dall'Europa (Italia compresa);
- **ATSC** (in arancione nella mappa): è utilizzato nell'America settentrionale (Canada, Messico e Stati Uniti) ed in Corea del Sud;
- **ISDB-T** (in verde nella mappa): è utilizzato Brasile ed in Giappone;

- **DMB-T** (in rosso nella mappa): è utilizzato in Cina e Hong Kong.

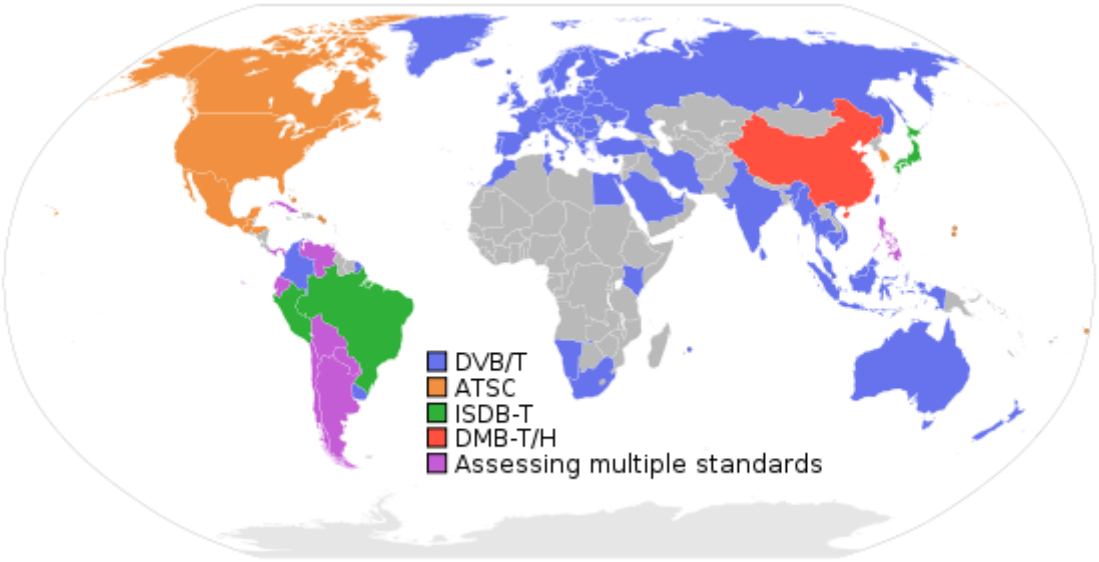


Figura 1 Sono colorati in viola i paesi che adottano più standard.

L'**ATSC**, acronimo di Advanced Television Systems Committee (traduzione letterale: Comitato per i Sistemi Televisivi Avanzati), è un'organizzazione internazionale senza fini di lucro volta allo sviluppo di standard volontari per la televisione digitale. Le organizzazioni membri della ATSC rappresentano le industrie di semiconduttori, satelliti, TV via cavo, computer, elettronica di consumo e sistemi di trasmissione video. In particolare ATSC sta lavorando per coordinare gli standard televisivi tra i differenti mezzi di trasmissione, con particolare attenzione alla televisione digitale, i sistemi interattivi, e le comunicazioni multimediali a larga banda.
Formati supportati dallo standard ATSC:

Linee verticali	Pixel orizzontali	Rapporto d'aspetto	Frequenza di quadro
1080	1920	16:9	60I, 30P e 24P
720	1280	16:9	60P, 30P e 24P
480	704	16:9 e 4:3	60I, 60P, 30P e 24P
480	640	4:3	60I, 60P, 30P e 24P

"I" sta per interlacciato, "P" per Progressive scan.
L’argomento verrà approfondito nel Capitolo 2.

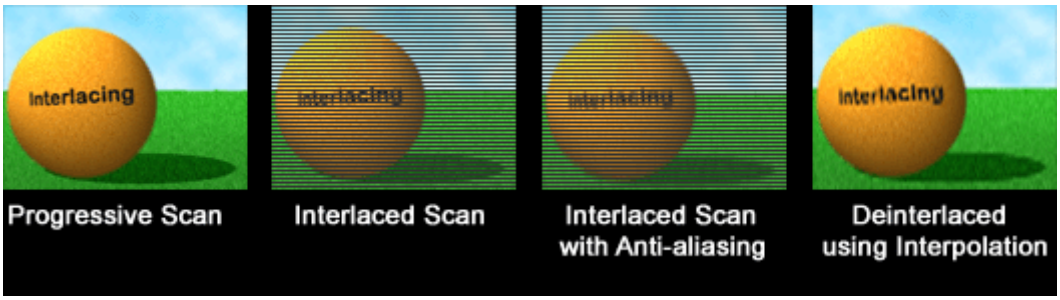


Figura 2 Tipi di frame

1.5.2 Standard interattivi

Gli standard interattivi si aggiungono a quelli trasmissivi per fornire servizi aggiuntivi, i più noti sono:

- **MHP**: è basato sul linguaggio di programmazione Java ed esiste in due versioni, DVB-HTML (poco fortunato perché molto complesso) e DVB-J; sviluppato inizialmente soprattutto in Italia ed in Corea è oggi impiegato anche in numerosi altri paesi;
- **MHEG-5**; è una parte di un insieme di standard internazionali relativi alla presentazioni di informazioni multimediali; si tratta di un linguaggio di programmazione adatto a chioschi multimediali e servizi televisivi interattivi, standardizzato dal Multimedia and Hypermedia Experts Group (MHEG). Un'applicazione MHEG-5 consiste in un insieme di scene fra cui l'utente si può muovere, ogni scena contiene degli elementi grafici (testo, immagini e video) e blocchi di codice. Tale codice permette l'esecuzione di azioni elementari

L'implementazione di questi standard nei sintonizzatori è opzionale: i modelli più economici, proprio per ragioni di costi, spesso non li supportano, permettendo quindi di ricevere correttamente le trasmissioni televisive ma non consentendo l'uso di servizi interattivi. È da notare che questi standard devono essere in primo luogo adottati dalle emittenti, altrimenti gli utenti non possono in ogni caso trarne beneficio.

1.5.3 Codifiche video

Nella maggior parte dei paesi la codifica video è effettuata secondo lo standard MPEG-2 (Moving Pictures Experts Group), ma il più efficiente standard H.264 (conosciuto anche come MPEG-4 AVC) ha cominciato ad essere popolare ove il lancio della televisione digitale è stato più recente. Alcuni paesi adottano entrambi gli standard: in Francia, per esempio, MPEG-2 è usato per le trasmissioni gratuite mentre H.264 è impiegato per trasmissioni a pagamento e in alta definizione.

CAPITOLO 2

2.1 Introduzione

In questo capitolo parleremo nella prima parte delle tecniche di compressione adottate nel DVB ovvero l'algoritmo di compressione MPEG e lo sviluppo che ha avuto col passare degli anni in seguito allo sviluppo della tecnologia DVB.

2.2 Tecniche di Compressione

2.2.1 L'algoritmo MPEG

Nel 1990, il bisogno di conservare e riprodurre immagini e suoni in movimento in formato digitale per applicazioni multimediali. Lo standard mpeg-1 consiste di tre parti distinte, pubblicate nel novembre del 1992:

- MPEG-1 system (ISO/IEC 11172-1) definisce la struttura Mpeg-1;
- MPEG-1 video (ISO/IEC 13818-2) definisce la codifica video Mpeg-2;
- MPEG-1 audio (ISO/IEC 13818-3) definisce la codifica audio per Mpeg-2.

Comunque, la qualità di immagine di MPEG-1 non era appropriata per applicazioni di largo-getto, fin da, fra le altre cose, si sta avendo un'evoluzione verso HDTV. Questo standard internazionale è noto come MPEG -2.

Come suo predecessore, MPEG-2 è specificato in tre parti distinte, pubblicato a novembre 1994:

- Sistema di MPEG-2 (ISO / IEC 13818 -1): definisce il flusso MPEG-2 ;
- Video di MPEG-2 (ISO / IEC 13818 -2): definisce la codificazione di video di MPEG-2;
- MPEG-2 audio (ISO / IEC 13818 -3): definisce l'audio di MPEG-2.

MPEG-2 è, fra le altre cose, la fonte che programma standard usata dalla TV di DVB (Radiodiffusione di Video Digitale) europea sistema che è il risultato del lavoro cominciato nel 1991 dall'ELG (Gruppo del Varo dell'europeo), in un secondo tempo divenire il comitato di DVB.

2.2.1.1 Mpeg-1

L'obiettivo principale per MPEG-1 era arrivare a un video di qualità di supporto con una bit-rate totale e costante di 1.5 Mb/s per conservare video ed audio su CD-ROM. La parte usata dal video è di 1.15 Mb/s, il rimanere 350kb/s essendo usato per audio e dati supplementari richiesti dal sistema per le altre informazioni. Comunque, la specificazione di MPEG-1 è molto flessibile e permette a parametri diversi di essere scelti dalla transazione tra la complessità di codifica, percentuale di compressione, e qualità.
Il codifica video utilizza gli stessi principi come lossy JPEG al quale tecniche nuove sono aggiunte per formare la "casella degli strumenti" di MPEG-1; queste tecniche sfruttano la correlazione forte tra immagini successive per ridurre notevolmente la somma di information richiesta per trasmetterli o conservarli. Queste tecniche, noto come "predizione con compensazione di movimento" consistono di dedurre la maggior parte di immagini con una sequenza dalla precedente e dalle successive, con un minimo di informazioni supplementare che rappresenta le differenze tra le immagini. Questo richiede la presenza nel codificatore di MPEG di un encoder estimatore di movimento che è la funzione più

complessa e determina il rendimento del codificatore; fortunatamente, questa funzione non è richiesta nel decodificatore.

2.2.1.2 Mpeg-2

MPEG-2 è uno standard introdotto nel 1994 da MPEG (Moving Pictures Experts Group). È un sistema di codifica digitale, definisce la codifica di sorgente audio, video, e il formato di multiplazione e trasporto per servizi multimediali diffusivi a qualità televisiva o superiore.
MPEG-2 è stato destinato al broadcast televisivo, fin dalla sua introduzione nel 1994. Una efficiente codifica per il video interlacciato e la scalabilità sono state le caratteristiche che hanno permesso di digitalizzare efficacemente i segnali televisivi. Grazie all'MPEG-2 si ottengono immagini televisive di buona qualità con bitrate compresi tra 4 e 9 Mbit/s
MPEG-2 è costituito da "profili" e "livelli". I *profili* definiscono la modalità di compressione utilizzata e stabiliscono di fatto il compromesso tra tasso di compressione e costo del decodificatore. I *livelli* definiscono la risoluzione di immagine ed il bitrate massimo da associare ad ogni profilo. Ci sono complessivamente 4 livelli e 5 profili le cui caratteristiche sono descritte in seguito. La combinazione attualmente utilizzata dalle trasmissioni digitali per ricezione diretta impiega il cosiddetto "main level @ main profile" (MP@ML).

Lo standard MPEG-2 utilizza tecniche di compressione basate sulla riduzione della ridondanza spaziale e temporale della sequenza video. La ridondanza spaziale è ridotta tramite tecniche a trasformata (*DCT, Discrete Cosine Transform*), quella temporale è ridotta tramite motocompensazione: tale metodologia prende il nome di tecnica ibrida a trasformata.

Lo standard definisce tre tipi di quadri:

- immagini codificate senza riferimento ad altre immagini (quadri Intra): sono dei punti di accesso alla sequenza codificata, in corrispondenza dei quali può iniziare la decodifica; sono caratterizzate da un modesto rapporto di compressione.
- immagini codificate mediante motocompensazione del movimento da immagini precedenti (quadri P): usate come riferimento ad altre predizioni.
- immagini codificate mediante motocompensazione bidirezionale (quadri B): offrono il maggior livello di compressione, non sono usate come riferimento per altre predizioni.

La codifica opera suddividendo l'immagine in blocchi 16x16, detti macroblocchi. Tutti i macroblocchi di un quadro I sono codificati senza predizione. Ciascun macroblocco di un quadro P può essere predetto a partire da un quadro I o P precedente (macroblocco P), oppure può essere codificato senza predizione (macroblocco di tipo I). Ciascun macroblocco di un quadro B può essere predetto bidirezionalmente rispetto al quadro I o P precedente e al quadro I o P successivo (macroblocco B), ovvero predetto rispetto al quadro I o P precedente (macroblocco P), oppure codificato senza predizione (macroblocco I).

Per macroblocchi I, si codifica il macroblocco mediante applicazione DCT e quantizzazione ai blocchi 8x8 componenti. Per macroblocchi P, si effettua la motocompensazione del macroblocco 16x16; la differenza tra la predizione e il blocco attuale, detta residuo di motocompensazione, è codificata mediante DCT e quantizzata su blocchi 8x8 pixel. Per macroblocchi B, si effettua la motocompensazione del macroblocco 16x16 rispetto al quadro di riferimento precedente e al quadro di riferimento successivo; la predizione è operata

mediando i due blocchi 16x16 così ottenuti; la differenza fra il macroblocco attuale e la predizione, detto residuo di motocompensazione è codificata mediante DCT e quantizzata su blocchi 8x8 pixel.

Il modo di codifica di ciascun macroblocco dei quadri P o B è scelto in modo da minimizzare il numero di bit richiesti per descriverlo. Poiché i vettori di moto di macroblocchi adiacenti sono correlati, sono codificati in modo differenziale rispetto al vettore di moto del precedente macroblocco adiacente. La quantizzazione comporta una perdita irreversibile di informazione ed è adattata alle caratteristiche dell'apparato visivo umano, mediante la scelta di opportune matrici di quantizzazione. Le matrici di quantizzazione possono variare da un'immagine ad un'altra e sono trasmesse all'inizio di ogni immagine; inoltre la matrice di quantizzazione può essere scalata da macroblocco a macroblocco mediante un fattore di scala (*quantizer_scale*), al fine di adattare la precisione della codifica dell'immagine al suo contenuto. Il quantizer_scale può essere maggiore, minore o uguale a 1, e codificato con un valore a 5 bit, con scala lineare o non.

I quadri della sequenza sono raggruppati in Group of Picture (GOP), il cui primo quadro è di tipo I. Tale organizzazione dei dati codificati consente la sincronizzazione del decoder con un ritardo al più pari alla durata del Gop.

L'efficienza di compressione varia in funzione delle caratteristiche locali del segnale video, di conseguenza il bit stream all'uscita del codificatore video è a bit rate variabile. Il canale ha invece tipicamente capacità costante, allora si usa un buffer tra canale e codificatore. Lo stato di riempimento del buffer è utilizzato per controllare il processo di codifica (quantizzazione, inserimento dei quadri predetti), al fine di evitare fenomeni di buffer overflow o di buffer underflow.
In un sistema MPEG-2 codificatore e decodificatore possiedono un buffer di comportamento simmetrico. Il buffer del codificatore è riempito a burst quando le immagini vengono codificate, e svuotato a velocità costante durante la trasmissione. Il buffer del decodificatore è riempito a velocità costante quando i dati vengono ricevuti e svuotato a burst durante il playout. Lo standard MPEG-2 definisce un modello ideale di decodificatore (*Video Buffering Verifier*, VBV), da utilizzarsi per limitare il bit rate istantaneo del codificatore, in modo che il bit rate medio sia tale da non far incorrere nell'overflow o nell'underflow del buffer del decoder. Il VBV è identificato a parametri del bit rate (misurato in unità di 400 bit/s), picture-rate, vbv_buffer_size (misurato in unità di 2048 Byte), vbv_delay (che definisce il tempo che intercorre tra la ricezione del primo bit di dati della prima immagine nel buffer e la decodifica dei dati stessi, misurato rispetto ad un clock a 90 KHz).

Descriviamo sinteticamente le caratteristiche dei livelli e dei profili dell'MPEG-2 che rappresentano la forza del sistema in quanto a flessibilità e adattabilità a varie applicazioni. È sorprendente come MPEG-2 riesca a spaziare tra la più bassa risoluzione di immagine SIF fino all'alta definizione HDTV semplicemente variando le associazioni tra livelli e profili. I livelli previsti sono:

- low (basso), corrisponde alla risoluzione più bassa come la SIF utilizzata nell'MPEG-1;
- main (principale), corrisponde alla struttura 4:2:0 fino ad una risoluzione di 720 x 576 pixel;
- high-1440 (alto-1440), dedicato alla tv ad alta definizione HDTV;

- high (alto), ottimizzato per il formato di schermo 16/9 in alta definizione.

La descrizione dei profili è invece un po' meno semplice di quella dei livelli in quanto implica la conoscenza delle metodologie di base con cui opera il sistema MPEG; questa è una sintesi riferita agli effetti dell'applicazione dei vari profili.

- Il profilo “simple” permette di semplificare notevolmente sia il codificatore di stazione che il decodificatore di utente in quanto non utilizza la predizione di tipo B.
- Il profilo “main” è quello che offre il miglior compromesso tra qualità e tasso di compressione, impiega le immagini relative alle predizioni I, P, B a svantaggio dei dispositivi di codifica e decodifica che sono più complessi.
- Il profilo “scalable” è destinato ad applicazioni particolari dove sia necessario ad esempio mantenere la compatibilità tra alta definizione e definizione standard oppure, riuscire ad ottenere una qualità accettabile in condizioni di ricezione difficile come potrebbe accadere ad esempio nella televisione digitale terrestre.
- Il profilo più elevato “high” è destinato all'alta definizione con le strutture 4:2:0 e 4:2:2.

I profili mantengono una certa compatibilità verso l'alto nel senso che, nella fase di ricezione, i profili più alti possono decodificare i profili inferiori.

Per maggiori dettagli si consiglia la visione della tesi (4) e la lettura dei libri (5) (6).

2.2.2 Dettagli codifiche video

Al contrario, **MPEG** è uno standard definito che consente lo scambio tra dati compressi da sistemi diversi. La differenza principale è individuabile nelle tecniche di analisi e compressione dei dati. MPEG analizza l'intera sequenza di fotogrammi (compressione interframe). I singoli frame di queste sequenze possono essere di tipo I, B e P e sono raccolti in gruppi chiamati **GOP** (Group of Pictures). Un GOP deve includere almeno un frame di tipo I mentre la lunghezza e la struttura della sequenza può essere liberamente definita dal produttore.
I frame di tipo I sono immagini di riferimento e vengono compresse individualmente. Ogni area all'interno di un frame può essere compressa a fattori differenti; ad esempio, al centro può essere utilizzato un fattore inferiore rispetto ai bordi, con un risparmio di un 15% nel flusso di dati senza perdita visibile di qualità. Nel flusso di dati MPEG, i frame I contengono tutte le informazioni necessarie alla decompressione e visualizzazione dell'immagine compressa.
I frame di tipo *B* sono immagini compresse in modo bidirezionale e contengono solo i dati relativi alle differenze tra altri due frame. I frame B- contengono un numero di dati molto inferiore rispetto ai frame I. L'inconveniente è che per decomprimere e visualizzare un frame B è necessario fare riferimento ai frame precedente e successivo.
I frame di tipo *P* sono detti *predicted.* Sono ottenuti mediante interpolazione di altri frame della sequenza e contengono ancora meno dati dei frame B.
La composizione dei GOP e la quantità di frame dei vari tipi I, B e P dipende dal produttore. L'unico requisito indispensabile è la presenza di almeno un frame di tipo I.

2.2.2.1 Video

Il Segnale Video Analogico è un sistema caratterizzato dai seguenti requisiti: 25 frame al secondo, 625 linee per ogni frame e 720 pixel per ogni linea.
La digitalizzazione del Segnale Video Analogico è ottenuta grazie al campionamento di ogni singola immagine, alla quantizzazione dei valori campionati ed alla codifica dei quanti; l'immagine digitale si può quindi vedere come una matrice di punti, pixel, ognuno dei quali sarà descritto da tre componenti rappresentanti le componenti del colore. Adesso introdurremo i concetti di luminanza e crominanza sui quali si basano le tecniche di compressione dell'immagini utilizzate nell'Mpeg-2, vedremo i principi di codifica e la divisione che si fa per livelli dell'immagine.

2.2.2.2 Luminanza e Crominanza

Come detto in precedenza ad ogni pixel vengono assegnate tre componenti rappresentanti le informazioni relative al colore. Mentre lo spazio colori RGB è la scelta ottimale per la grafica su calcolatore, questo spazio non è efficiente nella rappresentazione di immagini reali. Questo poiché molte ricerche sul modello fisiologico della visione umana hanno evidenziato che l'occhio è meno sensibile alla componente colore rispetto a quella di luminanza. Quindi vengono usate le coordinate YUV, derivate dalle RGB attraverso una combinazione lineare, che concentrano più informazione nella componente della luminanza rispetto alle componenti del colore.
In queste coordinate Y rappresenta la componente relativa alla luminanza, ovvero la luminosità di un punto, mentre U e V rappresentano l'informazione cromatica, cioè la tonalità del colore.
Le componenti Y, Cb e Cr sono invece l'equivalente digitale delle componenti Y, U e V ottenute scalando e modificando l'offset di quest'ultime in modo da concentrare una maggiore quantità di informazione nella componente relativa alla luminosità. Le componenti di crominanza risultano inoltre meno correlate così da poterle codificare separatamente. Le stesse ricerche mostrano inoltre che l'occhio è poco sensibile anche alle rapide variazioni cromatiche ed è per questo motivo che le componenti di crominanza Cb e Cr vengono sotto campionate rispetto alle componenti di luminanza Y.
Si avranno diversi tipi di sottocampionamento, come si può notare dalla figura di sotto, a seconda della qualità desiderata. Il sottocampionamento può avvenire in entrambe le direzioni o in una sola direzione.

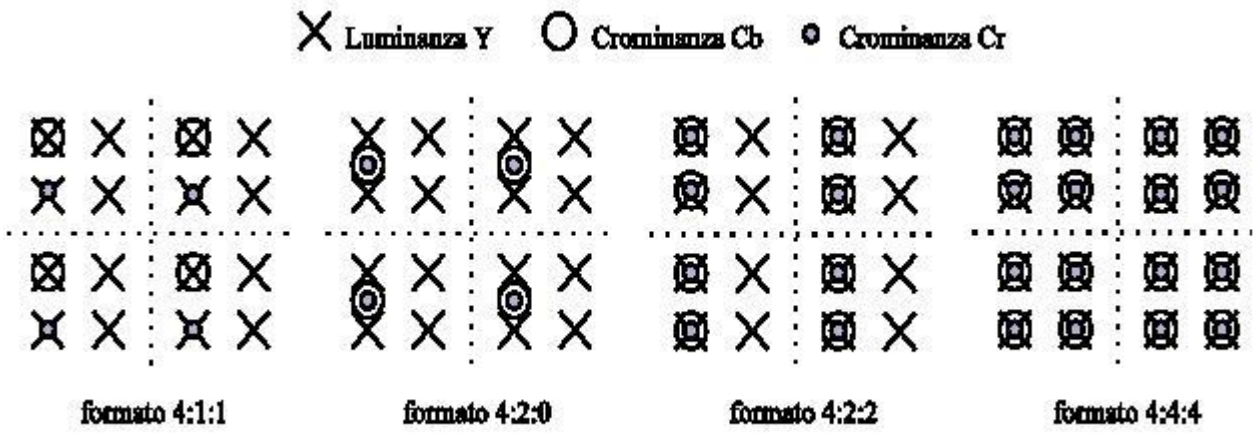


Figura 3 Schema esemplificativo dei possibili formati

Considerando le immagini della figura sopra, ognuna composta da 4x4 pixel, se dividiamo ancora queste immagini in quattro quadranti di dimensioni 2x2 pixel possiamo analizzare i seguenti tipi di sottocampionamento (da sinistra a destra):

- 4:1:1 - In effetti in ogni singolo quadrante, come possiamo vedere dalla figura, avrò 4 pixel che campionerò nel modo seguente: 4 componenti per la Luminanza cioè uno per ogni pixel, 1 componente per la Crominanza Cb ed 1 componente per la Crominanza Cr. In parole povere su 4 pixel di ognuno mi prendo la componente di luminanza inoltre per uno mi prendo quella di Crominanza Cb e per un'altro mi prendo la componente di Crominanza Cr. La scelta di questi ultimi è fatta prendendo due pixel in posizione verticale.
- 4:2:0 - Come possiamo vedere dalla figura, per ogni quadrante su 4 pixel prendo 4 componenti per la Luminanza cioè uno per pixel, 1 componente per la Crominanza Cb e 1 componente per la Crominanza Cr, solo che le componenti Cb e Cr non li prendo come pixel singoli, ma a cavallo fra due pixel sulla direzione verticale. In pratica per ogni singolo pixel, su i 4 del quadrante, calcolo la singola componente di Luminanza e i campioni delle componenti Cb e Cr li calcolo a cavallo di una coppia di pixel verticali. Questa particolare scelta esce dalla logica che guida gli altri formati, infatti i realizzatori invece di chiamarlo eventualmente formato 4:1:1 bis l'hanno chiamato 4:2:0.
- 4:2:2 - Come possiamo vedere dalla figura, per ogni quadrante su 4 pixel prendo 4 componenti per la Luminanza cioè uno per pixel, 2 componente per la Crominanza Cb e 2 componente per la Crominanza Cr, in questo caso a differenza di quello di prima i due campioni non sono presi a cavallo ma come singoli pixel. Quindi avremo 4 componenti per la Luminanza, 2 per la Crominanza Cb e 2 per la Crominanza Cr.
- 4:4:4 - Questo è considerato il campionamento normale, ovvero nel quadrante composto da 4 pixel prenderò 4 componenti per la Luminanza, 4 per la Crominanza Cb e 4 per la Crominanza Cr.

Per precisione ricordiamo che nell'YUV standard PAL per poter convertire, i tre vettori RGB in YUV si applicano le seguenti equazioni:

$$Y = 0.299\,R + 0.587\,G + 0.114\,B$$
$$U = 0.492\,(B - Y)$$
$$V = 0.877\,(R - Y)$$

2.2.3 DVB – frame video

Qui di seguito sono elencate le diverse risoluzioni ottenibili con la SDTV (televisione a definizione standard) e HDTV (televisione ad alta definizione)

Risoluzioni applicabili per SDTV:

- 720, 640, 544, 480 or 352 × 480 pixel, 24/1.001, 24, 30/1.001 or 30 frame/s
- 352 × 240 pixel, 24/1.001, 24, 30/1.001 or 30 frame/s
- 720, 704, 544, 480 or 352 × 576 pixel, 25 frame/s
- 352 × 288 pixel, 25 frame/s

Per HDTV:

- 720 x 576 x 50 frame/s progressive (576p50)
- 1280 x 720 x 25 or 50 frame/s progressive (720p50)
- 1440 or 1920 x 1080 x 25 frame/s progressive (1080p25 – film mode)

- 1440 or 1920 x 1080 x 25 frame/s interlace (1080i25)
- 1920 x 1080 x 50 frame/s progressive (1080p50) possible future H.264/AVC format

CAPITOLO 3

3.1 Introduzione

In questo capitolo parleremo degli standard DVB, daremo una definizione generale sullo schema di funzionamento della trasmissione che avviene nel DVB dall'invio del segnale della sorgente con la tecnica dello Scrambling e le successive fasi da parte del trasmittente e la ricezione di questo segnale dal ricevente che con la tecnica del Descrambling estrapola dal segnale le fonti (video/audio/data) necessarie per visualizzarle. Verranno analizzate le prestazioni e le capacità trasmissive del DVB. L'uso di reti di diffusione in isofrequenza, che permettono la trasmissione sulla stessa frequenza con gli stessi programmi (programmi tv) che servono diverse zone contemporaneamente senza creare interferenze. Verrà dato un accenno del sistema DVB-S sulla diffusione dei segnali numerici TV da satellite, cosi come verrà fatto per il DVB-IP che riguarda la diffusione dei dati via satellite. Verrà visto il sistema DVB-MHP implementato nei sistemi DVB che rende la televisione digitale non solo come uno strumento di trasmissione video, ma permettendo all'utente un interazione con i programmi (es. giocare, navigare, ect.).

3.2 Gli standard DVB

Un satellite generalmente è formato dai seguenti sottosistemi:

- pannelli solari e accumulatori per l'alimentazione degli apparati
- un sistema di antenne per ricevere e trasmettere il segnale
- un sistema di stabilizzazione per garantire il puntamento delle antenne nella giusta direzione
- un sistema di telemetria per la trasmissione dei dati riguardanti la posizione del satellite
- un sistema di comando per correggerne da terra l'orbita o la posizione.

Un satellite, quindi, è un ripetitore: riceve un segnale da un punto sulla terra e lo ritrasmette in un altro.
Il collegamento da terra verso il satellite è detto UP-LINK, mentre quello dal satellite verso terra DOWN-LINK.

1991	European Launching Group formed
September 1993	DVB founded with 80 members
November 1993	MPEG-2 (ISO/IEC 13818-2) approved by ISO
December 1993	DVB-S approved (EN 300 421)
1994	DVB registers DVB logo
March 1994	DVB-C approved (EN 300 429)
May 1994	DVB Common Scrambling Algorithm approved
September 1994	DVB approves Conditional Access Package
September 1994	DVB membership reaches 147
November 1994	ITU recommends DVB-S for digital satellite television.
March 1995	DVB-CI specification (Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications) (EN 50221)
March 1995	DVB forms Interactive Services Commercial Module to work on interactive services for the first time
December 1995	DVB-T approved (EN 300 744)
April 1996	First DVB-T trial transmissions on air in UK
April 1996	First demonstration of DVB-S interoperability
1996	Theo Peek (Philips) becomes DVB Chairman
1996	DVB-S (Specification for delivery of DVB services via digital satellite)
1996	DVB-C (Specification for framing structure, channel coding and modulation for digital cable systems)
1996	DVB's Memorandum of Understanding revised and restated to include Interactivity
April 1997	DVB membership grows to 207
April 1997	DVB agrees to incorporate HDTV elements in its specifications
April 1997	DVB approves SimulCrypt specification (TS 101 197-1)
April 1997	DVB approves data broadcasting specification (EN 301 192)
June 1997	Joint demonstration of terrestrial HDTV from ATSC and DVB (Montreux ITVS '97)
July 1997	DVB approves implementation guidelines for HDTV services
1997	Canal+ launch first DVB-C digital cable services in US
December 1997	DVB demonstrates terrestrial HDTV in Australia
December 1997	DVB approves MHP functional requirements
May 1998	Internet of air demonstrations using DVB-S in Africa
June 1998	DVB-T trials in Singapore
18 June 1998	Australia adopts DVB-T
15 November 1998	UK launches worlds first digital terrestrial television service with DVB-T
1 April 1999	Swedish digital terrestrial television launched
13 April 1999	DVB opens cooperation with China for development of digital terrestrial television
19 April 1999	DVB demonstrate mobile digital terrestrial television at NAB
25 May 1999	Singapore adopt DVB for digital terrestrial broadcasting
19 July 1999	India adopts DVB-T
September 1999	DVB demonstrates mobile TV on No. 4 trams in Amsterdam
9 November 1999	DVB Steering Board announce agreement on principles of MHP
14 February 2000	Field trials in Brasil confirm superiority of COFDM
March 2000	DVB launches MHP logo
10 April 2000	Worlds First with demonstration of simultaneous reception of mobile SDTV and fixed HDTV using its Hierarchical Modulation technology in US at NAB
May 2000	Argentina reconsiders 1998 adoption of ATSC
May 2000	Spanish digital terrestrial television launched
May 2000	DVB approves MHP (ES 201 812)

8 September 2000	Multimedia Home Platform (MHP) for interactivity launched at IBC
1 December 2000	Information Technology and Broadcasting Bureau (ITBB) of the Hong Kong Special Administrative Region Government recommends DVB-T
December 2000	DVB begins to discuss work on hand held devices planting seed for DVB-H
December 2000	Demonstrations of DVB-T hierarchical modulation in Brasilia, Brazil
December 2000	DVB SB approves new vision embracing internet and mobile technology, paving the way for DVB 2.0
1 January 2001	Australia launches digital services with DVB-T
31 January 2001	Russian cities of Moscow, Nizhy Novgorod and St. Petersburg launch trial DVB-T services
6 February 2001	DVB launches MHP WWW site
14 February 2001	DVB-RCS, return channel specification for satellite adopted
March 2001	UK government launched digital terrestrial awareness programme based on DVB logo
June 2001	MHP conformance and licensing arrangements approved by DVB Steering Board
8 June 2001	DVB wins prestigious Multichannel News International Ground Breaker Award for Technology in America
July 2001	Taiwan chooses DVB-T, reversing decision in 1997 for ATSC
3 September 2001	DVB launched patent pool co-ordination process for MHP
10 October 2001	US CableLabs adopts MHP
7 November 2001	Australia adopt MHP
November 2001	Finland launches DVB-T with MHP
May 2002	QuieroTV fails in Spain
3 July 2002	MHP Test Suite Approved
13 September 2002	MHP Test Suites begin to ship
7 April 2003	DVB-GEM (Globally Executable MHP) announced as a specification
4 August 2003	Berlin completes switch over from analogue to digital terrestrial transmission

Figura 4 Le tappe più significative del DVB

3.3 Schema di funzionamento generico DVB

Lo schema generico, si compone delle seguenti fasi(per ulteriori approfondimenti si veda (7)):

- **Scrambling**: è la creazione del segnale da trasmettere. L'emittente, in questa fase trasforma il segnale da analogico a digitale comprime il flusso dati tramite le specifiche Mpeg-2, ed eventualmente nel caso delle Pay-Tv lo codifica mediante algoritmi specifici.

- **Uplink e Downlink**: l'Uplink è l'invio del segnale al satellite. L'emittente invia il segnale al satellite che è situato ad un altezza di circa 36.000 Km, questo nella fase di DownLink si limita a rinviare il segnale a terra verso frequenze comprese nell'intervallo che va da 10.700Mhz a 12750Mhz.
- **Descrambling**: Una volta giunto a terra il segnale, catturato da un antenna parabolica tramite un cavo coassiale arriva ad un sistema ricevente (IRD) modulato in intervalli compresi tra i 950Mhz e i 2150Mhz. Il sistema ricevente (IRD) dovrà effettuare la decodifica del segnale ricevuto se cifrato, la decodifica Mpeg-2 del flusso audio/video e la trasformazione del segnale da digitale ad analogico da inviare alla televisione.

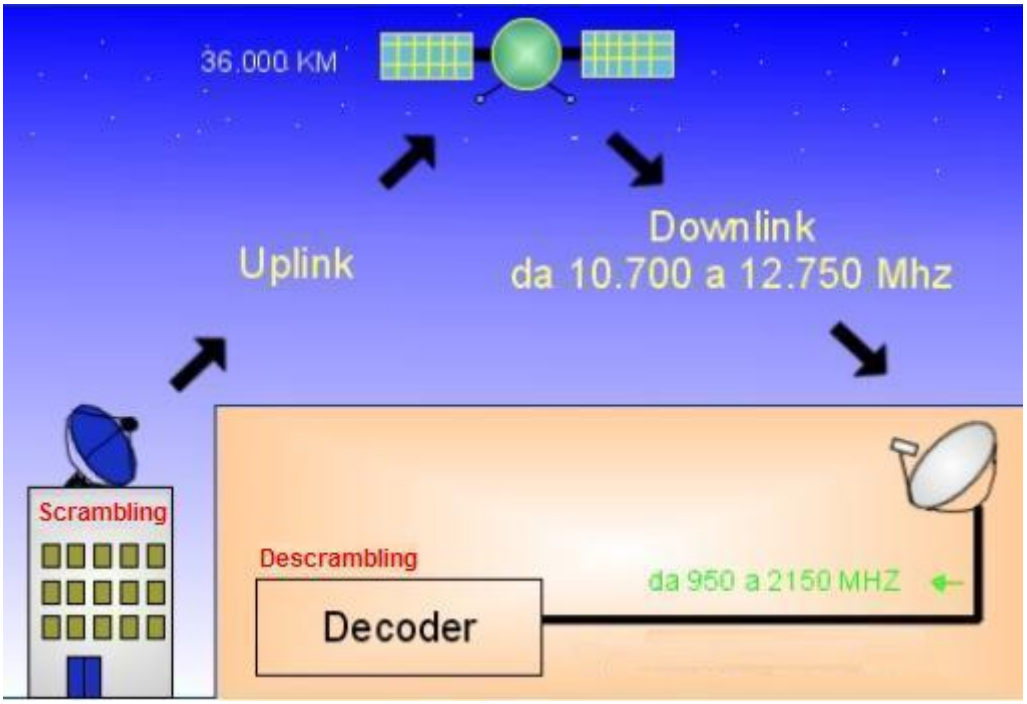


Figura 5 Schema generico di trasmissione

3.3.1 Scrambling

Lo scrambling, è la prima fase di una trasmissione satellitare. In questa fase l'emittente deve trasformare il segnale video/audio da trasmettere da analogico in digitale. Nella fase di Scrambling entrano in gioco i seguenti componenti aventi le seguenti specifiche:

- **ADC**: Convertitore Analogico-Digitale, se ne usano due, uno per il flusso video operante ad 8Bit di Luminanza e 8Bit di Crominanza ed uno per il flusso audio a 16Bit. Discuteremo queste tecniche in dettaglio nella sezione dedicata agli Standard DVB, per il momento ci basta sapere che saranno gli ADC ad occuparsi della conversione dei segnali analogici in sequenze binarie.
- **CODIFICATORE MPEG2**: Comprime il flusso digitale in pacchetti MPEG-2, anche questo per il momento lo immaginiamo come una scatola chiusa e rinviamo tutti i dettagli inerenti alla sezione dedicata allo Standard Mpeg-2. Per il momento assumiamo che questa scatola si occupi della compressione del segnale audio/video digitale.
- **CIFRATORE**: Codifica i pacchetti secondo specifici algoritmi, questa tecnica è solo usata da quelle emittenti televisive satellitari a pagamento, e quindi per una questione di sicurezza e per politiche di gestione degli accessi preferiscono cifrare il

segnale trasmesso. In questo testo si parlerà del sistema Irdeto e accennati altri sistemi attuali di crittografia quali SECA e NDS.

- **CROSS-INTERLEAVER**: Aggiunge bit di ridondanza per la correzione degli errori. Essendo una trasmissione broadcast, non è possibile dopo il riscontro di un errore da parte del decoder richiedere il pacchetto corrotto. Perciò si aggiungono informazioni ridondanti per assicurare l'integrità dei dati spediti.
- **MULTIPLEXER**: Invia all'unica uscita, a turno, ognuno dei flussi presenti nelle molte entrate (*TDM: multiplazione a divisione di tempo*). La multiplazione può essere di tipo deterministico, cioè una banda prestabilita per ogni canale, o di tipo statistico e quindi con una banda allocata dinamicamente per ogni canale in funzione della complessità delle immagini. All'interno del multiplexer può formarsi una coda di tipo FIFO.
- **MODULATORE QPSK (Quadrature phase-shift keying)**: Modulatore di fase e ampiezza a 4 stadi di una portante armonica e una modulante digitale, serve per modulare il segnale in modo da adattarlo al mezzo trasmissivo.

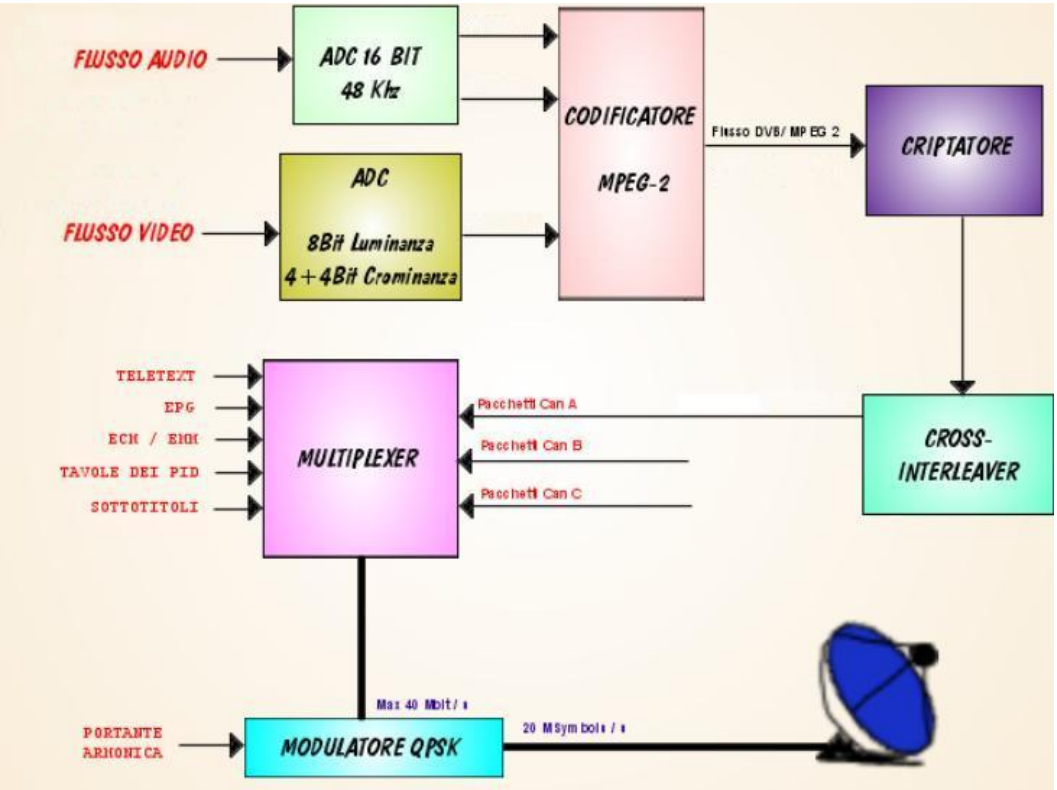


Figura 6 Schema che illustra la fase di scrambling

Durante lo *Scrambling* del segnale vengono eseguiti i seguenti passi:

1. I flussi analogici video e audio, vengono digitalizzati, cioè vengono convertiti in una sequenza di 0 e 1 tramite i convertitori "ADC" Convertitori da analogico a digitale.
2. Vengono compressi con l'algoritmo Mpeg-2, nel "CODIFICATORE MPEG-2", che abbiamo visto nel Capitolo 2.
3. Se necessario vengono cifrati nel "CIFRATORE"
4. Poi vengono aggiunti i bit di ridondanza per la correzione dell'errore nel "CROSS-INTERLEAVER"

5. A questo punto viene effettuato il multiplexing dei vari flussi dati nel “MULTIPLEXER”
6. In fine il segnale viene modulato in fase ed in ampiezza nel “MODULATORE QPSK” e passato alla parabola per poter essere inviato al satellite.

Alla fine dell'intero processo il segnale arriva alla parabola/antenna pronto per essere trasmesso al satellite, quindi passiamo alla seconda fase del processo generico di trasmissione chiamata Uplink/Downlink nella quale il segnale arriva al satellite che lo ritrasmette sulla terra. Questa fase sarà analizzata nella pagina seguente.

Il flusso uscente dalla fase di Scrambling è sotto forma digitale, la sua organizzazione logica, che segue lo standard dettato dall'Mpeg-2 (che vedremo in dettaglio nella prossima sezione), lo vede pronto per una comunicazione di pacchetto. Infatti dopo la fase dello scrambling, ogni pacchetto dati di tipo TPS (Transport Packet Stream) avrà una lunghezza totale di 188 byte.

Ritornando ai pacchetti TPS, questi sono organizzati nei seguenti campi:

- **SYNC**: Un byte usato per il sincronismo degli stessi TPS. Insieme al PID compone l'header del pacchetto.
- **PID**: Pachet Identifier, serve per identificare le informazioni trasmesse, è composto da tre bytes di prefisso dei quali solitamente solo i 2 byte meno significativi vengono utilizzati.
- **PAYLOAD**: 184 bytes detti bytes utili o data, è in questi bytes che risiedono le informazioni audio o video trasmesse.

SYNC 1 byte	**PID** 3 bytes	**PAYLOAD** 184 bytes

Ogni pacchetto quindi, secondo lo standard DVB/MPEG-2 è identificabile per mezzo del suo PID. Il valore del PID di ogni pacchetto del TPS viene deciso dall'emittente.
Tutto questo è stabilito nel documento DVB-S (lo standard dettato dal consorzio DVB per il Satellite che vedremo in dettaglio più avanti).

I provider, come possiamo vedere dalla figura a lato, inviano in uplink al satellite che si trova ad una quota di 36.000Km questi pacchetti. Solitamente questi pacchetti non si riferiscono ad un solo canale televisivo, infatti nella fase dello Scrambling come abbiamo già visto vengono multiplexati insieme più canali al fine di utilizzare tutta la banda.

Il satellite trasla verso le frequenze di Downing il segnale armonico modulato in fase, cambia se necessario la sua polarizzazione e lo ritrasmette verso terra a frequenze comprese nell'intervallo che va da 10.700Mhz a 12750Mhz.

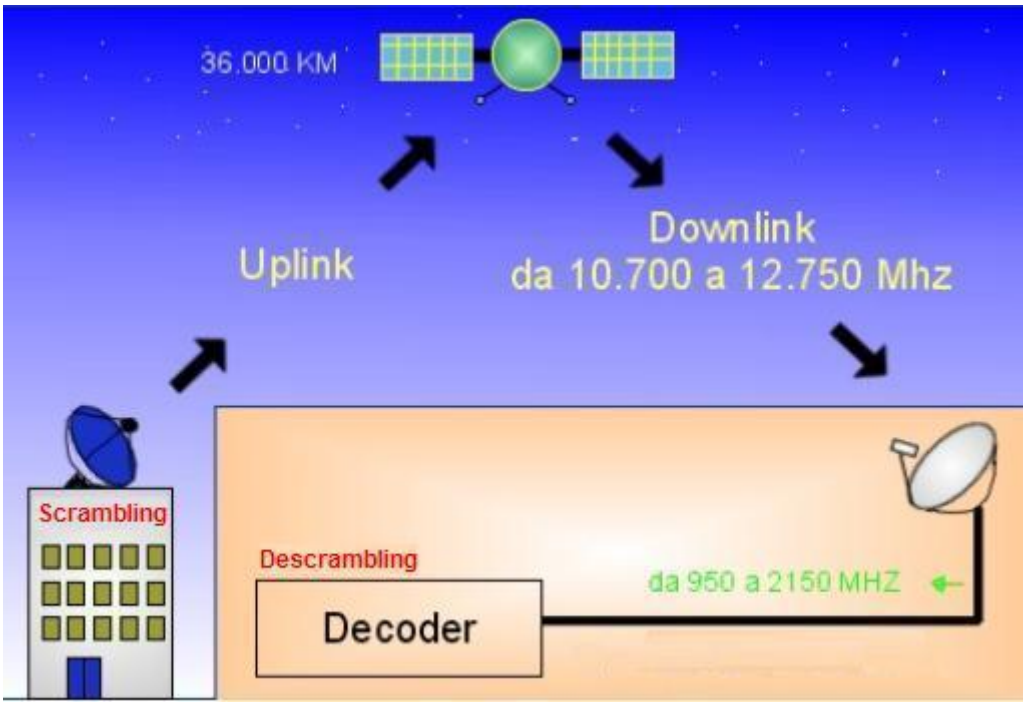


Figura 7 Schema generico di trasmissione satellitare nelle sue tre fasi: Scramling, Uplink e Downlink, Descrambling

A terra le antenne paraboliche che catturano il segnale lo convertono in frequenze comprese tra i 950 ed i 2150Mhz che tramite un cavo coassiale giungeranno ad un sistema ricevente detto (IRD). Il sistema ricevente satellitare detto, discusso da noi nella prossima pagina, si preoccuperà di effettuare la fase inversa allo Scrambling cioè il Descrambling, cioè di ricostruire il segnale audio/video ricevuto sotto forma di pacchetti TPS ottenendo un flusso analogico che l'utente potrà vedere sul propino televisore.

3.3.2 Descrambling

Nel momento in cui arriva il segnale a terra viene catturato dalle antenne paraboliche degli utenti finali tramite un cavo coassiale viene rielaborato da in sistema ricevente (IRD) che provvederà alla sia messa in chiaro. Questa fase è detta Descrambling, come possiamo quindi capire il mezzo che permette il descrabling del segnale è per l'appunto il sistema ricevente o IRD.

Un sistema ricevente IRD è composto dai seguenti componenti:

- **LNB**: Low Noise Block. E' situato sul fuoco dell'antenna parabolica. Il suo compito è quello di amplificare il segnale e traslare la banda delle frequenze ricevute dal satellite, attualmente comprese tra 10.700 e 12.750Mhz, in una banda di frequenze più basse denominata 1° IF (prima frequenza intermedia) compresa tra 950 e 2150 Mhz. L'LNB è collegato al decoder tramite un cavo coassiale con trasmissione fullduplex asimmetrica: il decoder invia (sul canale DiSEC, Digital Satellite Equipment Control, del cavo coassiale) i dati della banda (banda bassa o banda alta) e della polarizzazione all'LNB del canale da visualizzare, L'LNB invia sul cavo coassiale lo stream selezionato.
- **Sintonizzatore**: ha il compito di sintonizzare la frequenza del canale che si vuole visualizzare. Infatti quando operiamo un cambio di canale con il telecomando sul

nostro ricevitore satellitare è il sintonizzatore che ci permette di poter cambiare canale.

- **Demodulatore QPSK**: ritrasforma il segnale armonico modulato in fase, nella corrispondente sequenza binaria, è esattamente l'operazione inversa a quella che aveva eseguito l'emittente nella fase di modulazione QPSK.
- **FEC**: legge e utilizza i bit di ridondanza per correggere gli eventuali errori nei pacchetti DVB/MPEG2, questo avviene secondo delle tecniche utilizzate anche in altri settori e discusse in fondo a questa pagina.
- **Demultiplexer**: In base al valore dell'header di ogni pacchetto decide se ignorare il pacchetto, inviarlo alla CAM, inviarlo direttamente al decoder MPEG o, se si tratta di pacchetti di dati, lasciarli gestire alla CPU del ricevitore.
- **CAM**: Modulo di accesso condizionato. È la parte del decoder in grado di eseguire il descrambling, cioè è in grado di rimettere in chiaro il segnale cifrato. Si tratta di una scheda PCMCIA (aka PC-CARD), che può essere sostituita con una CAM con un altro algoritmo di descrambling (SECA, NDS, ecc). Per eseguire il descrambling si avvale dell'utilizzo di una SmartCard. Nel caso di eventi pay per view la CAM avverte tramite modem il gestore che l'utente sta guardando il programma. Il provider si occuperà di addebitare il costo dell'evento.
- **DECODER MPEG2**: riporta in forma non compressa il flusso audio/video.
- **DAC**: Converte il flusso audio/video in analogico, pronto per essere connesso ad una TV, via scart ad esempio.
- **EEPROM**: Memoria rom riprogrammabile elettronicamente, nella quale sono contenuti i valori necessari per la sintonizzazione di ogni canale.

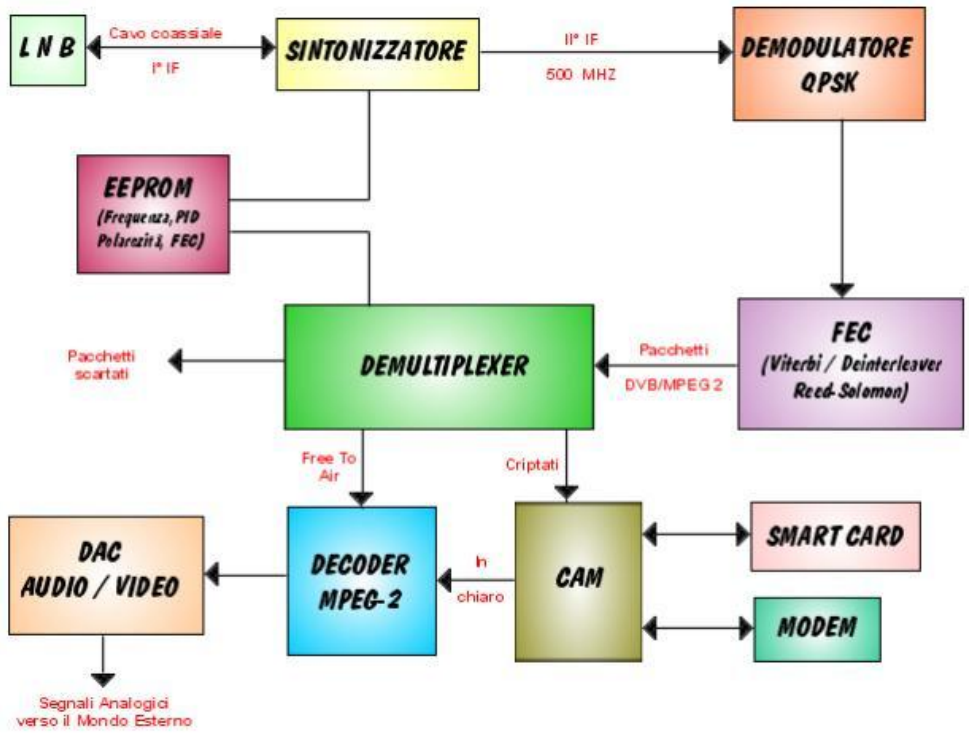


Figura 8 Schema tipo di un IRD o sistema ricevente

Quello che possiamo vedere nella figura sopra è lo schema di un sistema ricevente (IRD), il Descrambling del segnale avviene mediante le seguenti fasi:

1. Il segnale arrivato alla parabola viene amplificato e traslato dalle frequenze ricevute dal satellite in una banda di frequenze più basse tramite l'LBN
2. Tramite il cavo coassiale il segnale arriva al "SINTONIZZATORE" per permettere all'utente di selezionare la frequenza del canale che vuole visualizzare
3. Il segnale ancora di tipo armonico viene trasformato in binario nel "DEMODULATORE QPSK"
4. Vengono corretti eventuali errori nel "FEC" (Forwarding Errort Correction) che sfrutta le tecniche discusse di seguito.
5. Il flusso binario entra nel "DEMULTIPLEXER" che scomporrà il flusso in più sottoflussi contenenti informazioni di gestione e controllo dati
6. Il multiplexer alimenta con i suoi flussi dati la "CAM" che mediante l'interrogazione con la "SMARTCARD" provvederà al controllo delle autorizzazioni per la visualizzazione dei canali ad accesso controllato
7. Sempre il multiplexer alimenta questa volta il "DECODER MPEG-2" che si occupa di riportare in forma non compressa il flusso audio/video
8. In fine il segnale decodificato viene inviato al "DAC (Convertitore digitale-analogico)" che provvederà a convertire il flusso audio/video in analogico per essere inviato ad un televisione.

Nel quarto punto abbiamo detto che eventuali errori vengono corretti nel "FEC", vista l'importanza che riveste tale tecnica di seguito verrà fatta una descrizione un poco più in dettaglio.

3.3.2.1 Forward Error Correction

La trasmissione satellitare è soggetta ad un alto livello di disturbo, quindi è necessario implementare una forma di correzione degli errori.
Essendo un canale unidirezionale e data la natura real-time e broadcast del messaggio non è possibile chiedere al satellite il rinvio dei pacchetti errati, quindi insieme ai byte di informazione vengono inviati dei byte ridondanti per la correzione.
Questa tecnica è chiamata FEC (Forward Error Correction) (8) (9).
Nel nostro caso vengono usati 2 strati di FEC, come possiamo vedere nella figura. Il primo chiamato Viterbi è espresso in numero frazionario. La frazione esprime il rapporto tra il numero n di bit di dati in entrata e il numero n più i bit usati per la correzione (es 2/3: ogni 3 bit ricevuti 2 sono di dati e 1 è usato per la correzione). Il secondo strato di FEC è chiamato Reed-Solomon code (R/S). L'R/S è solitamente 188/204, cioè ogni 204 bytes, 188 sono di dati e i restanti sono usati per la correzione d'errore. Questa stessa catena di FEC viene utilizzata nella correzione di errori per i CD-Audio e i DVD.

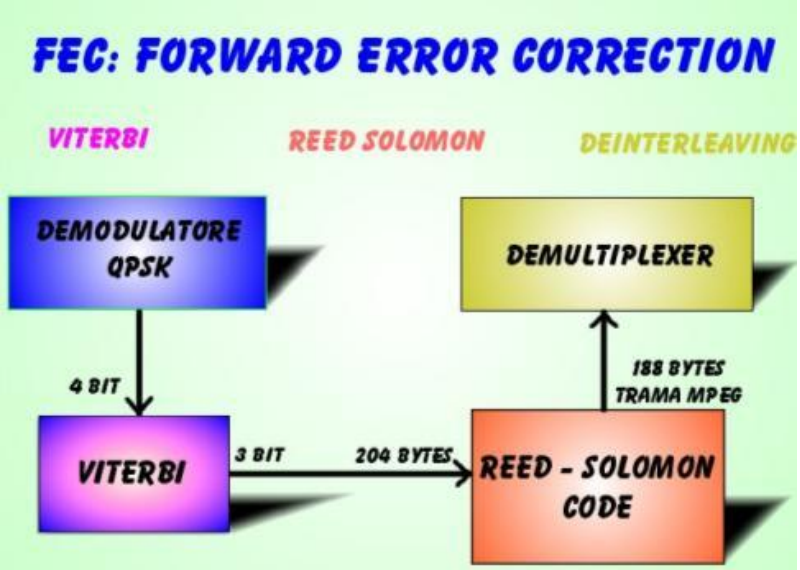


Figura 9 Forward Error Correction

Ogni emittente decide i diversi valori di FEC che incideranno sulla banda (quindi possibilità di inviare più o meno canali per ogni transponder) e sulla qualità.
In più per correggere efficacemente burst di errori (cioè più bit errati consecutivi) il flusso viene inviato in un ordine diverso come mostrato in figura, e riordinato dopo la trasmissione, dall'IRD (interleaving/deinterleaving).

Giunti a questo punto abbiamo visto come si compone uno "Schema generico" di trasmissione e possiamo proseguire con lo studio degli Standard DVB/MPEG-2 che governano tale schema di trasmissione.

3.4 Prestazioni e capacità trasmissiva

Il sistema DVB-T offre una capacità utile per la trasmissione del flusso binario che varia da circa 5 Mb/s a 31,7 Mb/s, a seconda della configurazione di trasmissione adottata: costellazione, tasso di codifica del codice correttore interno e dalla durata dell'intervallo di guardia. Per un dato insieme di questi parametri, le modalità operative 2k e 8k offrono la stessa capacità trasmissiva.
Come risulta dalla tabella 2, l'impiego di una configurazione ad elevata capacità trasmissiva, come il 64-QAM (rate 7/8; intervallo di guardia normalizzato), comporta prestazioni meno robuste in termini di rapporto **portante/rumore** (C/N) richiesto per una corretta ricezione (circa 26,1 dB su canale affetto da rumore gaussiano).
Per contro, un sistema a bassa capacità trasmissiva, come il QPSK (rate 1/2; 1/4), è molto robusto e richiede un basso valore di C/N (circa 3,1 dB). La scelta della configurazione è quindi il risultato di un compromesso tra capacità trasmissiva e robustezza del segnale, in modo da soddisfare i requisiti di servizio.
La tabella 2 riporta, per tutte le combinazioni di costellazione e tasso di codifica previste dalla normativa, le prestazioni del sistema in termini di C/N, valutate per mezzo di simulazioni al calcolatore; riporta inoltre i valori del flusso binario utile (Mb/s) in funzione dell'intervallo di guardia normalizzato.
I valori del rapporto C/N richiesto si riferiscono alla ricezione Quasi Error Free (QEF), corrispondente a meno di un evento di errore per ora sul segnale all'ingresso del

demultiplatore (BER<10E-11), dopo che è stato sottoposto al procedimento di correzione degli errori tramite algoritmo di Viterbi e decodifica Reed-Solomon.

		C/N richiesto per BER=2 x 10-4 dopo Viterbi- QEF dopo Reed-Solomon			Flusso binario utile (Mb/s)			
		Canale			$\Delta = T_g / T_u$			
Modulazione	Codice	Gaussiano	Rice (Ric.Fissa)	Rayleigh (Ric.Portatile)	1/4	1/8	1/16	1/32
QPSK	1/2	3,1	5,6	5,4	4,98	5,53	5,85	6,03
QPSK	2/3	4,9	5,7	8,4	6,64	7,37	7,81	8,04
QPSK	3/4	5,9	10,7	6,8	7,46	8,29	8,78	9,05
QPSK	5/6	6,9	13,1	8,0	8,29	9,22	9,76	10,05
QPSK	7/8	7,7	16,3	8,7	8,71	9,68	10,25	10,56
16QAM	1/2	8,8	11,2	9,6	9,95	11,06	11,71	12,06
16QAM	2/3	11,1	14,2	11,6	13,27	14,75	15,61	16,09
16QAM	3/4	12,5	16,7	13,0	14,93	16,59	17,56	18,10
16QAM	5/6	13,5	19,3	14,4	16,59	18,43	19,52	20,11
16QAM	7/8	13,9	22,8	15,0	17,42	19,35	20,49	21,11
64QAM	1/2	14,4	16,0	14,7	14,93	16,59	17,56	18,10
64QAM	2/3	16,5	19,3	17,1	19,91	22,12	23,42	24,13
64QAM	3/4	18,0	21,7	18,6	22,39	24,88	26,35	27,14
64QAM	5/6	19,3	25,3	20,0	24,88	27,65	29,27	30,16
64QAM	7/8	20,1	27,9	21,0	26,13	29,03	30,74	31,67

Figura 10 Modulazioni e fattori di compressione

Nelle simulazioni è stata ipotizzata una perfetta stima del canale e non sono incluse né la perdita di potenza dovuta alle portanti pilota, né le perdite dovute alla realizzazione del ricevitore e agli apparati inclusi nella catena di trasmissione.
Le prestazioni sono date per un canale ideale affetto esclusivamente da rumore bianco Gaussiano (AWGN) e per due esempi di canale multipath tipici della diffusione terrestre: il canale di Rice (F), rappresenta un tipico caso di ricezione fissa, per il quale è presente la linea di vista con il trasmettitore (segnale principale) più una serie di echi; il canale di Rayleigh (P), è un esempio di ricezione portatile con antenna omnidirezionale, caratterizzato dalla assenza della linea di vista. I tassi di codifica più alti (5/6 e 7/8), quando vengono associati alla costellazione a più elevata efficienza spettrale (64-QAM), risultano molto sensibili al fading selettivo in frequenza.
In pratica, per la stima del massimo numero di programmi TV che possono essere allocati in un canale a 8 MHz, assumendo una ricezione fissa con antenna direttiva, la configurazione più idonea è il 64-QAM a tasso 2/3; essa fornisce una capacità di flusso binario di circa 24 Mb/s, nel caso di Tg/TU=1/32, che consente tipicamente la trasmissione di 4 programmi a qualità convenzionale (SDTV a 6 Mb/s ciascuno) o 6 programmi a qualità News (LDTV a 4 Mb/s ciascuno).
Questa configurazione di trasmissione è particolarmente idonea per le reti multifrequenza (MFN). L'impiego della multiplazione statistica associata alla codifica MPEG-2 a bit-rate variabile consente inoltre di aumentare il numero di programmi senza peggiorare la qualità audio/video.
Per maggiori dettagli si veda (10) (11).

3.5 Le reti di diffusione in isofrequenza (SFN)

Un considerevole vantaggio che offre la modulazione digitale OFDM impiegata nello standard DVB-T è la possibilità di realizzare reti di diffusione terrestre in isofrequenza, cioè di avere più trasmettitori in funzione, che servono zone adiacenti, sulla medesima frequenza, con gli stessi programmi; in pratica si può utilizzare lo stesso canale di emissione per vaste aree, servite da più trasmettitori, senza che essi si disturbino l'un l'altro (SFN - Single Frequency Network – cioè rete a singola frequenza).

Nella trasmissione analogica, ciò è praticamente impossibile. Nei sistemi analogici, utilizzando la tecnica dell'offset (di riga, o, meglio, di quadro) si possono ridurre le zone di interferenza ai limiti delle aree di servizio di ciascun trasmettitore rispetto al trasmettitore che serve l'area adiacente, ma, in pratica, anche con una pianificazione della rete estremamente oculata ed impiegando sistemi d'antenna che evitino il più possibile l'irradiazione al di fuori dell'area di servizio prevista, di fatto, una rete analogica isofrequenziale è irrealizzabile senza consistenti zone di interferenza, nelle quali la qualità del segnale degrada consistentemente.
Vediamo ora come si realizzano le reti di diffusione digitale a singola frequenza (SFN).
Innanzitutto, la precisione/stabilità di frequenza (che normalmente è richiesta essere di 500Hz), deve essere significativamente maggiore rispetto ai trasmettitori impiegati nelle reti MFN (Multi Frequency Network – ovvero reti con più frequenze).
Nelle reti SFN, tutti i trasmettitori devono essere sincronizzati ad un unico riferimento di frequenza, per il quale normalmente si utilizza il GPS (Global Positioning System - cioè il sistema di navigazione satellitare realizzato e mantenuto dal Dipartimento della Difesa USA).
Il segnale proveniente dai satelliti GPS è ricevibile pressoché ovunque nel mondo e contiene una precisissima informazione di tempo cui poter agganciare i trasmettitori della rete SFN (la precisione/stabilità sarà pertanto dell'ordine di grandezza di 1Hz).
Ciascun trasmettitore della rete SFN dovrà trasmettere esattamente lo stesso Transport Stream (il flusso dei dati digitali contenente i programmi) e lo dovrà emettere in modo da essere sincronizzato con gli altri trasmettitori. Per fare ciò, all'atto della generazione (normalmente nel multiplexer che dovrà essere opportunamente predisposto), il Transport Stream viene suddiviso in "Megaframes" e vengono aggiunti dei dati (MIP – Megaframe Inizialization Packet) al fine di poter sincronizzare l'emissione da ogni trasmettitore.

3.6 Il sistema DVB-S (diffusione dei segnali numerici TV da satellitare)

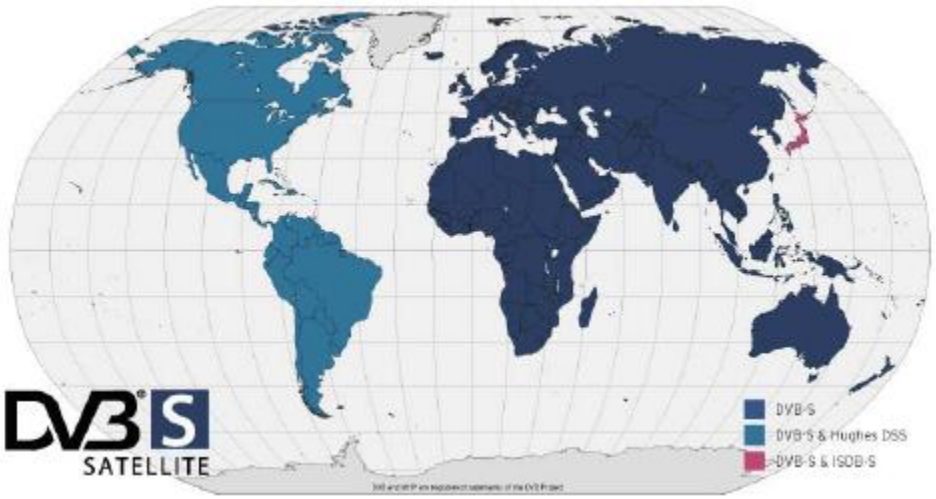


Figura 11 Diffusione standard satellitari

Il sistema DVB-S (12) (13) (14) adottato nelle trasmissioni satellitari, specificato nella norma ETS 300 421 degli standard ETSI, utilizza gli standard MPEG per la codifica, la compressione del segnale sorgente e per la multiplazione dei programmi. Per ogni transponder del satellite, grazie alla multiplazione dei programmi, è possibile trasmettere ad una velocità complessiva di 38.015 Mbits al secondo più programmi contemporaneamente .
La tecnologia satellitare, grazie allo standard DVB-S, viene sfruttata in maniera analoga sia per la diffusione dei programmi televisivi, che dei programmi radiofonici, che per la trasmissione di dati.
In particolare il DVB-S prevede:

- L'utilizzo dell'MPEG-2 Transport Stream (visto nel capitolo 2) per l'incapsulamento dei dati e la relativa trasmissione.
- Trattamento del segnale con sequenza pseudo casuale per la dispersione di energia spettrale, ovvero l'energia associata al segnale in fase di trasmissione. Nel caso di un segnale digitale l'energia si distribuisce in modo uniforme all'interno della banda disponibile. I dati all'interno di un pacchetto vengono randomizzati, ovvero diffusi in modalità casuale.
- La protezione dagli errori attraverso l'interleaving, ovvero l'interlacciamento del flusso digitale seriale per ridurre gli effetti degli errori a burst. Questa tecnica permette di scomporre errori di tipo burst, ovvero più bit errati consecutivi, in tanti errori che coinvolgono un solo bit, o in generale un numero piccolo di bit per ogni blocco.
- L'utilizzo dello schema di codifica Reed-Solomon (16 bits), per il Forward Error Correction (FEC), che effettua la correzione degli errori nei blocchi di bytes.
- La codifica convoluzionale parametrizzabile, che introduce ridondanza per rendere i segnali di informazione robusti alla corruzione dovuta a segnali di disturbo.
- Il filtraggio in banda base, che riguarda la conversione del segnale da frequenze intermedie, comprese tra i 900 Mhz e i 2150 Mhz, a frequenze alte, comprese tra i 10700 Mhz e i 12750 Mhz.
- La modulazione QPSK (Quadrature Phase Shift Keying), per la trasformazione del segnale in forma binaria nel corrispondente segnale modulato in fase (FM). Questa

tecnica di modulazione è la soluzione ideale per i collegamenti via satellite, poiché evita gli effetti degradanti del rumore (segnali di disturbo) a cui sono sottoposti tali collegamenti.

In figura è possibile vedere le operazioni, previste nel DVB-S, che vengono effettuate sui pacchetti MPEG-2 TS (tran sport Stream) prima di essere inviati al satellite.

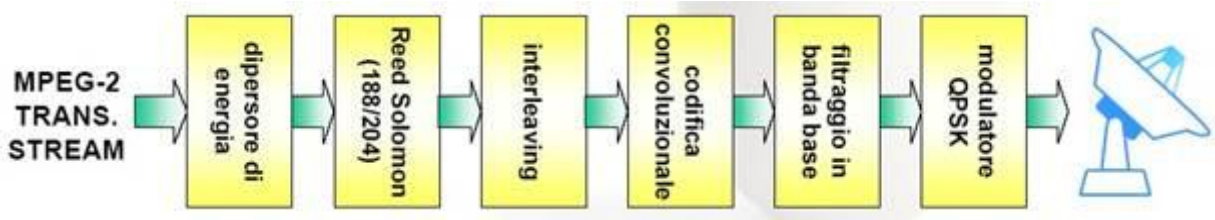


Figura 12 Operazioni effettuate su MPEG-2 TS

La trasmissione satellitare è soggetta ad un alto livello di disturbo, quindi è necessario implementare una forma di correzione degli errori. Essendo un canale unidirezionale e data la natura real-time e broadcast del messaggio, non è possibile chiedere al satellite il rinvio dei pacchetti errati, quindi insieme ai byte di informazione vengono inviati dei byte ridondanti per la correzione degli errori. Questa tecnica è chiamata FEC.

Il FEC utilizzato con la modulazione QPSK si compone di due forme di correzione degli errori.
La prima, chiamata codice Viterbi, si scrive con una frazione (ad esempio 2/3). Questa frazione esprime il rapporto tra il numero 'n' di bit di dati in entrata ed il numero 'n + i' di bit usati per la correzione degli errori (es. 2/3: ogni 3 bit ricevuti, 2 sono di dati ed 1 è usato per la correzione).
Dopo aver estratto il codice di correzione degli errori Viterbi ed averlo utilizzato, viene utilizzata una seconda forma di correzione degli errori chiamata codice Reed-Solomon. Su 204 bits trasmessi, 188 contengono dei dati ed i 16 bits restanti sono utilizzati come bit di parità per aiutare a correggere gli eventuali errori restanti.
Oltre a questo, il meccanismo del FEC utilizza anche l'intreccio dei flussi (interleaving) di dati per evitare che un'interferenza improvvisa interrompa la trasmissione.
Esempio:
Consideriamo il messaggio seguente: **“This is a sample message”**. Dopo l'intreccio il messaggio potrebbe diventare così: **“eTs haais mgi smeaesp l”**. Se un errore dovesse riprodursi e cancellasse la parte "m - g - i" del messaggio, il messaggio non intrecciato sarebbe **“This *s a sa*ple messsa*e”**.
Quindi solamente dei caratteri isolati (rappresentati dagli asterischi) mancano al messaggio anziché una parola intera se il messaggio non fosse stato intrecciato. Questo nel caso di immagini equivale a dire che il disturbo è diffuso e quindi meno evidente rispetto a un disturbo concentrato in una singola frazione immagine.
Dopo aver effettuato le operazioni elencate in precedenza, il segnale viene modulato sulla portante dal broadcaster, usando il sistema di modulazione QPSK. Grazie a questo complesso meccanismo di “impacchettamento”, il sistema può essere adattato alla caratteristica di errore del canale, dove errori improvvisi vengono agevolmente randomizzati, e quindi assorbiti.

3.7 Il sistema DVB-IP (diffusione di dati via satellite)

Lo standard DVB IP, utilizzato per la distribuzione di dati via satellite, è basato sugli standard ETSI/DVB per DVB-S (ETS 300 421 – modulazione e codifica di canale per sistemi satellitari) e

DVB-SI (ETS 300 468 – Service Information). La specifica della distribuzione dati DVB IP è definita dagli standard ETSI EN 301 192 per Data Broadcasting e illustra una varietà di modi per la diffusione di dati.
Tale specifica identifica quattro modalità di diffusione dei dati:

- il **data piping,** che prevede l'inserimento dei dati, che devono essere trasmessi in broadcast, direttamente all'interno della sezione payload dei pacchetti MPEG-2 TS;
- il **data streaming**, ovvero la trasmissione di dati per mezzo di flussi. Esso prevede l'inserimento dei dati, da trasmettere in broadcast, all'interno dei pacchetti PES (Packet Elementary Stream), come definito dal sistema MPEG-2 TS;
- il **Multi Protocol Encapsulation** (MPE), che fornisce un meccanismo per incapsulare protocolli per la comunicazione su rete, su flussi MPEG-2 TS. La trasmissione dei datagrams contenenti i dati, viene effettuata incapsulando i datagrams stessi nella sezione DSM-CC dei pacchetti MPEG-2 TS;
- il **data carousel,** dove i dati da trasmettere vengono organizzati in moduli, i quali a loro volta sono suddivisi in blocchi. Tutti i blocchi di tutti i moduli sono della stessa dimensione, eccetto l'ultimo blocco di ogni modulo, il quale può essere di dimensione inferiore. I moduli sono una delineazione logica dei gruppi di dati separati, all'interno del data carousel.

La modalità di diffusione che ha importanza rilevante per il DVB IP è il MPE.
Il formato MPE è standardizzato dalla ETSI e ciò garantisce un'interoperabilità tra hardware diversi che prevedono tale funzione. Il protocollo MPE supporta servizi di data broadcasting che richiedono l'incapsulamento di più protocolli di comunicazione, dei quali un esempio è il protocollo IP. Ciò riguarda le applicazioni Unicast, dove ogni datagram viene targato per essere indirizzato verso un singolo utente, e le applicazioni multicast , dove il datagram viene indirizzato verso un gruppo di utenti. I pacchetti vengono "marchiati" tramite l'indirizzo MAC (Media Access Control), di cui parleremo più avanti, tramite il quale l'utente può capire se il pacchetto è indirizzato a lui.
Nei pacchetti indirizzati a più utenti vengono specificati i diversi MAC address (vedi figura sotto). Nell'esempio vediamo le sezioni contenute all'interno di un pacchetto:

- la sezione table id, riportante l'ID (identificatore) del pacchetto;
- la sezione length, che specifica il numero dei MAC a cui è indirizzato il pacchetto;
- diverse sezioni contenenti i MAC addres ai quali è indirizzato il pacchetto;
- la sezione CRC32 o checksum, contenente un valore grazie al quale è possibile controllare eventuali errori di trasmissione, eseguendo una somma di controllo sui valori binari dei dati trasmessi.

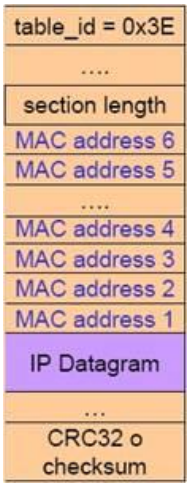


Figura 13 Esempio di pacchetti con specifica dei MAC

La tecnologia che sta alla base dei sistemi DVB IP è quella del trasporto di dati tramite l'incapsulamento dei datagrams IP all'interno del flusso DVB.
Di seguito è mostrato lo stack dei protocolli previsto per lo standard DVB IP (figura sotto).

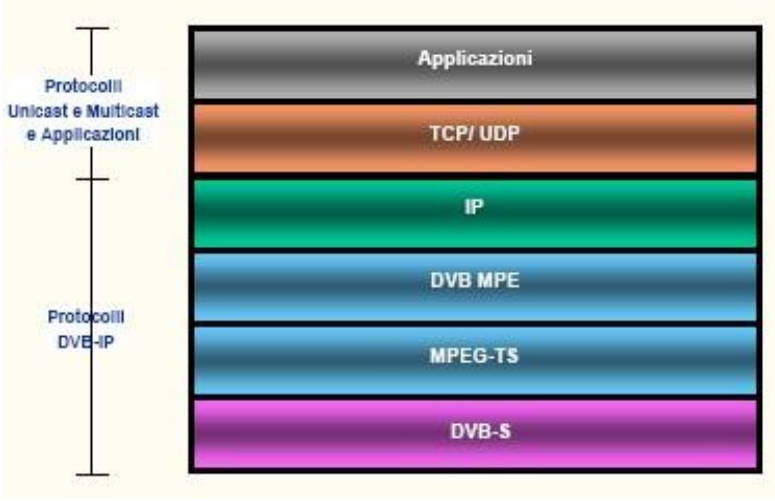


Figura 14 Stack dei protocolli DVB IP

In sostanza quindi ogni datagram IP viene inserito in una sezione privata (una delle sezioni definite nello standard MPEG) del pacchetto per il trasporto (figura). Ogni datagram IP deve avere una dimensione non superiore a 4080 bytes. Il DSM-CC, ovvero il Digtal Storage Media è uno strumento sviluppato appositamente per controllare i flussi MPEG ed è basato sulle sezioni private.

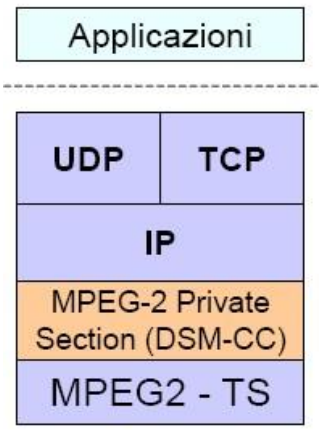


Figura 15 Meccanismo per il trasporto di protocolli di rete su MPEG-2 TS

I sistemi DVB IP esistenti possono essere classificati in due categorie:

- **sistemi bidirezionali**, chiamati DVB RCS (Return Channel System);
- **sistemi unidirezionali**, chiamati DVB IP one way.

I **sistemi bidirezionali** DVB RCS (figura sotto), indirizzati ad un mercato business, utilizzano per le richieste di dati un canale satellitare dedicato ad alta capacità (fino a 2 Mbps).
Un sistema bidirezionale attraverso l'utilizzo di un apparato per l'uplink satellitare, indicato in figura, sotto, come outdoor unit (ODU), trasmette le richieste al canale satellitare dedicato tramite il return link. I dati dal computer passano attraverso l'indoor unit (IDU), la quale effettua tutte le operazioni necessarie per la trasmissione dei dati sul satellite, quindi giungono all'outdoor unit che si occupa della trasmissione dei dati verso il satellite. Lo stesso apparato viene utilizzato anche per la ricezione dei dati richiesti. Infatti i dati ridiscendono a terra attraverso il forward link e vengono ricevuti tramite l'outdoor unit. Poi questi dati sono passati all'indoor unit che li elabora in modo opportuno ed infine li passa al computer.

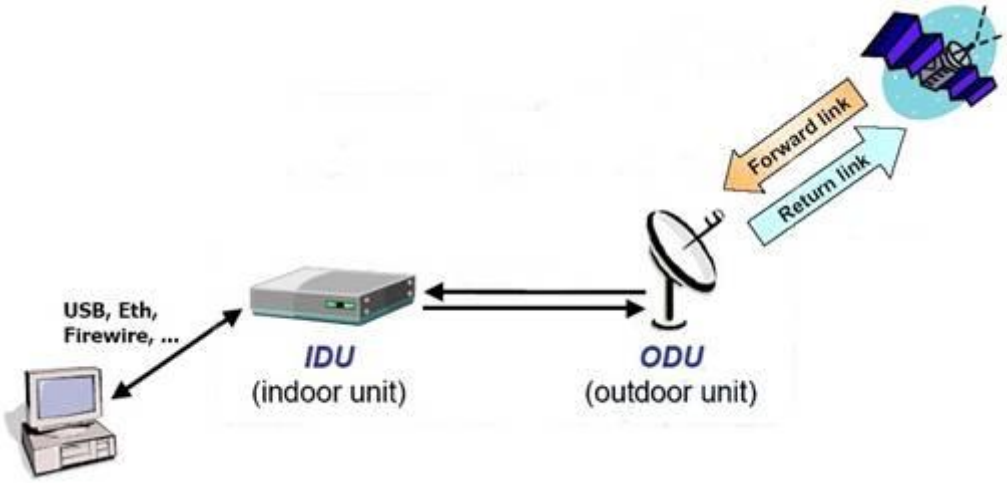


Figura 16 Schematizzazione di un sistema bidirezionale

I **sistemi unidirezionali** (figura sotto), rivolti al mercato consumer, permettono all'utente la ricezione delle informazioni sul link satellitare, con una capacità che varia dai 300 kilobytes fino ai 2 Megabytes al secondo (a seconda del tipo di servizio, del tipo di abbonamento e del provider), tramite un'antenna parabolica collegata al Pc, che deve essere dotato di un'apposita scheda DVB (conforme agli standard DVB), per poter ricevere ed elaborare i dati in arrivo dal satellite in modo opportuno. Per le richieste occorre invece l'abbonamento ad un ISP (Internet service provider) terrestre, a cui connettersi mediante l'utilizzo di un normale modem con collegamento PSTN, ISDN, ADSL o anche per mezzo di un cellulare Gprs dotato di modem. Le richieste passano dall'ISP locale ed attraversano la Rete fino ad arrivare ad una stazione base dotata di un sistema di diffusione DVB, la quale si occupa di recuperare i dati richiesti e trasmetterli al satellite. Infine i dati dal satellite giungeranno fino all'utente.

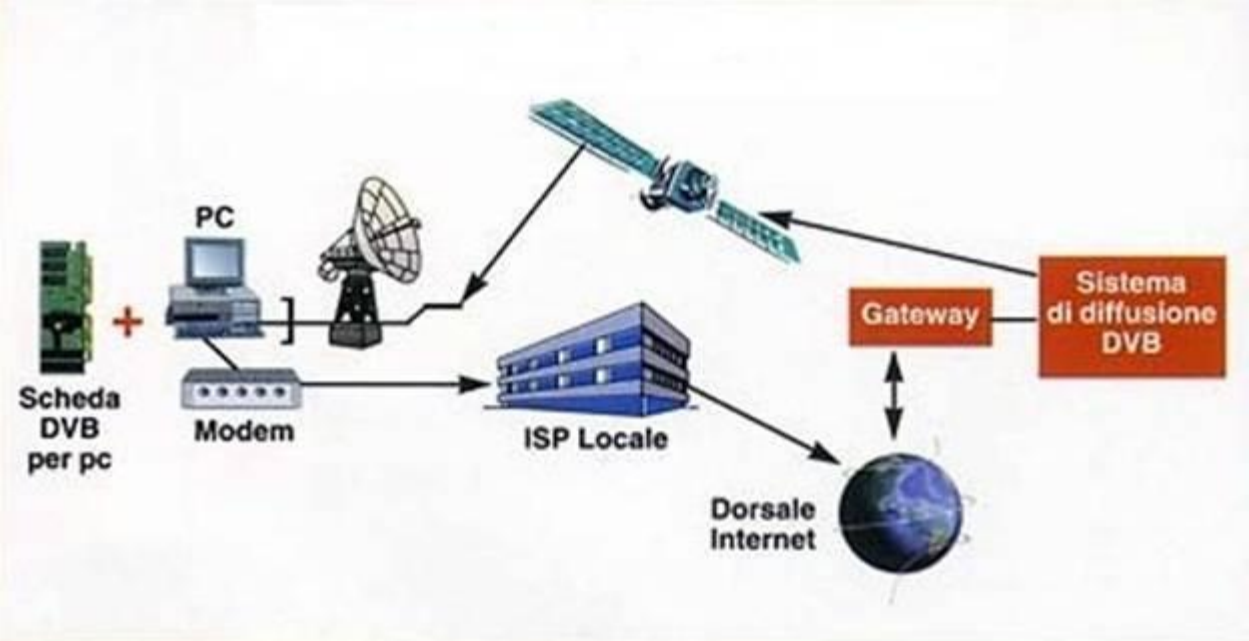
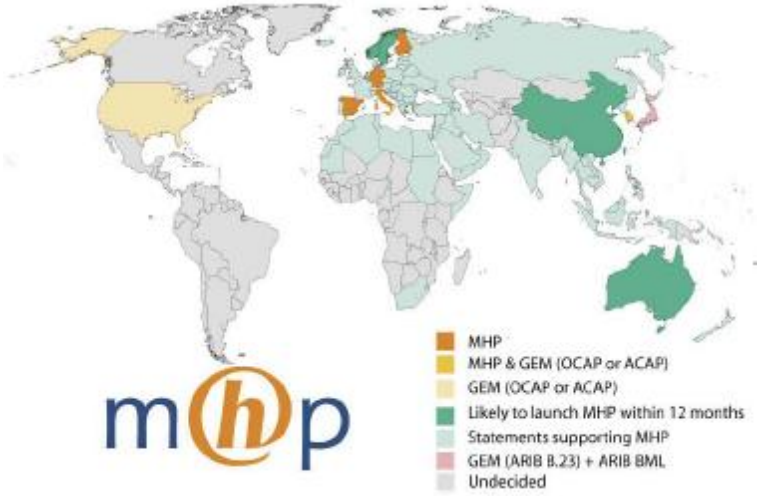


Figura 17 Schematizzazione di un sistema unidirezionale

In questo documento comunque si farà riferimento solo ai sistemi unidirezionali, i quali sono maggiormente diffusi.

3.8 Il sistema DVB-MHP, adottato per la televisione digitale interattiva



3.8.1 La piattaforma MHP

Il gruppo di progetto DVB lavora sin dal 1997 alle specifiche relative ad uno standard aperto, per la gestione della multimedialità e dell'interattività: il DVB-MHP (Digital Video Broadcasting – Multimedia Home Platform) (15).

Nasce un nuovo gruppo di lavoro con l'incarico di redigere una lista dettagliata di requisiti che il nuovo standard dovrà soddisfare.

Entrano a far parte di questo gruppo numerose aziende del settore, tra le quali la Sun Microsystems®, che contribuirà allo sviluppo di una piattaforma basata su Java™.

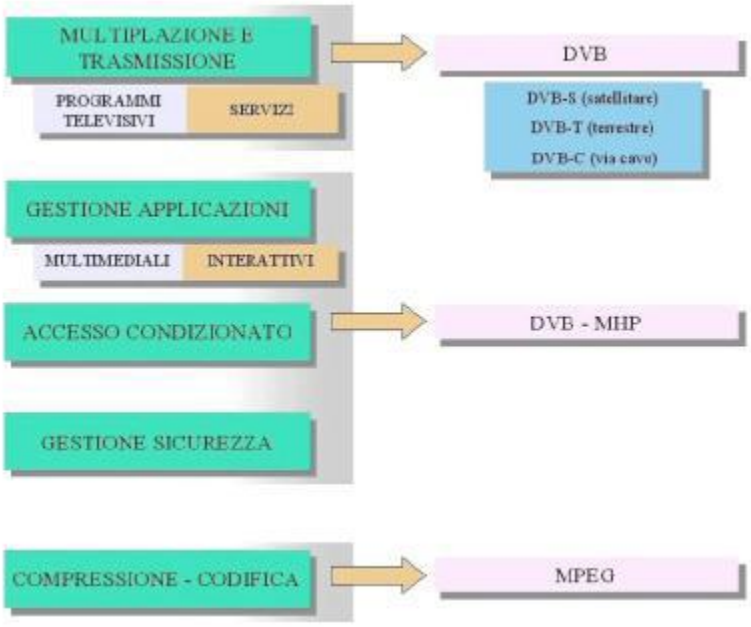


Figura 18 Aspetti tecnologici che concorrono nella piattaforma digitale

Questo standard è aperto all'utilizzo di ogni soggetto interessato, anche non membro del DVB, permettendo a gruppi diversi di interoperare, rispettando le specifiche minime della piattaforma; gli apparati di ricezione diventano intercambiabili tra loro e i gestori delle reti possono utilizzare servizi diversi verso apparati diversi. I principali benefici della specifica MHP (come per qualunque standard pubblicato) sono:

- Standard aperto, orientato a garantire la piena interoperabilità tra qualsiasi programma irradiato e qualsiasi tipo di ricevitore a casa dell'utente (fatta salva la distinzione tra profili);
- Costi più economici per le licenze di utilizzo della piattaforma, rispetto all'utilizzo di piattaforme proprietarie;
- Possibilità di scegliere tra molti più fornitori, che non nel caso di soluzioni proprietarie.

Poiché si prevede che a lungo termine lo standard DVB-MHP sarà probabilmente adottato quasi universalmente; la sua introduzione destrutturerà il modello di mercato verticale o proprietario delle piattaforme software esistenti degli attuali service providers. Tuttavia, nel breve-medio termine, l'affermazione della piattaforma MHP potrà incontrare vari problemi di affermazione. Lo standard presenta anche alcune lacune, tra queste quella di non coprire pienamente l'aspetto dell'accesso condizionato per il quale, poiché si entra nel campo della Pay Tv, esistono molti standard proprietari e non si può sperare in nulla di più che nella presenza di STB con Common Interface, cioè con un ingresso (slot) in grado di ospitare schede del tipo PCMCIA per il supporto di vari standard di crittazione del segnale televisivo.
In questo modo, l'utente può con lo stesso apparecchio, cambiando solo la scheda PCMCIA, ricevere canali crittati secondo vari standard.
L'aspetto della sicurezza delle transazioni è coperto nello standard solo dal profilo Internet access.

CAPITOLO 4: Sicurezza nel sistema DVB

4.1 Introduzione

La tv a pagamento richiede che la rappresentazione MPEG-2 sia cifrata in modo tale da non poter permettere ad un utente non autorizzato la visione di canali a pagamento. A tale scopo è sorta la necessità di utilizzare un sistema per l'accesso condizionato (CAS) che utilizza algoritmi di cifratura all'interno del Common Scrambling Algorithm (CSA). In questo capitolo analizzeremo la struttura del sistema CSA definito nel DVB, che permette l'uso di differenti algoritmi simmetrici per la visione sicura della tv digitale.
In particolare, paragrafo 4.3.1, descriveremo più in dettaglio un esempio di applicazione di cifratura e relativa decifratura simmetrica, analizzando la cifratura a blocchi e a flusso utilizzata e il modo in cui viene eseguito lo schedule della chiave.
Nella sezione 4.4 saranno proposte le diverse modalità di distribuzione della chiave utilizzando una gerarchia a livelli, cosi definita in quanto sono coinvolte più entità a diversi livelli per garantire una maggiore sicurezza contro la pirateria. Saranno analizzate la gerarchia a 2 livelli, 3 livelli ed infine a 4 livelli.
Nella sezione 4.5 descriveremo brevemente le tecniche di Scrambling dalle quali si sono poi sviluppate quelle utilizzate nei moderni sistemi per la visione della tv digitale (con l'utilizzo di CSA), soffermandoci brevemente sulle tecniche Cut and Rotate e Line Shuffle.

4.2 Il sistema per l'accesso condizionato

Un sistema di accesso condizionato, in sigla CAS (dal corrispondente termine inglese "conditional access system"), è una tecnologia che utilizza algoritmi per consentire l'accesso a dati o contenuti codificati o cifrati da parte del distributore. Attraverso questo meccanismo viene permesso l'accesso solo a coloro che sono autorizzati, secondo le modalità che il distributore dei dati o contenuti avrà scelto. È il tipico caso dell'accesso a programmi o piattaforme televisive a pagamento sia satellitari che terrestri (16).

4.3 Struttura CSA

Nella figura in basso viene descritta in modo schematico la struttura del sistema CSA utilizzato nei sistemi DVB (17) (18) (19).

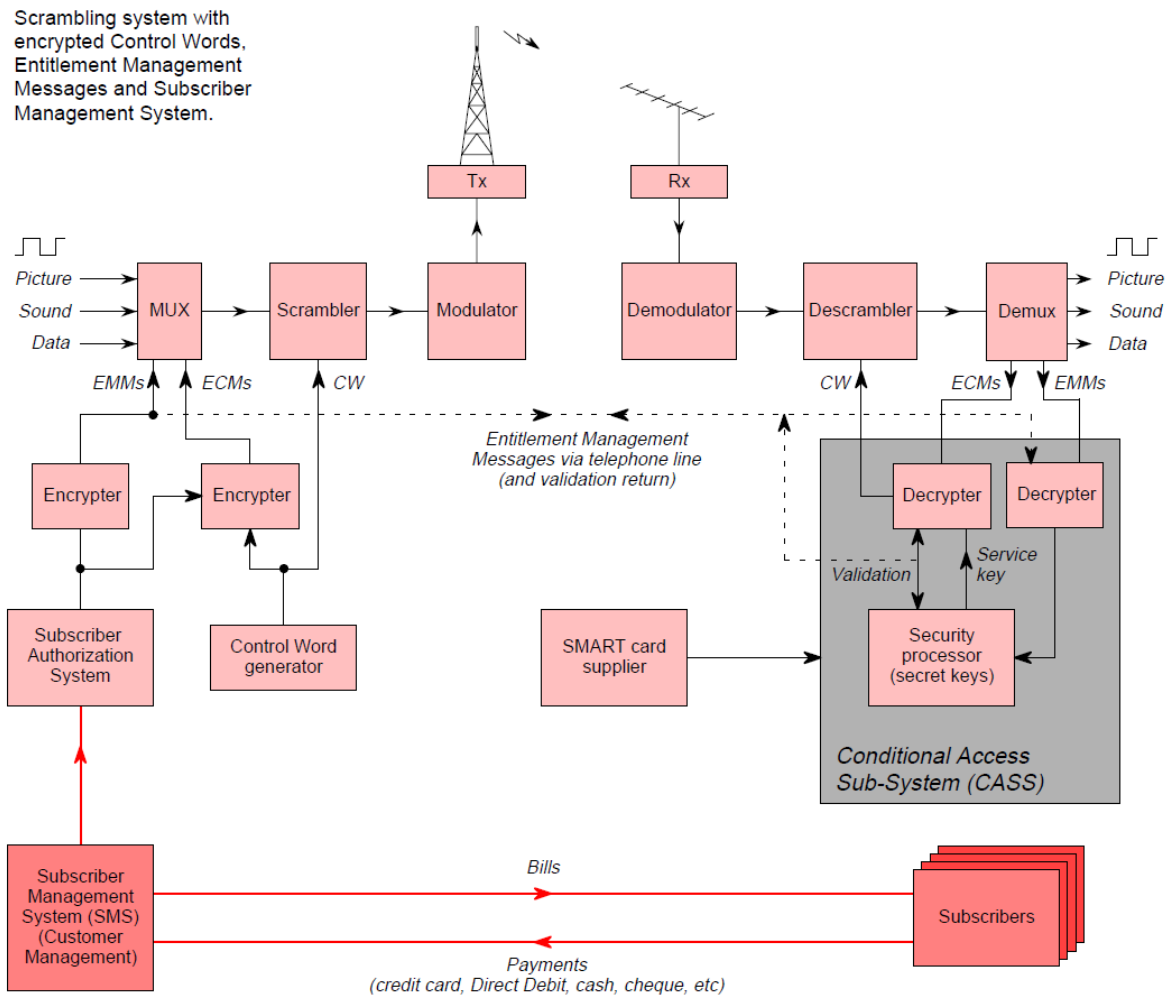


Figura 19 Schema di funzionamento architettura sistema CSA

Partendo dal basso dello schema sopra, il Sistema di Gestione degli abbonati (SMS) verifica la regolarità degli abbonamenti (fatture pagate, scadenza abbonamenti ancora non raggiunta, ecc.).

Al livello intermedio, possiamo distinguere operazioni effettuate dal Service provider (lato sinistro della figura) e dall'apparato ricevente (lato destro).

Un generatore di chiavi produce le Control Word (CW), che vengono utilizzate dallo Scrambler per rendere il segnale audio/video/dati incomprensibile. La CW, inoltre, viene cifrata tramite la Service Key (SK) ed incapsulata in un messaggio chiamato Entitlement Control Message (ECM) in input al multiplexer.

Il Service provider riceve dal Subscriber Management System la lista degli utenti autorizzati a ricevere, e crea un messaggio Entitlement Management Message (EMM) da passare al multiplexer. In questo messaggio sono incapsulate le informazioni di indirizzamento e le chiavi elettroniche (cifrate) utilizzate dal meccanismo di cifratura.

I messaggi EMM ed ECM vengono quindi passati, assieme al segnale in uscita dallo scrambler, al Multiplexer e, dopo il processo di Modulazione, le informazioni vengono trasmesse sul canale.

Dal lato Subscriber, il segnale codificato viene passato in ingresso al demodulatore; il demultiplexer estrae dal segnale i messaggi EMM ed ECM.
Il Conditional Access Sub-System (CASS), tramite la SK, decifra la CW presente nel messaggio ECM, permettendo così al Descrambler di decodificare il segnale audio/video/dati.
Il CSA utilizza la CW che viene cifrata con un altro sistema simmetrico non standardizzato (di proprietà dell'ente trasmissivo e per questo segreto) che utilizza la SK. A sua volta, la SK viene cifrata con un ulteriore sistema simmetrico non standardizzato che utilizza una chiave chiamata User Key (UK).
La CW viene modificata, in genere, ogni due secondi e una volta cifrata, inserita nel ECM, la SK viene modificata, in genere, ogni dieci secondi e una volta cifrata, inserita nel EMM, mentre la UK viene modificata raramente.
ECM ed EMM, che costituiscono il flusso dati per la decodifica, vengono opportunamente sincronizzati ed inviati col relativo flusso audio/video MPEG-2 cifrato.
Al contrario del CSA, i sistemi di codifica consistenti nella cifratura e gestione delle chiavi, degli abbonamenti in pay tv e degli eventi in pay per view non sono stati unificati e standardizzati, in quanto ogni operatore ha preferito, per motivi di sicurezza e commerciali, utilizzare il proprio sistema.
I più diffusi sono:

- Irdeto,
- Mediaguard della SECA,
- Viaccess,
- Nagravision,
- Conax,
- Cryptoworks della Philips,
- Videoguard della NDS (chiamato Nds).

La codifica Seca viene usata quasi esclusivamente dal gruppo francese CanalPlus, proprietario di emittenti in molti Stati europei, e Nds soltanto dal gruppo britannico Sky a cui, tra l'altro, appartiene anche Sky Italia.
Il DVB prevede che gli utenti della tv a pagamento possano rimettere in chiaro le chiavi ed il segnale audio/video ricevuti tramite un sistema composto da un ricevitore con decodifica chiamato comunemente decoder (Integrated Receiver Decoder, IRD), fornito dall'emittente o acquistato, e da una smart card fornita dall'emittente.
Il decoder deve supportare la codifica dell'emittente di cui si desidera la visione in modo che possa decodificare la SK e la CW. Inoltre deve essere in grado di effettuare il descrambling del flusso MPEG-2 (che poi decomprimerà per ottenere audio e video) con la CW decodificata.
Infine, il decoder, deve essere dotato di un lettore (CAM – common access module) di smart card in formato standard ISO 7816. La smart card costituisce il nucleo del sistema di accesso condizionato in quanto la sua EEPROM contiene la UK e i dati relativi all'abbonamento sottoscritto dall'utente quali, per esempio, i canali visibili e la data di scadenza.
Inoltre, la smart card, possiede un microprocessore in grado di effettuare la decifrazione della SK con la UK e della CW con la SK.
La SK e la CW vengono trasmesse alla smart card tramite il lettore del decoder nel formato ECM ed EMM, successivamente il decoder riceve la CW decifrata dalla smart card e provvederà al descrambling del flusso MPEG-2.
La complessa "gestione gerarchica delle chiavi" definita dal DVB ha una validità molto generale in quanto, non costituendo standard, viene adattata da ogni sistema di codifica in funzione della propria strategia di gestione.

Le variazioni più comuni riguardano la frequenza con cui viene generata una nuova CW e il relativo ECM e una nuova SK e il relativo EMM.
Gli ECM hanno una frequenza molto alta e vengono generati all'incirca ogni dieci secondi mentre gli EMM molto bassa e vengono generati sporadicamente con frequenza oscillante fra uno e trenta giorni.
Considerato che i sistemi di codifica sono diversi e l'acquisto di un decoder con codifica integrata potrebbe risultare vincolante per l'utente, il DVB ha definito due tecniche di codifica: *simulcrypt* e *multicrypt*.
Il *multicrypt* prevede l'adozione dello standard Common Interface (DVB-CI) in cui il decoder è dotato di uno o più slot PCMCIA (Personal Computer Memory Card International Association) dove inserire i Conditional Access Module (CAM) che supportano i vari sistemi di codifica e dispongono di uno slot per l'inserimento della smart card. In pratica quello che accade con questa tecnica è la possibilità di utilizzare un unico decoder predisposto ad allogiare al suo interno CAM che possono avere differenti codifiche di cifratura.
Il *simulcrypt* prevede la contemporanea cifratura delle chiavi con codifiche diverse nel decoder stesso senza il supporto alla CAM. Differenze tra simulcrypt e multicrypt comporta per i fornitori dei servizi radiotelevisivi accordi di licenza con tutti i fornitori dei sistema di accesso condizionato, utilizzati per cifrare i servizi radiotelevisivi, licenze che per i fornitori dei servizi radiotelevisivi comportano dei costi che inevitabilmente ricadono sugli utenti attraverso il canone di abbonamento ai servizi radiotelevisivi.

4.3.1 Dettagli algoritmo CSA

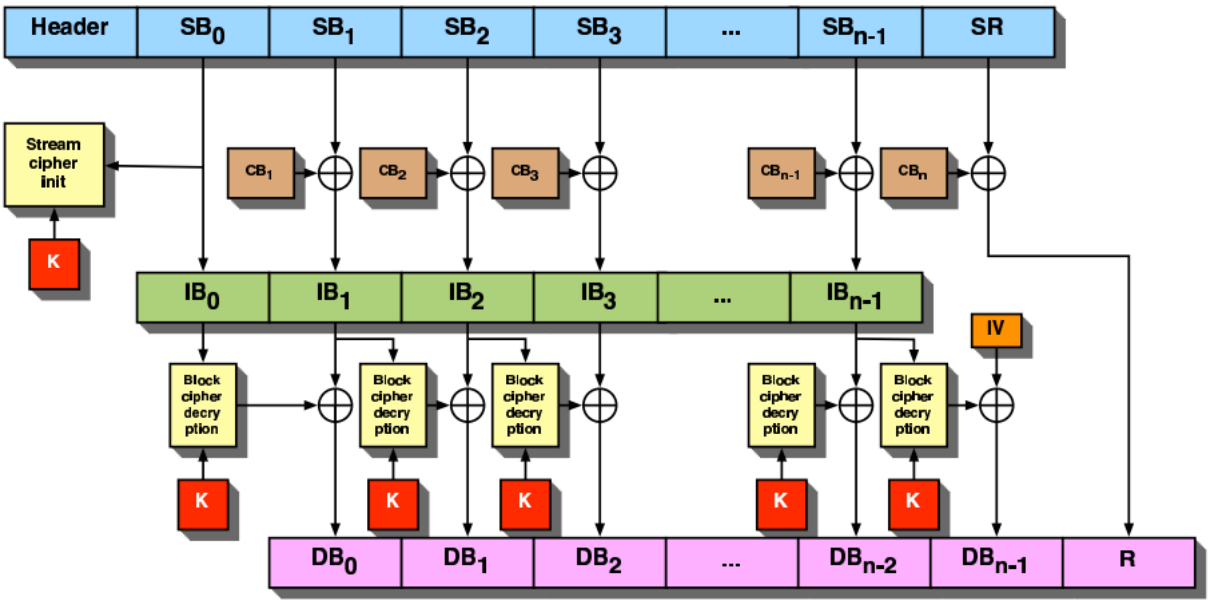


Figura 20: Processo di Descrambling nell'algoritmo CSA

L'algoritmo CSA (20) (21) è ottenuto usando in cascata due sistemi crittografici differenti, un cifrario a blocchi e un cifrario a flusso. Entrambi gli algoritmi hanno una chiave comune (K) di 64 bit, chiamata common key. Per la fase di scrambling il payload di un pacchetto di m-byte viene diviso in blocchi di 8-byte (DB_i) ciascuno. È possibile che la lunghezza del pacchetto non sia multipla di 8-byte. Se cosi fosse, l'ultimo blocco è chiamato residuo (R).

La sequenza di blocchi di 8 byte è cifrata in ordine inverso con il cifrario a blocchi in modalità CBC (Cipher Block Chaining), mentre il residuo è lasciato cosi com'è. Il vettore di inizializzazione (IV) è sempre uguale a zero. Nota, che il residuo rimane inalterato in questo passo di cifratura.
L'ultimo output della cifratura IB_0 è usato come "nonce" per il cifrario a flusso. I primi m-8 byte del keystream generato dal cifrario a flusso sono messi in XOR con il blocco cifrato $(IB_i)_{i\geq 1}$ seguito dal residuo per produrre i blocchi cifrati SB_i.

4.3.1.1 La parte di cifrario a blocco di DVB CSA

CSA utilizza un cifrario a blocchi iterato di 56 round. Ha due ingressi:

- un blocco di 64 bit di dati,
- uno di 64 bit per la chiave (common key K);

ottenendo un blocco di output a 64 bit.
Ogni round del cifrario utilizza la stessa trasformazione ϕ, che prende un vettore lungo 8-byte con un singolo byte della chiave espansa come input e in output restituisce un vettore di 8-byte. (22)

Schedule della chiave

Sia p una funzione di permutazione definita su stringhe di 64 bit, la chiave espansa di 448 bit $\mathrm{k}^{\mathrm{E}} = (\mathrm{k}_0^{\mathrm{E}}, \ldots, \mathrm{k}_{447}^{\mathrm{E}})$ è ottenuta in modo ricorsivo nel seguente modo:

$$\begin{aligned} k^E_{0,\ldots,63} &= k_{0,\ldots,63} \\ k^E_{64i,\ldots,64i+63} &= \rho(k^E_{64(i-1),\ldots,64i-1}) \oplus \texttt{0x0i0i0i0i0i0i0i0i} \quad \text{for all } 1 \leq i \leq 6 \end{aligned}$$

Dove 0x0i0i0i0i0i0i0i0i deve essere interpretato come un costante esadecimale.

La funzione round

La funzione utilizza due permutazioni non-lineari π e π'. Queste permutazioni sono legate da un'altra permutazione σ ad esempio $\pi' = \sigma * \pi$. La permutazione σ mappa il bit 0 con 1, il bit 1 con 7, il bit 2 con 5,il bit 3 con 4, il bit 4 con 2, il bit 5 con 6, il bit 6 con 0 e il bit 7 con 3.
Sia S = (s_0,…,s_7) che rappresenta lo stato interno del cifrario a blocchi in un round arbitrario.
La funzione ϕ è data da:

$$\begin{aligned} \phi(s_0, \ldots, s_7, k) = (&s_1, s_2 \oplus s_0, s_3 \oplus s_0, s_4 \oplus s_0, \\ &s_5, s_6 \oplus \pi'(k \oplus s_7), s_7, s_0 \oplus \pi(k \oplus s_7)) \end{aligned}$$

La trasformazione inversa per il round di decifratura del messaggio è il seguente:

$$\begin{aligned} \phi^{-1}(s_0, \ldots, s_7, k) = (&s_7 \oplus \pi(s_6 \oplus k), s_0, \\ &s_7 \oplus s_1 \oplus \pi(s_6 \oplus k), s_7 \oplus s_2 \oplus \pi(s_6 \oplus k), \\ &s_7 \oplus s_3 \oplus \pi(s_6 \oplus k), s_4, s_5 \oplus \pi'(s_6 \oplus k), s_6) \end{aligned}$$

Encryption e Decryption

Un testo in chiaro P = (P_0,…,P_7) produce un testo cifrato C = (C_0,…,C_7) con la funzione round ϕ. Si ottiene la decifratura dello stesso applicando il round inverso della stessa funzione applicata per la cifratura (ϕ^{-1}).

Per effettuare la cifratura sono necessarie le seguenti operazioni:

$$\begin{aligned} S^0 &= P \\ S^r &= \phi(S^{r-1}, (k_{8r}, \cdots, k_{8r+7})) \quad \text{for all } 1 \leq r \leq 56 \\ C &= S^{56} \end{aligned}$$

Per effettuare la decifratura sono necessarie le seguenti operazioni:

$$\begin{aligned} S^0 &= C \\ S^r &= \phi^{-1}(S^{r-1}, (k_{448-8r}, \cdots, k_{455-8r})) \quad \text{for all } 1 \leq r \leq 56 \\ P &= S^{56} \end{aligned}$$

4.4 Distribuzione delle chiavi – Gerarchia delle chiavi in un sistema CAS

Per garantire una maggiore sicurezza, spesso i sistemi dedicati alla diffusione di contenuti a pagamento utilizzano una struttura gerarchica per la distribuzione delle chiavi. Le caratteristiche di tale gerarchia variano da sistema a sistema ed attualmente non sono vincolate dallo standard utilizzato per la cifratura.
Il sistema di cifratura delle chiavi consiste nella gestione, la protezione, l'invio e l'aggiornamento delle chiavi operative. I parametri che determinano la struttura gerarchica di solito sono il numero di utenti, numero di canali, ecc. (23).
Ogni utente (abbonato) deve essere identificato univocamente per mezzo di una chiave, detta MasterPrivateKey MPK o Secret Key.
MPK e CW sono i livelli elementari di una gerarchia di chiavi di un sistema ad accesso condizionato:

- MPK ad alto livello
- CW a basso livello

Tali chiavi vengono raggruppate e trasmesse in pacchetti che permettono al gestore di interagire con ogni singola smart card mediante l'invio di due tipi di pacchetti:

- ECM (Entitlement Control Message) è un messaggio contenente la chiave cifrata (CW) necessaria al descrambling dei servizi. Se l'utente possiede le necessarie abilitazioni, la chiave decifrata viene utilizzata per controllare il descrambler e quindi riportare in chiaro il servizio richiesto.
- EMM (Entitlement Management Message) è un messaggio, indirizzato ad un utente specifico o gruppo di utenti, per abilitare o meno la visione di uno specifico servizio. Gli EMM sono anche utilizzati per attivare o disattivare uno specifico decoder o gruppo di decoder e fanno parte del sistema a chiave elettronica e di indirizzamento "over-the-air".

Questi ultimi (EMM) sono dei messaggi di gestione che i provider inviano alle card per impostarne e aggiornarne alcuni valori (Entitlements), come ad esempio la data, o per aggiungere o rimuovere Channel ID, aggiornare le key (Ciphred Keys), impostare la nazionalità della carta etc. Gli EMM possono essere indirizzati ad una singola smart card o ad un gruppo di esse (Address). Il campo MAC serve per garantire l'integrità dei dati (vedi paragrafo "integrità e verifica dei dati").

Un ECM, invece, porta con se le informazioni per decodificare un canale cifrato (Pay TV o Pay-Per-View) tramite le Control Word (Ciphred CW e Access Bitmap), è indirizzato a tutte le smart card e viene generato circa ogni 2 secondi.

Oltre MPK e CW in un sistema ad accesso condizionato sono presenti molte chiavi, ciascuna delle quali ha funzioni e caratteristiche diverse; per consentire la gestione di queste chiavi, c'è bisogno che esse siano ordinate gerarchicamente.
Esistono più sistemi gerarchici di gestione delle chiavi. Al fine di analizzare la complessità di spazio di un sistema ad accesso condizionato, bisogna introdurre due concetti fondamentali :

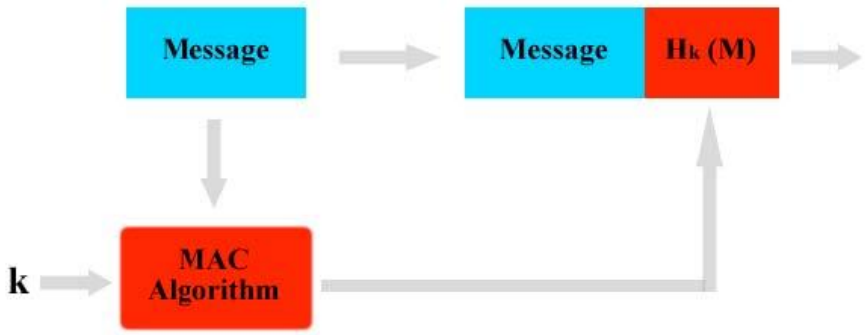
- CTU: Contract Time Unit (di solito un giorno), indica il periodo minimo di abbonamento, ma anche il massimo periodo di tempo durante il quale un nuovo utente appena registrato è autorizzato a fruire della visione gratuita dei PPC (Pay-Per-Channel).
- CTP: Contract Time Period (solitamente un mese), è riferito al periodo che intercorre tra la riscossione, da parte della pay-tv, di due quote consecutive di pagamento dell'abbonamento.

La gerarchia delle chiavi in un CAS può essere a 2, 3 o 4 livelli, ma, al fine di rendere chiare le motivazioni che lascino preferire un tipo di gerarchia ad un'altra, nei prossimi paragrafi andremo ad analizzare ognuna di queste tipologie, evidenziandone pregi e difetti, ipotesi di applicabilità e complessità.

Integrità e verifica dei dati

La verifica dell'integrità dei dati è una procedura importante nei sistemi di cifratura. Il decoder e la smart-card devono assicurarsi che i dati che si scambiano siano protetti da intrusioni esterne, e che tale procedura non venga aggirata; ciò costituirebbe un disastro in termini di sicurezza. (24) (25)
Il MAC è un checksum crittografico generato usando una chiave simmetrica, che garantisce l'integrità dei dati.
Nel grafico che segue è illustrato un esempio generico di funzionamento del MAC:

- il valore MAC, calcolato tramite l'algoritmo, viene accodato al messaggio in chiaro. Il ricevente ricalcola il MAC per il messaggio ricevuto, e lo confronta con quello che gli è stato inviato: se i due valori coincidono, il ricevente è certo che il messaggio ricevuto è uguale a quello originariamente inviato. Con questa procedura è assicurata l'integrità dei dati.



Con l'ausilio del MAC con chiave segreta, la smart card è in grado di verificare l'integrità dei messaggi scambiati (EMM – ECM) con il decoder. In questo modo non è possibile per un intruso inviare messaggi alla smart card per reperire sulla stessa dati sensibili per la visione abusiva di contenuti.

4.4.1 Gerarchia a due livelli

Il metodo più semplice, per concedere ad un utente l'autorizzazione alla visione, è distribuire le chiavi di scrambling cifrandole in base alla MPK di ciascun utente (chiave primaria che l'utente ha ricevuto durante il processo di registrazione).
Un siffatto sistema non è applicabile ad un sistema Pay-TV in quanto porta diversi svantaggi.
Primo fra tutti, il problema della sicurezza, trasmette le CW cifrandole tramite le chiavi private MPK di ciascun utente, implica la generazione di un gran numero di messaggi contenenti CW cifrate con la stessa MPK, e ciò avvantaggia gli attaccanti. In più, nel caso di sistemi con un grande numero di utenti, questo comporta un carico sulla larghezza di banda non sopportabile. In conclusione una gerarchia a due livelli è utilizzabile per dati di tipo statico a lungo termine, ma non è applicabile in un sistema che abbia un grande numero di utenti e canali.
Complessità (S = numero di abbonati attivi, T = numero di canali di tipo PPC)

Riferimento	Aggiornamento (Refresh)	Messaggi richiesti
Control word	5-20 secondi	S*T
Master Private key	Mai	Nessuno

Analizzando la tabella ci rendiamo conto che nella gerarchia a due livelli, sono necessari l'invio di S*T messaggi ad ogni refresh della CW, questo causa, nel caso di milioni di utenti abbonati, un overhead sul numero di messaggi inviati.

4.4.2 Gerarchia a tre livelli

Per ridurre il carico di messaggi da inviare ad ogni refresh delle CW, è necessario aggiungere un terzo livello fra i due livelli preesistenti: il livello di Authorization Key (AK).

La chiave AK è unica per ogni canale e varia nel tempo. Per ogni canale, l'AK viene cifrata in base alla MPK di ogni utente e trasmessa in broadcast. In tal modo ciascun subscriber sarà in grado di decifrare la chiave AK, perché ogni utente è a conoscenza della propria MPK. La ricezione da parte di un utente della chiave AK indica l'avvenuta identificazione del subscriber. Le CW vengono quindi cifrate in base alla corrispondente chiave AK relativa al canale, e inviate a ciascun utente (1 messaggio per ogni canale).
Complessità (S = numero di abbonati attivi, T = numero di canali di tipo PPC)

Riferimento	Aggiornamento (Refresh)	Messaggi richiesti
Control word	5-20 secondi	T
Authorization Key	Circa un CTP	S*T
Master Private key	Mai	Nessuno

In questa gerarchia a tre livelli, sono necessari l'invio di T messaggi ad ogni refresh della CW e S*T messaggi per l'AK, che varia in un CTP. Si ha un miglioramento delle prestazioni in quanto non vengono inviati S*T messaggi ad ogni refresh della CW come avviene nella gerarchia a due livelli, ma solo ogni CTP.
Una gerarchia a tre livelli non è indicata per sistemi con milioni di utenti e centinaia di canali, ma può essere utilizzata in due casi: PayPerView (PPV) e Sistemi con pochi canali o con pochi gruppi esclusivi di canali.
Lo standard ITU Rec.810,1992, definisce una gerarchia di chiavi a tre livelli.

4.4.2.1 Pay Per View

Per poter fruire di un canale in PayPerView ciascun utente deve poter collegarsi al sistema, ad esempio tramite linea telefonica (modem). Avvenuto il processo di identificazione, il sistema cifra la chiave AK con la MPK dell'utente e la invia in broadcast (n.b. la chiave di autorizzazione AK viene aggiornata ad ogni evento PPV).
Dato che l'utilizzo eccessivo della MPK potrebbe arrecare danni alla sicurezza del sistema, un'ulteriore chiave potrebbe essere necessaria (midterm key), oppure si potrebbe ricorrere ad un sistema di firma digitale.

4.4.3 Gerarchia a quattro livelli

Per superare gli svantaggi delle gerarchie a due e tre livelli, nell'articolo (23) viene proposta una gerarchia a quattro livelli.
Per sistemi con largo numero di utenti e canali, la gerarchia a tre livelli implica la necessità di trasmettere T * S messaggi ad ogni refresh delle chiavi AK; per ridurre tale carico, c'è bisogno di un quarto livello aggiuntivo, il "Group Key" (gli utenti sono classificati in G gruppi, in base ai canali di cui si ha diritto alla visione).
Le chiavi di ciascuno dei quattro livelli sono utilizzate per cifrare e distribuire le chiavi del livello successivo. Ciascun utente riceve la Group Key cifrata con la sua MPK, per un totale di S messaggi.
La chiave AK di ciascuno dei T canali è cifrata tramite la Group Key e trasferita in un messaggio di tipo EMM, che viene indirizzato in broadcast agli S utenti (classificati in G gruppi).
Le chiavi CW vengono cifrate tramite le chiavi AK e inviate in broadcast a ciascun utente.

Complessità (S = numero di utenti attivi, T = numero di canali e G = numero di gruppi di subscribers attivi)
Nella tabella il numero di messaggi in totale richiesti per distribuire le AK è (T * G) + S, mentre nella gerarchia a tre livelli era T * S.
Questo rappresenta un notevole miglioramento in quanto G è sicuramente minore di S, essendo gli utenti attivi (S) raggruppati in G gruppi.

Riferimento	Aggiornamento (Refresh)	Messaggi richiesti
Control word	5-20 secondi	T
Authorization Key	Circa un CTP	T*G
Group Key	Circa un CTP	S
Master Private key	Mai	Nessuno

Un'ulteriore riduzione del carico di messaggi da spedire si può ottenere raggruppando i canali di un sistema pay-tv in “bouquet” (insiemi disgiunti di canali tematici): gli utenti possono sottoscrivere abbonamenti ad uno o più bouquet (Sport, Cinema, Hot Club ecc...). In questo scenario, ai canali di uno stesso bouquet è associata la stessa chiave AK.
Complessità (S = numero di utenti attivi, T = numero di canali, G = numero di gruppi di subscribers attivi, B = numero di bouquet)
Dalla tabella è possibile notare un'ulteriore miglioramento sul numero di messaggi contenenti le chiavi AK e CW: B (numero di bouquet) è minore di T (numero totale di canali)

Riferimento	Aggiornamento (Refresh)	Messaggi richiesti
Control word	5-20 secondi	B
Authorization Key	Circa un CTP	B*G
Group Key	Circa un CTP	S
Master Private key	Mai	Nessuno

Al fine di minimizzare il traffico di messaggi di tipo EMM, si può operare una “rimappatura” per ridistribuire omogeneamente i vari gruppi di utenti. Un gruppo di utenti si dice attivo se vi appartiene almeno un subscriber con smart card attiva.
Una smart card è attiva se non si è ancora raggiunta la data di scadenza dell'abbonamento. Lo scopo della rimappatura è evitare gruppi sparsi, ovvero gruppi con poche smart card attive. In presenza di gruppi sparsi, il Service Provider analizza i gruppi di utenti e trasferisce le smart card da un gruppo ad un altro, in modo da ottenere il minimo numero di gruppi con il massimo numero di smart card attive per gruppo.

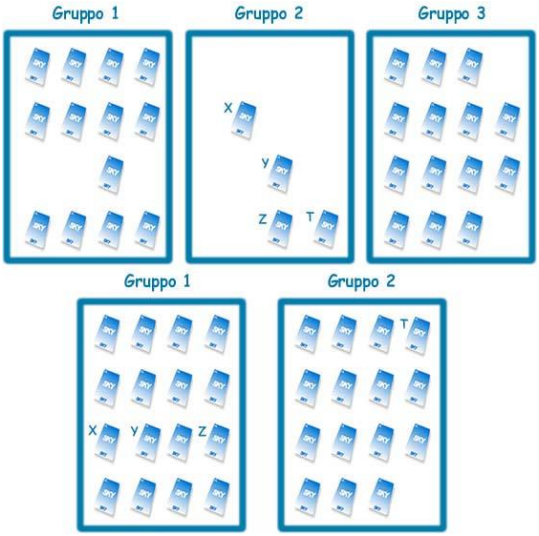


Figura 21: Esempio di rimappatura

4.5 Tecniche di Scrambling

La sicurezza in un sistema di scrambling si misura in base a quanto risulta semplice rispondere ad un attacco.
Inizialmente si pensò ad un'architettura di tipo Embedded Secure Microcontroller (ESM):

- il controllo principale sul decoder era inserito proprio nei circuiti del decoder stesso, ma risultava debole nella stessa misura in cui lo è un chip.

Per questo un siffatto sistema non garantiva la sicurezza richiesta: un chip poteva essere considerato sicuro solo per pochi mesi, in quanto, essendo posto nel decoder, era sotto il completo controllo dell'abbonato, che avrebbe potuto aprirlo ed esaminarlo senza che il Service provider se ne accorgesse e potesse porvi rimedio.
Si rese quindi necessario l'utilizzo di un'architettura che ovviasse ai suddetti svantaggi (Detachable Secure Microcontroller - DSM):

- in questo modello si è pensato di introdurre l'elemento principale di controllo separato dal decoder e facilmente aggiornabile e verificabile dal Service Provider.

Nasce così il concetto di smart card applicata alla visione dei canali satellitari. In sistemi del genere il decoder non contiene segreti del sistema e, anche se attaccato, non produce benefici all'hacker.
Di conseguenza gli hacker non attaccano più il decoder ma iniziano a sperimentare attacchi alle smart card, elemento principale che garantisce o nega la visione.
In questo paragrafo illustreremo le tecniche di scrambling a partire dalle quali si sono poi sviluppate quelle utilizzate dagli odierni sistemi per le tv digitali. Tutte le operazioni applicate al segnale audio/video sono trasparenti all'utente finale: il Service Provider effettua lo Scrambling e trasmette al Subscriber il segnale, che viene ricostruito dal descrambler. Nel caso in cui l'utente non ha acquisito i diritti per la visione e le informazioni per effettuare il descrambling (CW), il Conditional Access System non procede al descrambling e non dà in output nessun segnale video. Un pirata che dovesse riuscire in qualche modo ad ottenere comunque il segnale audio/video, non essendo a conoscenza delle informazioni di scrambling e della CW, non sarebbe in grado di ricostruire l'immagine a video, ottenendo in output l'immagine scramblata.

4.5.1 Cut and Rotate

Nei sistemi che utilizzano questa tecnica la linea, che rappresenta l'immagine digitalizzata, viene tagliata in un dato punto e le due sezioni vengono ruotate in modo che l'ultima sezione diventi la prima e viceversa. E' un metodo abbastanza sicuro, ma il punto di taglio deve essere segreto. Il punto di taglio viene stabilito da un generatore di numeri pseudo-casuale e trasmesso in forma cifrata. La sicurezza è garantita dall'alta frequenza di generazione dei punti di taglio.

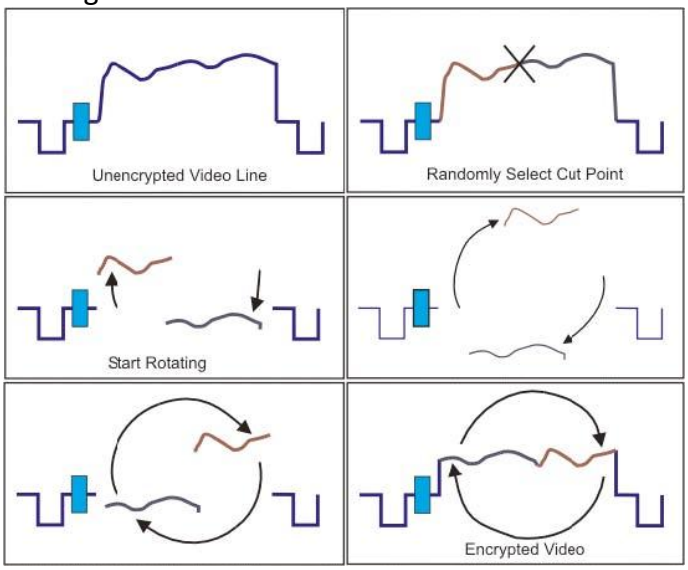


Figura 22: Cut and Rotate

4.5.2 Line Shuffle

L'immagine di scrambling viene rappresentata a righe, che vengono permutate tra di loro in maniera pseudo-casuale, nonostante il contenuto dell'intera immagine risulti inalterato.

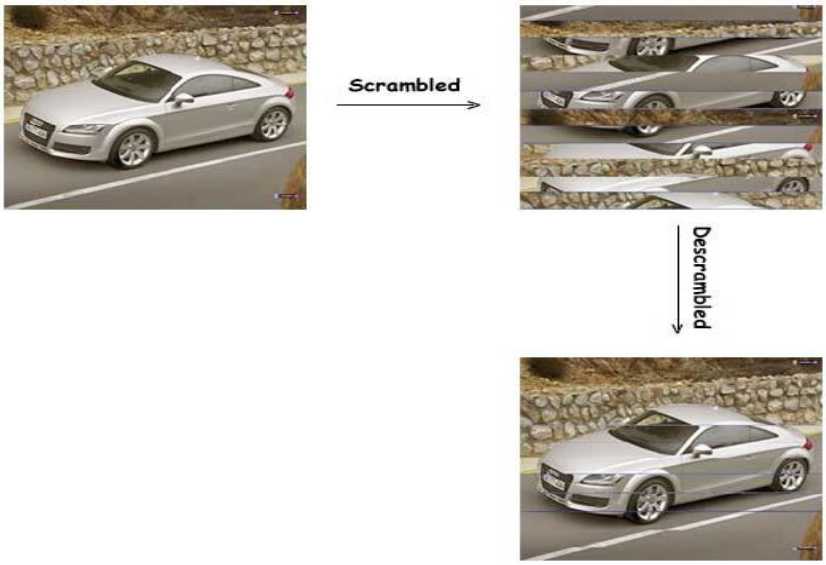


Figura 23: Line Shuffle

Per attaccare questa tecnica di scrambling, l'hacker dovrebbe riuscire a conoscere, in tempo ed ogni volta, l'ordine con cui le righe vengono scambiate. Questa tecnica richiede un carico di memoria eccessivo, e quindi implica l'impiego di un decoder più costoso che la possa gestire correttamente. Una valida alternativa potrebbe essere dividere ciascuna linea in linee di ampiezza minore e scambiarle fra loro. Quest'approccio risulta essere più economico, pur conservando lo stesso livello di sicurezza di quello originale.

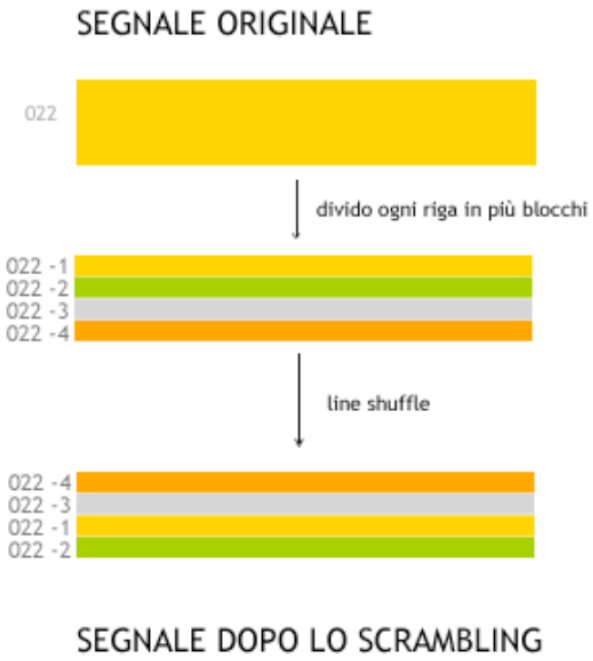


Figura 24: segnale dopo scrambling

Capitolo 5: Panoramica Codifiche DVB

5.1 Il sistema Irdeto

5.1.1 la Smart card Irdeto

La SmartCard Irdeto è una scheda "intelligente" che ci permette di vedere "in chiaro" i programmi che vengono trasmessi "cifrati" con il sistema Irdeto. Questo vuol dire che se si sottoscrive un abbonamento ad una PayTV (PTV) che trasmette con codifica Irdeto, ci verrà fornita una SmartCard che ci permetterà di vedere in chiaro i canali di quella PTV per i quali ci siamo abbonati. (26)
La scheda per funzionare correttamente ha bisogno di una "controparte", che si chiama CAM (Modulo di Accesso Condizionato), anche esso deve essere compatibile con lo standard Irdeto, insieme questi due moduli permettono la visione in chiaro della PTV. All' interno della SmartCard è presente un microprocessore di tipo TamperedProof (a prova di scasso), questo vuol dire che se proviamo fisicamente ad estrarre il microprocessore dalla scheda, esso si autodistruggerà, la stessa triste fine la otterremmo se tentassimo di estrarre completamente tutti i dati (lettura fisica di tutta la scheda) dalla SmartCard.
A questo punto evinciamo che l'unica maniera per interagire con la scheda è quella di comunicare tramite il set di istruzioni utilizzate per lo scambio di informazioni tra CAM e SmartCard, l'unico problema è che IRDETO si guarda bene dal rendere pubbliche queste informazioni, quindi l'unica maniera per tentare di capire come funziona questo processo è quella di analizzare il flusso delle informazioni che transitano tra CAM e SmartCard e compilare poi una specie di reference-guide. A complicare il discorso è il fatto che esistono naturalmente più versioni del sistema operativo (ACS) Irdeto caricato sulla SmartCard, si è scoperto che la maggior parte dei comandi viene comunque accettato a prescindere dalla versione del sistema operativo, la programmazione viceversa no.

5.1.2 Funzionamento in dettaglio di una smart card Irdeto

Una volta inserita nel decoder, si instaura una comunicazione tra CAM e SmartCard, a grandi linee avviene questo:
La CAM invia un reset alla SC che le risponde inviando la versione del sistema operativo, la CAM poi richiede alla scheda di identificarsi con il serial number (ascii ed esadecimale), e con altre informazioni riguardanti l'emittente, il paese (Italia, Germania ecc. ecc.), poi la CAM invia la propria chiave, le chiavi di decodifica per la smart-card inserita ed un comando contenente l'identificativo del canale (Channel-ID) e la chiave di decodifica del canale cifrata.
A questo punto la SmartCard opera delle verifiche con le chiavi in suo possesso se le verifiche sono positive, la SmartCard dà l'OK per la visione del canale e fornisce la chiave di decodifica alla CAM, quindi la CAM comincia la decodifica.
La SmartCard non fa che cifrare con un algoritmo DES-Like la/le chiavi di canale che la CAM invia con il comando 01 05 utilizzando come chiavi di codifica la PlainKey relativa al canale selezionato e la data, il risultato di questa cifratura viene ricifrata utilizzando la chiave che la CAM aveva inviato precedentemente con il comando 01 02, il tutto viene inviato come risposta al comando 01 0..
Esaminiamo ora quali sono le informazioni fondamentali che servono ad una SmartCard Irdeto per funzionare :
Ogni SmartCard "IRDETO" viene identificata da un numero seriale esadecimale HexSerial :

- HEX SERIAL - lunghezza 3 bytes

In Ogni SmartCard possono essere memorizzati due Providers o Emittenti, essi sono identificati con i numeri "00" o "10"

- PROVIDER - lunghezza 1 byte

Ad ogni Provider viene associata una data DateStamp di sistema che viene aggiornato automaticamente dall'emittente :

- DATE-STAMP - lunghezza 2 byte

Tramite l'Hex Serial si ottengono dal Provider della SmartCard una MasterKey ed un ProviderID, la MasterKey è la chiave associata al ProviderID (o meglio è associata al ProviderGroup come vedremo nel prossimo passo, quindi è valida per i 256 ProviderID appartenenti allo stesso ProviderGroup) memorizzato in uno dei due Provider ("00" o "10", generalmente lo "00") ed una volta decifrata (PlainMasterKey) è la chiave utilizzata per la decifratura delle KeyProviderGroup. Il Provider-ID puo' essere cambiato o modificato solo fornendo la sua MasterKey (pena la mancanza di aggiornamenti):

- MASTER KEY - lunghezza 8 bytes
- PROVIDER-ID - lunghezza 3 bytes

Il ProviderID è composto dal ProviderGroup che occupa i primi 2 bytes del ProviderID :

- PROVIDER-GROUP - lunghezza 2 bytes

Il restante byte del ProviderID è chiamato CardId o CustomerId ed identifica l'utente del provider :

- CARD-ID o CUSTOMER-ID - lunghezza 1 byte

Ad Ogni ProviderGroup vengono associate diverse KeyProviderGroup che sono delle chiavi di decrittazione dei vari programmi del Provider, queste chiavi vengono inviate in forma cifrata, verranno poi decifrate all'interno della scheda tramite la PlainMasterKey e la KeyDateStamp e memorizzate in opportune locazioni di memoria :

- KEY-PROVIDER-GROUP - lunghezza 1+8 byte

Il primo byte di ogni KeyProviderGroup è il KeyIdentificator ed è l'identificatore della chiave stessa, questo ci informa della funzione della chiave (es. decifra la PayPerView), il KeyIdentificator non è utilizzato nella chiave, è solo un suo descrittore, infatti la chiave vera e propria è lunga solo 8 bytes :

- KEY-IDENTIFICATOR - lunghezza 1 byte

Ad ogni KeyProviderGroup è associata una data KeyDateStamp

- KEY-DATE-STAMP - lunghezza 2 byte

Attenzione al DateStamp, il DateStamp di sistema normalmente è relativo ai due Provider ed ai relativi Provider-ID, infatti ci sono due DateStamp nella SmartCard, uno per il Provider 00 ed una per il Provider 10. Alla KeyProviderGroup è associato un suo relativo KeyDateStamp (che è il DateStamp del provider della chiave nel momento in cui viene trasmessa la chiave stessa), nelle versioni di ACS 1.6 per inserire una KeyProviderGroup bisogna prima aver modificato il DateStamp di sistema del relativo Provider con il KeyDateStamp loggato insieme alla chiave.

Solo dopo aver modificato il DateStamp di sistema del provider con il KeyDateStamp si può inserire la KeyProviderGroup. Un altro DateStamp viene fornito alla scheda quando andiamo ad abilitare i Channel-ID, questo DateStamp è relativo solamente ai Channel-ID e non è da confondere con il DateStamp di sistema. Ogni canale o gruppo di canali di un Provider viene identificato da un Channel-ID, questo è lungo 2 bytes

- CHANNEL-ID – lunghezza 2 bytes

Ad Ogni Channel-ID viene associato un suo Channel-DateStamp anche esso lungo 2 bytes ed una relativa Expiration-Date lunga anche essa 2 bytes che sta ad indicare quando tale canale non sarà più visibile in chiaro (es. scadenza dell'abbonamento, eventi in PPV, ecc. ecc.)

- CHANNEL-DATE-STAMP – lunghezza 2 bytes
- EXPIRATION-DATE – lunghezza 2 bytes

Gli aggiornamenti dei canali, le chiavi di provider, ecc.ecc. vengono fornite dall'emittente direttamente al provider-id della scheda, le chiavi finali di decrittazione dei canali (PlainKeys) vengano estratte da un opportuno algoritmo di decodifica che prenda in pasto la PlainMasterKey, le KeyProviderGroup ed il KeyDateStamp. Queste chiavi vengono poi memorizzate in specifici registri di memoria della SmartCard che differiscono tra di loro a seconda della versione del sistema operativo.
Il gestore comunque invia periodicamente alla scheda identificata dall'HexSerial la sua MasterKey relativa al suo Provider-ID, questo fa in modo che anche se volessimo modificare la coppia prov-id e masterkey dopo un certo periodo di tempo ci ritroveremmo con i valori originali. Due parole sulla MasterKey, la MasterKey viene inviata anch'essa in forma cifrata, una volta decifrata all'interno della SmartCard (PMK, PlainMasterKey), scopriamo che al contrario delle KeyProviderGroup non è uguale per tutte le schede ma bensì per gruppi di 256 schede e quindi per ProviderGroups, si è scoperto che è grazie alla PlainMasterKey ed alla KeyDateStamp che la SmartCard opera la decodifica delle KeyProviderGroup in PlainKey.
Attenzione alla Key 00, erroneamente per diverso tempo essa è stata confusa con la PlainMasterKey, da verifiche effettuate sembra invece che sia una PlainKey che viene inserita direttamente dal costruttore, viene utilizzata a volte per la decodifica di alcuni channel-id, per ora non se ne conosce la posizione in memoria ne come dumparla o procurarsela. A questo punto bisogna parlare delle schede con provider-id 0300/0400, queste smartcard sono delle schede di tipo particolare, o sono il frutto di un ECM (Contromisura Elettronica) inviata dal gestore oppure sono delle schede mai inizializzate dal gestore stesso (schede nuove in attesa di attivazione o schede del tipo Welcome Kit).

5.2 Il sistema Seca

5.2.1 Breve storia

La prima società europea ad offrire un pacchetto di canali (bouquet) a pagamento fu la britannica Sky Tv nel 1990. Le trasmissioni avvenivano via satellite in analogico e, sebbene riservate alla sola
Gran Bretagna, erano ricevibili in quasi tutta l'Europa. La codifica veniva effettuata col Videocrypt, un sistema ibrido in cui lo scrambling (del solo video, in quanto Sky preferiva lasciare l'audio in chiaro) veniva effettuato con la tecnica del cut and rotate, mentre la generazione, codifica e gestione delle relative chiavi avvenivano per mezzo di tecniche digitali . Nel 1994, il tedesco Markus Kuhn, un giovane informatico esperto di sistemi per l'accesso condizionato, riuscì a mettere in chiaro l'intero bouquet in vari modi: operando sull'algoritmo di scrambling senza l'ausilio delle chiavi (in questo caso l'immagine veniva visualizzata solo in bianco e nero), con una smart card "clonata" che emulava perfettamente quella originale e, infine, sostituendo la smart card con un PC dotato di apposito software e collegato al decoder. Kuhn diffuse i risultati della sua ricerca attraverso le BBS ed Internet, così il fenomeno della visione abusiva cominciò a prendere piede in tutta l'Europa occidentale. Le conoscenze tecniche diffuse da Kuhn, stimolarono la creazione di diversi gruppi di studio delle codifiche delle TV a pagamento via satellite, che operavano a stretto

contatto, scambiandosi i risultati delle loro ricerche. La sinergia portò alla forzatura del sistema D2-MAC/Eurocrypt, utilizzato dall'operatore scandinavo Viasat e dal francese CanalPlus, nonostante cifrasse le chiavi col DES.
Nel 1996 cominciarono le trasmissioni digitali via satellite, causando un progressivo abbandono della tecnica analogica. La prima società europea ad offrire un bouquet digitale a pagamento via satellite fu la francese Canal Satellite Numérique (CSN) del gruppo CanalPlus nel 1996. Le trasmissioni venivano codificate col sistema Mediaguard realizzato dalla società SECA, appartenente allo stesso gruppo, riprendendo alcuni concetti del D2-MAC/Eurocrypt. Seguirono, subito dopo, l'italiana D+ e la tedesca DF1 che codificavano le trasmissioni col sistema Irdeto. Nel 1998, dopo soli due anni dall'avvento della TV digitale a pagamento, la pirateria era già in grado di forzare tutte le codifiche. La prima a cedere è stata Irdeto, seguita da Seca. Il sistema di codifica SECA è stato originariamente utilizzato in Italia nel 1997 da Telepiù che, allora, era una società controllata da Canal Plus, la cui affiliata, Canal Plus Technologies, ha fornito il sistema. La prima versione utilizzata da SECA era nota come SECA Mediaguard I, e, nel maggio 2002 , è stata rimpiazzata da SECA II. Nel luglio 2003 Canal Plus Technolgies è stata acquisita da Thomson e nel gennaio 2004 il business è stato acquistato da Nagra. SKY Italia è nata il 1 maggio 2003 dalla fusione di Telepiù e Stream ad opera del magnate Rupert Murdoch. All'epoca Stream utilizzava i sistemi di codifica Irdeto, SECA ed NDS. SKY ha abbandonato il sistema di codifica Irdeto nel febbraio 2004. Il numero degli abbonati a SKY ha superato i 3 milioni e 830 mila nel giugno 2006, con un incremento delle sottoscrizioni di oltre 1 milione e 900 mila famiglie nei primi due anni e mezzo di presenza sul mercato italiano.

5.2.2 Gerarchia delle chiavi e comunicazione della smartcard

Il sistema di chiavi Seca è molto complesso ed è basato su una chiave, chiamata "Crypted Controlword" (Parola di controllo codificata, CW), di otto byte. Da questa chiave si ottiene la cosiddetta "Decrypted Controlword" (Parola di controllo decodificata, DW). Per effettuare questa operazione sono necessarie altre due chiavi : "Primary Key" PK (chiave primaria) e "Secondary Key" SK (chiave secondaria). Queste ultime due chiavi sono utilizzate insieme a formare una chiave di 16 bytes, usata per decifrare la chiave di controllo. Ci sono altri due set di chiavi oltre quelle elencate: la "Operational Key" OK (chiave operativa) e la "Managment Key" MK (chiave di amministrazione). La chiave operativa è quella che effettivamente mette in chiaro il canale sintonizzato, mentre la chiave amministrativa è quella che si occupa di cambiare automaticamente la chiave operativa, secondo le direttive del broadcaster. L'operazione di modifica della chiave operativa ad opera della chiave amministrativa è chiamata Auto Update (AutoAggiornamento). Per finire, ma non per questo meno importanti, sono da menzionare le "Provider Keys" (chiavi del gestore) e le "SECA Keys" (chiavi del SECA). Le prime sono le chiavi che consentono al provider di attivare, modificare e disabilitare la smartcard, mentre le seconde sono le chiavi che autorizzano ad effettuare cambiamenti sulla smartcard, a tutti i livelli. Va precisato che, mentre possono esistere Provider Keys per un solo gestore, con le giuste SECA Keys si possono aggiungere e rimuovere più providers e non solo modificarli (canali facenti parte del bouquet, ma appartenenti ad altro provider o broadcaster). Ogni Smartcard è caratterizzata da un numero di serie, riprodotto sulla superficie della Smartcard stessa in forma decimale, ed anche all'interno del suo chip mediante 8 byte esadecimali; questo seriale è comunemente chiamato UA (Unique Address). Altri dati sono il PPUA (4 Byte, di cui i primi 3 sono lo SA [Shared Address] e il 4° byte è il CWP [CustomWord Pointer] e il PBM (PackageBitMap – 8 Byte). Il PPUA identifica un abbonato, o un gruppo di abbonati mediante il CWP; serve per

l'aggiornamento delle OK (Operational Key) quando queste vengono cambiate dal gestore. Il PBM invece è una matrice con cui viene definito il tipo di abbonamento, ovvero specifica a quali pacchetti TV un utente è abbonato. Le Management Key sono chiavi che permettono di decodificare le nuove Operational Key quando queste vengono cambiate e inviate in forma cifrata alla Smartcard, che, mediante un algoritmo e il PPUA, le aggiorna in eeprom. La chiave di tipo Data è relativa alla data di scadenza dei diritti di visione e viene aggiornata col cambio di Operational Key. Solitamente le PayTV, che utilizzano il sistema di codifica Seca, cambiano mensilmente le Operational Key e relativa Data, e molto raramente Management Key e PPUA. Una Card con MK e PPUA validi è in grado di autoaggiornarsi al cambio delle OK; inoltre, per renderla autoaggiornante anche al cambio di MK e PPUA, è necessario avere l'Unique Address. Riepilogando, i dati utili sono:

- UA (Unique Address - 8 Byte hex o un numero decimale scritto sulla Smartcard)
- PPUA (4 Byte)
- MK (ManagementKey - 8 Byte) che può assumere valori da MK00 a MK0B
- OK (8 Byte) che può assumere valori da 0C a 0D
- PBM (PackageBitMap - 8 Byte)
- DATE (2 Byte)

N.B. In realtà la codifica Seca prevede l'uso della doppia Key, cioè le key di tipo MK e OK sono doppie; in tal caso si parla di MK Primaria ed MK Secondaria, stesso discorso per le OK. L'utilizzo della doppia key è a totale discrezione della PayTV, per rendere il sistema di codifica meno vulnerabile.

5.3 Il sistema VideoGuard (NDS) in breve

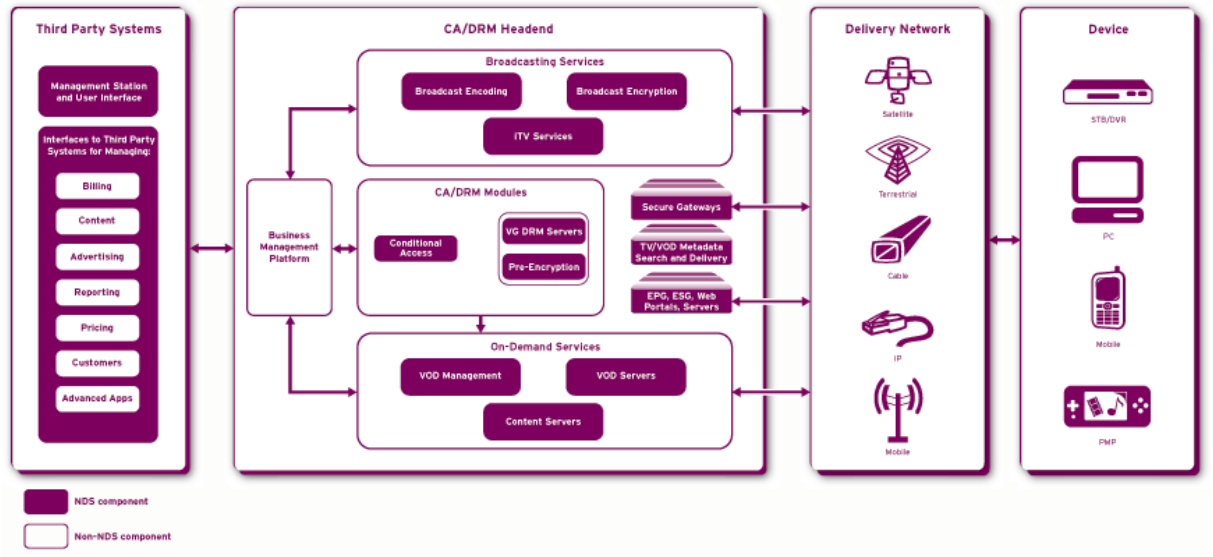


Figura 25: struttura NDS

VideoGuard, prodotto dalla società **NDS** Group , è un sistema di accesso condizionato per televisioni a pagamento. È usato maggiormente nelle trasmissioni digitali via satellite (DVB-S) del gruppo News Corporation, che possiede la maggioranza di NDS. È stata implementata per la prima volta con la piattaforma British Sky Broadcasting (BSkyB), che trasmette per Gran Bretagna e Irlanda. Molte altre compagnie televisive trasmettono in tutto il mondo con il sistema VideoGuard, tra cui: Viasat (Scandinavia), Sky Italia e Foxtel (Australia).
Dato che la maggior parte dei contenuti forniti dalle televisioni a pagamento richiede un abbonamento, il sistema VideoGuard protegge i contenuti, codificando sia i canali in abbonamento, sia i canali visibili in pay per view (ad esempio film di prima visione o eventi sportivi). I diritti di accesso sono "caricati" sulla smart card dell'abbonato sia "on air" (tramite segnali di controllo inviati assieme alle trasmissioni), sia tramite la tradizionale linea telefonica, sfruttando il modem integrato nel ricevitore: in questo modo è possibile ordinare facilmente eventi in pay per view oppure aggiungere opzioni e pacchetti aggiuntivi al proprio abbonamento.
In Gran Bretagna, il sistema VideoGuard è stato introdotto da News Corporation per sostituire il vecchio sistema analogico VideoCrypt. Attualmente il sistema non è ancora stato violato, anche se sembra che sia stato possibile clonare le smart card. È probabile che la prima implementazione del sistema fosse poco sicura, poiché vicina alla violazione, quindi il broadcaster BSkyB ha provveduto alla sostituzione di tutte le smart card dei propri abbonati, oltre all'aggiornamento di tutti i ricevitori con un nuovo software in grado di leggere le nuove schede.
In Italia, Il sistema di decodifica VideoGuard ha sostituito i precedenti sistemi SECA Mediaguard e Irdeto che venivano utilizzati rispettivamente per le emittenti Tele+ e Stream (ora rimpiazzate da SKY).
A differenza di molti altri broadcaster satellitari, i canali di News Corporation possono essere ricevuti ufficialmente soltanto tramite un decoder proprietario, nel quale la tecnologia VideoGuard è implementata internamente. A causa del controllo di News Corporation sulla tecnologia, è impossibile ottenere una licenza per l'implementazione di modulo di accesso condizionato (conditional access module o CAM) di terze parti compatibili con VideoGuard. Questa situazione è vista da molti come un monopolio, usato per favorire soltanto alcuni

produttori di set top box (ad es. PACE o Philips). In diretta contrapposizione, tutti gli altri sistemi di codifica (Ad es. Irdeto, Nagravision, Viaccess) mettono a disposizione CAM hardware e/o software per la fruzione di canali a pagamento). Attualmente, neanche in Italia, con la legge del decoder unico, abrogata nel 2005, che imponeva l'utilizzo di un solo decoder per fruire dei contenuti a pagamento, si è riusciti a sbloccare questa situazione. Da diverso tempo però, Sky Italia fornisce il decoder "base" in comodato d'uso gratuito ai propri abbonati.
Nel 2005, un produttore di hardware è riuscito ad effettuare un parziale reverse engineering di Videoguard, al punto che una card ufficiale può essere utilizzata in un decoder common interface (molto spesso è necessario però aggiornarne il firmware), per fruire della visione dei canali per la quale si è regolarmente pagato. È stato reso disponibile anche un emulatore software di CAM VideoGuard per i decoder satellitari Dreambox (basati su Linux). In ogni caso, spesso i broadcaster aggiungono un controllo aggiuntivo, accoppiando il numero seriale del ricevitore con la smart card. Come risultato, i programmi possono essere fruiti soltanto con il decoder abilitato, anche se la protezione è facilmente aggirabile con una delle soluzioni ottenute dal reverse engineering.
SKY Italia trasmette in chiaro (quindi senza codifica VideoGuard) solamente i canali di servizio SKY Inside.
Il sistema VideoGuard (NDS) può essere, attualmente, aggirato con la tecnica del **Card-Sharing** (che ne parleremo brevemente nel capitolo 6).

CAPITOLO 6:

6.1. Introduzione

In questo capitolo parleremo della pirateria della televisione a pagamento nel paragrafo 5.2, introdurremo una breve storia sull'evoluzione della pirateria digitale satellitare. Si parlerà delle tecniche utilizzate per la visione abusiva, tra queste quella di maggiore interesse e che in questo testo citeremo solo per titolo informativo è la tecnica del card-sharing che è l'unica tecnica oggi in grado di poter usufruire della visione dello stesso pacchetto di programmi per più utenti utilizzando una sola carta regolarmente abbonata. Verranno illustrate i tipi di smart card che negli anni sono state utilizzate dai pirati e i relativi programmatori hardware utilizzati. Nella parte finale del capitolo verranno trattati i motivi del successo della pirateria satellitare e le eventuali proposte per combatterla, evidenziando i successi che le forze dell'ordine hanno effettuato negli anni.

6.2. La pirateria della televisione a pagamento

Le PayTV codificano lo stream DVB (Audio/Video digitale in forma compressa) mediante sistemi di cifratura (Irdeto, Seca, Seca2, Viaccess, NDS, etc.) (27).
Per la decodifica dello stream cifrato e la relativa messa in chiaro della trasmissione, non basta avere un decoder digitale, ma occorre anche un Modulo di Accesso Condizionato (CAM) che, dopo aver effettuato con successo la procedura di autenticazione della smart card, ne permette la visione.
In pratica la combinazione CAM/smart-card opera sulla decodifica.
La televisione a pagamento è un servizio ad accesso condizionato che consiste nella visione di programmi televisivi riservata ai soli utenti autorizzati in quanto paganti.
Attualmente tale servizio viene erogato in due modalità:

- **pay-tv**, che permette la visione di specifici canali per un determinato periodo di tempo (tipicamente un anno) pagando il relativo abbonamento;
- **pay per view**, che permette la visione di un singolo evento (un film, una partita o un concerto) pagando il relativo costo.

La tv a pagamento si avvale di un apposito sistema per l'accesso condizionato (Conditional Access System) che consente la cifratura del segnale audio/video da parte della stazione emittente e la sua decifratura da parte dei soli utenti autorizzati.
Le tv a pagamento sono soggette a continui attacchi critto analitici, o di altra natura, che hanno l'obiettivo di mettere in chiaro i programmi per consentirne la visione anche a coloro che non sono autorizzati in quanto non paganti.
Tali azioni non possono essere classificate in alcuna forma di hacking, né di tipo tecnologico, né, tantomeno, ideologico.
Il loro obiettivo non è quello di approfondire la conoscenza tecnica del sistema (hacking tecnologico), né quello di testare la sua forza nei confronti di un attacco (hacking etico) e, né, tantomeno, quello di rendere pubbliche e condivise informazioni o conoscenze riservate a pochi (hacking sociale).
Vanno invece considerate come azioni di cracking con chiari scopi commerciali consistenti nella vendita o nella modifica di sistemi per la ricezione non autorizzata delle tv a pagamento.
Le analisi svolte sia da società indipendenti sia dagli stessi operatori del settore risultano discordanti riguardo l'entità del problema, ma presentano tutte un quadro allarmante.

Nel 2003, in Europa (compresa quella dell'Est dove il fenomeno è in rapida crescita), sembra siano stati venduti sistemi per la visione abusiva per la ragguardevole cifra di un miliardo di Euro.
Le società televisive e i vari Stati hanno subito danni per svariati miliardi di Euro per mancati abbonamenti e per mancati introiti fiscali mentre i posti di lavoro persi per mancati investimenti sono stati diverse migliaia.
Analoga, se non più grave, è la situazione di tutto il continente americano.
Da più parti si ritiene che un'attività così diffusa sia gestita da una rete internazionale di organizzazioni criminali, di cui fanno parte anche tecnici altamente qualificati e specializzati, che possono così realizzare lauti guadagni generando una pericolosità sociale molto bassa se non nulla. Tutte queste connotazioni hanno finito col rendere comunemente noto il fenomeno come pirateria della tv a pagamento.
In termini più propriamente tecnici, la tassonomia IBM definisce i pirati come attaccanti di classe III, ossia organizzazioni consolidate composte da tecnici con conoscenze specialistiche ma integrabili e con considerevole disponibilità di risorse che sanno analizzare in dettaglio sistemi, usare tecnologie e prodotti avanzati e progettare attacchi molto sofisticati.
La situazione attuale potrebbe divenire ancora più grave con la graduale introduzione della tv digitale terrestre che sta interessando quasi tutti i paesi dell'Europa occidentale e alcuni dell'orientale.
Questa nuova tecnologia, che affiancherà la tv digitale via satellite e via cavo, permetterà la trasmissione di programmi televisivi via etere utilizzando le antenne terrestri già esistenti.
Rispetto alla tv analogica terrestre, il numero di canali aumenterà in maniera considerevole e molti saranno a pagamento.
I Paesi interessati stanno effettuando sperimentazioni a livello nazionale, regionale o urbano, da tempo più o meno considerevole, per poter effettuare il definitivo passaggio dall'analogico al digitale in un arco di tempo molto ampio che va dal 2006 al 2010-2012.
Dopo la città di Berlino, che è stata la prima ad aver completato il passaggio nell'agosto del 2003, l'Italia dovrebbe essere il primo Paese a convertirsi completamente alla nuova tecnologia.
Infatti la Legge 3 maggio 2004, n. 112, recante norme di principio in materia di (ri)assetto del sistema radiotelevisivo, meglio nota come Legge Gasparri, prevede che il passaggio debba avvenire entro il 2006.
Mediaset ha già acquisito i diritti per la trasmissione in pay per view delle partite interne di alcune squadre di calcio di serie A, a partire dal 2005.
Nei paesi scandinavi, dove la sola Norvegia ha legiferato il passaggio entro il 2007, vengono già offerti alcuni canali a pagamento.
La Gran Bretagna è stata la prima nazione a sperimentare il digitale terrestre ed ha previsto la conversione entro il 2010.
Intanto, dopo il fallimento di ITV, la prima tv digitale terrestre a pagamento europea, è attiva Top Up Tv con un'offerta di una decina di canali tematici a pagamento. In Francia, le prime tv a pagamento dovrebbero iniziare le trasmissioni nel settembre 2005.
La copertura della tv digitale terrestre è limitata al solo territorio nazionale di ogni singolo Stato al pari di quella via cavo e non all'intera Europa come quella via satellite ma i canali tematici a pagamento potrebbero risultare molto appetibili per la pirateria.
Sarebbe opportuno cercare di limitare questo rischio con interventi urgenti di natura culturale, legislativa e tecnica.

6.3. Breve storia della pirateria

La prima società europea ad offrire un pacchetto di canali (bouquet) a pagamento fu la britannica Sky Tv nel 1990 (negli Stati Uniti il primo bouquet fu proposto da Hbo nel 1986 con codifica VideoChiper violata dopo soli sei mesi).
Le trasmissioni avvenivano via satellite in analogico e, sebbene riservate alla sola Gran Bretagna, erano ricevibili in quasi tutta l'Europa.
La codifica veniva effettuata col Videocrypt, un sistema ibrido in cui lo scrambling (del solo video in quanto Sky preferiva lasciare l'audio in chiaro) veniva effettuato con la tecnica analogica del taglio e rotazione (ogni linea dell'immagine viene tagliata in due parti che vengono ruotate e scambiate; la divisione avviene in un punto casuale diverso per ciascuna linea) mentre la generazione, codifica e gestione delle relative chiavi con tecniche digitali.
Nel 1994, il tedesco Markus Kuhn, un giovane informatico esperto di sistemi per l'accesso condizionato, riuscì a mettere in chiaro l'intero bouquet in vari modi:

- operando sull'algoritmo di scrambling senza l'ausilio delle chiavi (in questo caso l'immagine veniva visualizzata solo in bianco e nero), con una smart card "clonata" che emulava perfettamente quella originale e, infine, sostituendo la smart card con un PC dotato di apposito software e collegato al decoder [Videoc]. Kuhn diffuse i risultati della sua ricerca attraverso le BBS ed Internet ed il fenomeno della visione abusiva cominciò a prendere piede in tutta l'Europa occidentale (si consideri che l'abbonamento poteva essere sottoscritto solo da residenti in Gran Bretagna in quanto i diritti televisivi acquisiti da Sky erano limitati a quell'area geografica). Sky sostituì la card serie 08, ormai violata, con la 09 ma senza alcun successo.

Le conoscenze tecniche diffuse da Khun stimolarono la creazione di diversi gruppi di studio delle codifiche delle tv a pagamento via satellite che operavano in stretto contatto scambiandosi i risultati delle loro ricerche.
La sinergia portò alla forzatura del sistema D2-MAC/Eurocrypt, utilizzato dall'operatore scandinavo Viasat e dal francese CanalPlus, nonostante cifrasse le chiavi col DES.
Analoga sorte toccava alla codifica Nagravision utilizzata dalla tedesca Premiere e da alcuni canali spagnoli.
Nel 1995 Sky introdusse la serie 10 apportando notevoli modifiche alla generazione, codifica e gestione delle chiavi e riuscì a mettere fuori gioco tutti i critto analisti; anche la successiva e ultima serie, la 11, resistette ai vari tentativi di forzatura.
Nel 1996 cominciarono le trasmissioni digitali via satellite con il conseguente progressivo abbandono della tecnica analogica. La prima società europea ad offrire un bouquet digitale a pagamento via satellite fu la francese Canal Satellite Numérique (CSN) del gruppo CanalPlus nel 1996.
Le trasmissioni venivano codificate col sistema Mediaguard realizzato dalla società SECA, appartenente allo stesso gruppo, riprendendo alcuni concetti del D2-MAC/Eurocrypt.
Seguirono, subito dopo, l'italiana D+ e la tedesca DF1 che codificavano le trasmissioni col sistema Irdeto.
Successivamente vennero introdotte la codifica Viaccess dal gruppo francese ABSat, la Conax dal gruppo scandinavo Canal Digital, la Nds dal gruppo britannico Sky ed, infine, nel settembre del 1997, la Nagravision dal gruppo spagnolo Via Digital.
Nel 1998, dopo soli due anni dall'avvento della tv digitale a pagamento, la pirateria era già in grado di forzare tutte le codifiche, come peraltro ampiamente previsto.
La prima a cedere è stata Irdeto, seguita nell'ordine da Seca, Viaccess e Nagravision.

Questi sistemi sono stati irrimediabilmente compromessi e, nel 2002, le società che li hanno realizzati hanno introdotto una seconda versione che ha richiesto il cambio di smart card.
In particolare, Nagravision2, chiamato Aladin, è basato su IDEA, uno dei più forti cifrari simmetrici esistenti. Nel 2003, Seca2 è stato parzialmente ma costantemente forzato mentre Irdeto2 e Viaccess2 lo sono stati solo sporadicamente e per brevi periodi.
La situazione attuale vede compromessi Seca2 per quanto riguarda i bouquet italiani e spagnoli e Conax per il bouquet scandinavo. Irdeto2, Viaccess2 e Nagravision2 non sembrano attualmente soggetti a forzature ma l'unico sistema ancora completamente integro è Nds, sebbene in America sia stato aperto (va considerato che l'Nds americano sembra essere meno forte rispetto a quello europeo).

6.4 Le tecniche per la visione abusiva

Come abbiamo già detto nei precedenti paragrafi, gli attacchi alle tv a pagamento sono spesso coronati da successo e, cosa ancora più grave, i risultati possono essere facilmente riprodotti dal punto di vista tecnico e resi immediatamente disponibili anche a persone senza alcuna preparazione ed esperienza specifica.
La tecnica più comune per accedere abusivamente alle tv a pagamento è quella di "clonare" la smart card.
In realtà, essa non viene riprodotta in tutte le sue caratteristiche, sia per le difficoltà tecniche sia per i costi delle apparecchiature necessarie ad effettuare il reverse engineering.
Viene invece realizzata una smart card, chiamata trick card, con architettura hardware (processore e memorie) diversa da quella originaria ma in grado di emularla in quasi tutte le sue funzioni.
Sulla trick card vengono caricati il sistema operativo per la sua gestione, il software di emulazione della codifica e le ServiceKey in chiaro.
Sono state sviluppate anche trick card capaci di autoaggiornare le chiavi, periodicamente modificate dalle televisioni, o in grado di resistere agli Electronic Counter Measure (ECM), comandi inviati dalle emittenti nel tentativo di metterle fuori uso e consistenti in un cambio di chiavi imprevisto o nella cancellazione della EEPROM.
A volte, gli ECM vengono resi inefficaci grazie a un blocker, un dispositivo che si interpone tra la card e il suo lettore.
Le operazioni di scrittura del software e delle chiavi sulle trick card vengono effettuate mediante dei semplici dispositivi elettronici chiamati "programmatori", collegabili alle porte di un PC e gestibili con software in ambiente grafico di semplice ed immediato utilizzo.
Trick card (senza alcun software ad eccezione del sistema operativo) e relativi programmatori vengono legalmente venduti a prezzi irrisori nei negozi di elettronica mentre software per la programmazione, file e chiavi sono facilmente ma illegalmente reperibili su Internet.
Un'altra tecnica ampiamente sperimentata ma non generalizzabile è costituita dalla modifica dei decoder.
Le modifiche dell'hardware, per quanto efficaci, non sono molto diffuse perché sono complesse e possono essere effettuate solo da esperti, mentre le modifiche del software sono molto semplici e possono essere effettuate anche da persone con scarse conoscenze.
In genere, viene sostituito il firmware originale del decoder in modo da trasformarlo da monocodifica a multicodifica o, come si dice in gergo, allcam.
Ad esempio, un decoder con codifica Irdeto integrata sarà in grado di gestire anche le codifiche Seca, Viaccess e Nagravision.

Il firmware può anche essere integrato con altri software, detti in genere “emulatori”, in grado di aumentare ulteriormente il numero di codifiche o di bouquet rimessi in chiaro.
Il caricamento del firmware o di altri software sul decoder viene effettuata con un PC dotato di un semplice programma in ambiente grafico fornito a corredo del decoder stesso.
Con analoghe modifiche hardware e software è possibile trasformare CAM, in genere Irdeto, in allcam chiamati freecam.
Le difficoltà tecniche di tali interventi sono state completamente superate dall’introduzione ufficiale sul mercato di CAM allcam in cui il firmware può essere modificato con un semplice programmatore collegato ad un PC e gestito da un software con interfaccia grafica.
Gli allcam stanno avendo un enorme successo commerciale (attualmente sono disponibili una decina di questo tipo di CAM) e i più evoluti possono memorizzare nella propria EEPROM sia un emulatore che le chiavi rendendo addirittura inutile l’uso della trick card.
Va rilevato che, in genere, questi CAM non vengono venduti con alcuna codifica a bordo in quanto il produttore non ne possiede i diritti e il firmware per trasformarli in allcam viene prodotto da terze parti indipendenti.
L’ultima frontiera relativa agli allcam è costituita da un programmatore universale in grado non solo di programmare vari tipi di CAM ma di trasformare un CAM di un tipo in un altro più potente in quanto dotato di un maggior numero di funzioni, anche inerenti la decodifica.
Naturalmente la disponibilità di ricevitori e CAM allcam, ha portato allo sviluppo di trick card multicodifica (x in 1).
Attualmente è molto diffusa la 6 in 1, una sola trick card è in grado decodificare ben sei codifiche diverse.
Stravolgendone completamente la filosofia, anche l’Open Source è divenuto uno strumento, peraltro elitario, della pirateria.
Sono in commercio decoder con sistema operativo Linux che, oltre a consentire modifica del firmware, allcam, emulatori e memorizzazione delle chiavi, permettono anche di modificare, aggiornare, estendere le funzioni del sistema operativo e di sviluppare software di decodifica in maniera relativamente semplice.
Questi programmi possono poi risiedere sull’hard disk del decoder, senza alcun problema di memoria, ed essere eseguiti quando servono.
Alcune di queste macchine sono anche dotate di scheda di rete e possono essere collegate ad Internet; sfruttando questa possibilità, è stato sviluppato un programma che permette l’aggiornamento automatico delle chiavi prelevate da appositi siti.
Naturalmente questi ricevitori vengono venduti con software assolutamente “innocuo” ma, anche in questo caso, è possibile reperire facilmente su Internet, firmware, add-on e software vari che li trasformano in potenti sistemi per la visione abusiva.
Un discorso del tutto analogo può essere fatto per le schede di ricezione della tv via satellite su PC. La differenza sostanziale, rispetto a un decoder, sta nella maggiore potenza di calcolo di un PC che permette di aumentare notevolmente la capacità di decrittazione.
Inoltre è possibile utilizzare una scheda che non preveda il descrambling in quanto questa funzione può essere eseguita dal PC.
Un'ultima tecnica, anche se di livello molto basso in quanto estranea alla crittoanalisi, è la riattivazione di smart card scadute o sostituite, o la maggiorazione dell’abbonamento su smart card attive (per esempio, da base a full).
In questo caso, vanno individuate le locazioni di memoria della EEPROM della smart card in cui si trovano le informazioni relative al numero di card e alla data di scadenza o al tipo di abbonamento e sostituite con un numero e una data validi o con un altro tipo di abbonamento.

La card va generalmente usata in combinazione con un blocker per evitare eventuali disattivazioni da parte dell'emittente.
Al contrario di tutte le altre sinora descritte, questa tecnica è piuttosto complessa e può essere messa in atto solo da specialisti.

6.5 La Tecnica del Card-Sharing

Il **card sharing** è la pratica con la quale si tende a condividere abbonamenti con più utenti in modo hardware o software.
Il principio di funzionamento è molto semplice: attraverso un decoder collegato ad una rete (Internet o Intranet) che fa da server e in cui è inclusa la smart card con l'abbonamento, è possibile fare in modo che altri decoder client, collegati al decoder server, riescano ad utilizzare la stessa smart card (e di conseguenza a "mettere in chiaro" gli stessi canali) pur essendo fisicamente distanti svariati metri se non migliaia di chilometri dalla smart card stessa.
I primi tentativi di far funzionare un sistema di card sharing erano via cavo su rete dedicata, ossia la card veniva inserita in appositi apparecchi collegati al decoder server, da questi apparecchi partivano fisicamente dei cavi che finivano in altri apparecchi analoghi (senza card all'interno) inseriti negli altri decoder. Successivamente è stato sperimentato il card sharing su rete basata su protocollo IP, come Internet. Questo è stato favorito:

- dalla comparsa sul mercato di decoder satellitari con porta Ethernet (come il Dreambox ed altri) oppure attraverso schede PCI DVB-S collegate ad un normale Personal Computer;
- dal basso quantitativo di dati in transito da un decoder all'altro necessari al suo funzionamento;
- dall'aumento proporzionale della banda delle connessioni a Internet casalinghe.

Per quanto riguarda la legalità, il card sharing limitato all'interno di una stessa abitazione non è illegale (sebbene talvolta può violare le condizioni contrattuali del provider), ad esempio per usare la stessa smart card su più decoder all'interno di uno stesso appartamento senza doverla togliere e rimettere ogni volta col rischio di danneggiarla. Il card sharing che coinvolge terzi è invece ovviamente un reato poiché di fatto evita che chi si collega col decoder "client" paghi il dovuto all'emittente.
Nota:
Esiste attualmente in rete una guida dettagliata su come applicare l'uso del Card-Sharing ed è stata prodotta dalla comunità di "Cuba Libre" a solo scopo di studio. Il titolo del documento per chi ne fosse interessato è: **Guida al CardSharing dalla "A" alla "Z" via LAN/WAN per card NDS3 (Cielo IT) e non solo… (by Je Souis Blonde)**
La cosa importante da ricordare che l'abuso di questi studi va contro le leggi vigenti ed ogni uso è a proprio rischio.

6.5.1 Come funziona

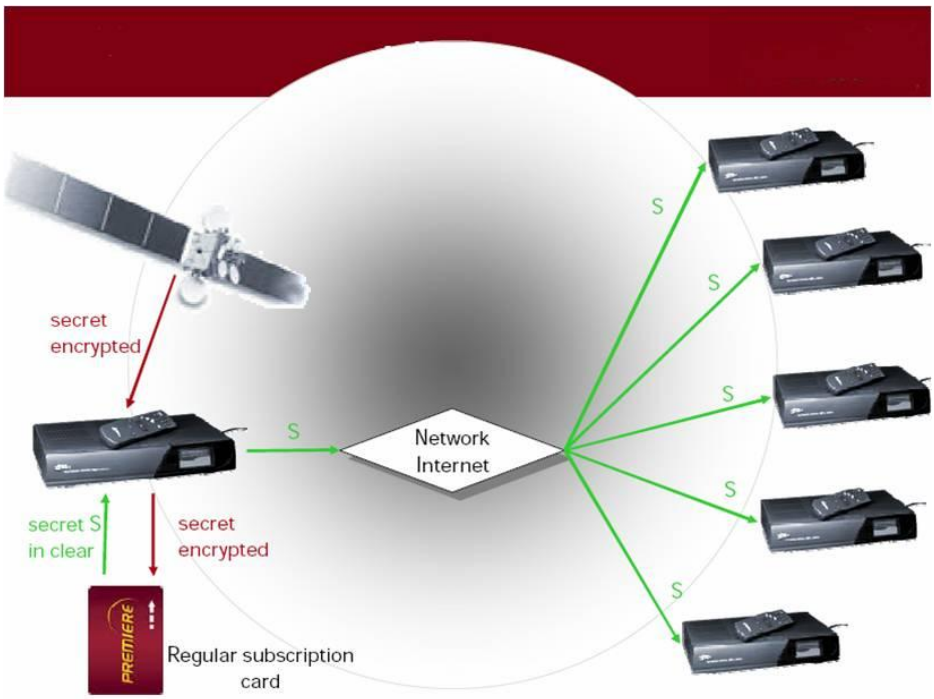


Figura 26: Schema generico del Card-Sharing

Per utilizzare questa tecnica è necessario l'utilizzo di un particolare decoder: il Dreambox

6.5.2 Il Dreambox

Il DreamBox è un decoder basato su tecnologia Linux per la ricezione digitale DVB di canali satellitari, via cavo e digitale terrestre come set-top box. È prodotto in Germania dall'azienda Dream Multimedia. Il firmware è aggiornabile dagli utenti per mezzo di immagini ufficiali o di terze parti. Tutte le unità supportano il sistema DreamCrypt CA, mentre con l'emulazione software di CAM è possibile accedere a molti sistemi CA.
Grazie alla natura del suo firmware open source, che ne permette piuttosto facilmente una completa personalizzazione a seconda delle esigenze del singolo utente, è considerato da molti esperti come il migliore (o almeno uno dei migliori) decoder oggi in commercio. Per lo stesso motivo, però, non è il più indicato per i neofiti della TV digitale, dato che potrebbero facilmente trovarsi spaesati in mezzo alle centinaia di firmware diversi disponibili in rete.

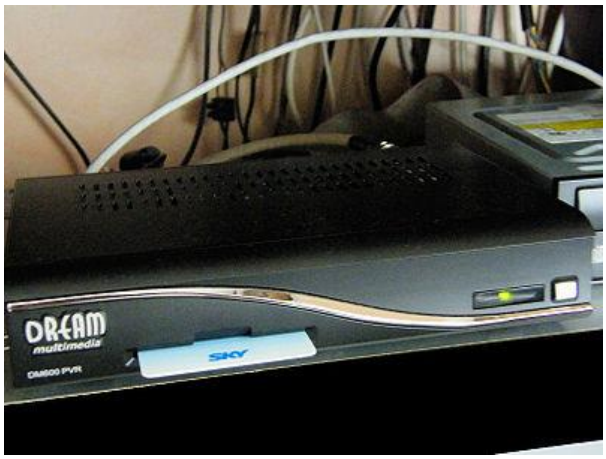


Figura 27: un Dreambox 600PVR

Il lavoro di sviluppatori non ufficiali e l'uso della scheda ethernet integrata permettono tra le altre cose anche il processo noto come card sharing.
La distribuzione standard di Linux installata nel Dreambox è in gran parte sotto licenza GPL e usa API Linux standard LIRC per permettere agli utenti di modificare le sue funzioni.
Il software di visualizzazione dei programmi televisivi e di gestione delle funzionalità VCR, è Enigma, anch'esso distribuito come software libero. La peculiarità di Enigma è la gestione dei plugins, che permette di aggiungere facilmente nuove funzioni a quelle di base: così il Dreambox diventa di volta in volta un browser internet, un aggregatore RSS, un juke box, un lettore di stream video in rete, un visualizzatore di immagini digitali etc. Con il Dreambox 7025 è stata introdotta la versione 2 di Enigma, che sfrutta le capacità grafiche avanzate del nuovo processore ATI.
Per tutti i modelli di Dreambox sono disponibili emulatori CA facilmente reperibili su Internet che emulano i sistemi CA sviluppati da VideoGuard, Mediaguard, Irdeto, Conax, Nagravision, Viaccess, Cryptoworks e altri produttori proprietari. Questi emulatori non sono legali, in quanto si tratta di lavori di reverse engineering che in quanto tali violano la licenza dei proprietari dei sistemi CA: il loro utilizzo tuttavia attualmente non è perseguito, se la finalità è l'utilizzo di abbonamenti regolarmente sottoscritti. Per molti utenti Dreambox, le softcam sono spesso utilizzate per il card sharing per permettere di condividere l'utilizzo di una smart card originale su una rete di decoder, permettendo la visione a più utenti con un solo abbonamento. Anche questa pratica è illegale e penalmente perseguita quando possibile.
Vista la grande disponibilità di firmware personalizzati ed alternativi a quelli ufficiali, molto diffuso tra gli utenti Dreambox è il software FlashWizard Pro che consente di effettuare un "multi-boot" ovvero la possibilità di selezionare in fase di avvio del decoder quale immagine firmware utilizzare. Grazie a FlashWizard Pro è possibile caricare sul decoder Firmware originale e non, effettuare e ripristinare backup dei medesimi; tali potenzalità consentono di testare immagini alternative o modifiche a quella impiegata senza comprometterne l'usabilità grazie alla rapidità ed alla semplicità d'utilizzo del programma. Le immagini in multi-boot sono caricate su Pendrive USB, CompactFlash, Hard Disk o rete grazie al supporto NFS. FlashWizard Pro è un progetto interamente sviluppato in Italia.
Per chi volesse approfondire è descritto come utilizzare questa tecnica nella rivista mensile “Win Magazine” sulle uscite n°133 e n°136 anno 2009/2010.

6.6 Le Smart-card utilizzate nella pirateria

Eccezion fatta per le carte originali modificate (dette Modified Original Smart Card MOSC), che necessitano di un' ottima conoscenza delle procedure di lettura e scrittura dei dati per poter funzionare.

E' bene precisare che una smart card non è un dischetto su cui si può leggere e scrivere i dati a piacimento. Per usare una smart card è necessario disporre di un lettore di smart card e di applicazioni appositamente progettate per quella card. Le smart card si distinguono in due principali famiglie: card a microprocessore e card a memoria. Le **card a memoria** non hanno capacità di elaborazione, e svolgono prevalentemente la funzione di contenere dei dati, che possono essere modificati di volta in volta tramite i programmatori. Inoltre le card a memoria si distinguono in due altre categorie: **card a memoria libera** e **card a memoria protetta**.

Le **card a memoria libera** possono essere sia scritte che lette senza bisogno di presentare un codice segreto alla card.

Le **card a memoria protetta** invece non possono essere scritte senza la presentazione del codice. Ciò le rende abbastanza sicure per la maggior parte delle applicazioni.

Le card a memoria, inoltre, si differenziano tra loro per la **capacità di memoria**, che varia comunque sempre nell'ordine dei Kbytes.

Le **card a microprocessore** sono card tecnologicamente più avanzate, infatti oltre a poter contenere dei dati, hanno altre funzioni. Tali funzioni variano molto da card a card, dunque si dovrà ricercare quella con le caratteristiche più adatte alle proprie esigenze.

Le smart card, possono essere considerate come delle vere e proprie evoluzioni delle schede magnetiche.

La banda magnetica è stata infatti sostituita con un chip che costituisce il cuore del sistema.

In questo singolo chip vengono memorizzate tutte le informazioni (sistema operativo e i dati immessi dall'utente) necessari per l'interscambio e l'aggiornamento dei dati tra le card e le apparecchiature dove trovano applicazione.

Le componenti fondamentali delle smart card sono:

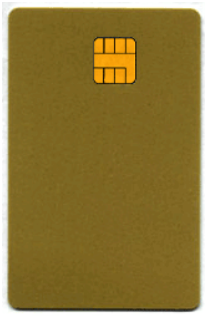
- **La CPU,** ad 8 bit che serve a svolgere tutte le operazioni aritmetico-logiche;
- **La memoria ROM,** contenente il sistema operativo, necessario per permettere alla card stessa di interfacciarsi con le varie apparecchiature;
- **La RAM,** per la memorizzazione temporanea dei dati: la cosidetta "area di lavoro";
- **Una memoria EEPROM** (Elettrically Erasable and Programmable Read Only Memory), contenente la struttura delle directory e i file immessi dall'utente. Questa è la memoria principale della card e può essere sia scritta che letta tramite un programmatore adatto.
- **Una porta di I/O,** necessaria per l'interscambio fisico delle informazioni secondo una serie di contatti ISO.

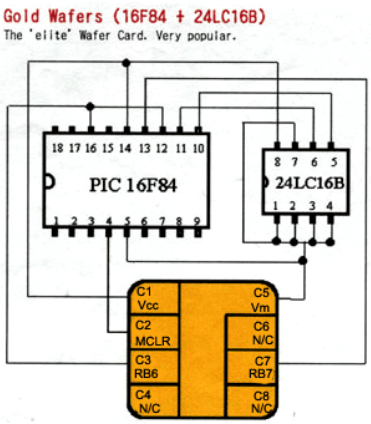
Esistono in commercio molti tipi di smart card pirata :

- **La wafer card**

E’ una card con processore da 8 bit, contenente al suo interno un pic 16F84

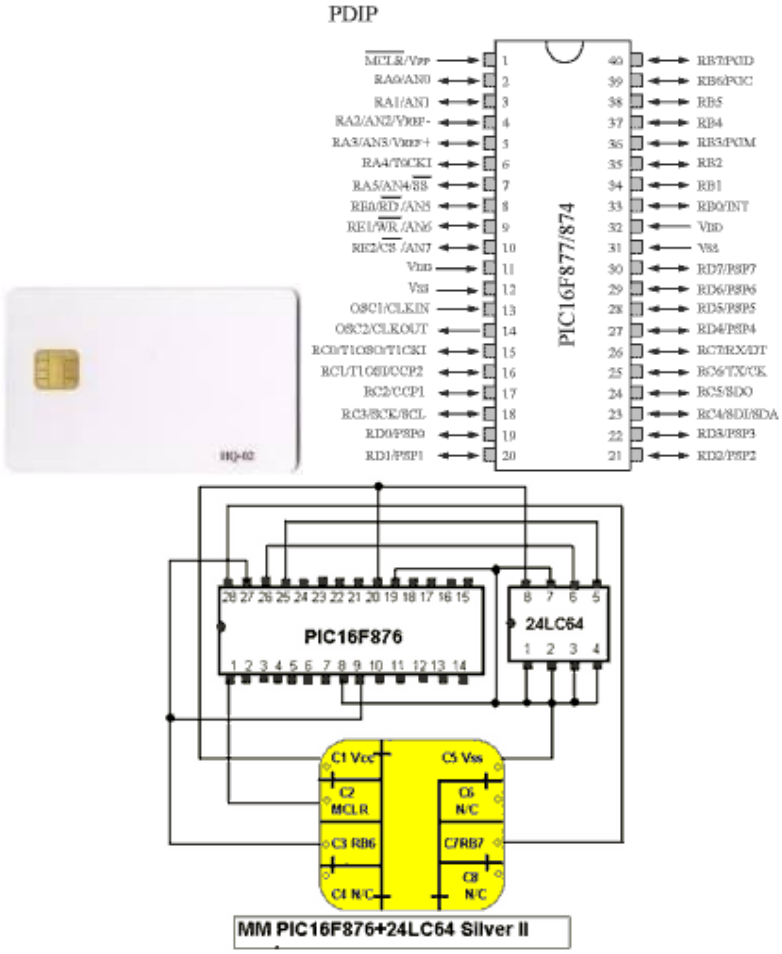
- **La gold card IC**





E’ una card con processore da 8 bit, contenente al suo interno un pic 16F84. L’apparato interno è identico ad una wafer card più evoluto per quanto riguarda la dimensione dei chip e cambia la sua estetica

- **Silver card**



E' una card molto potente infatti ha 8 Kbytes di memoria programma e 64Kbit di memoria per l'immagazzinamento dei dati. Ha un processore a 4 Mhz e monta un pic 16F876/7

- **Smart card blue IC**

E' una smart card basata su microcontrollore da 1 Kb. Ha una memoria EEPROM da 2 Kb e monta un pic 16F84.

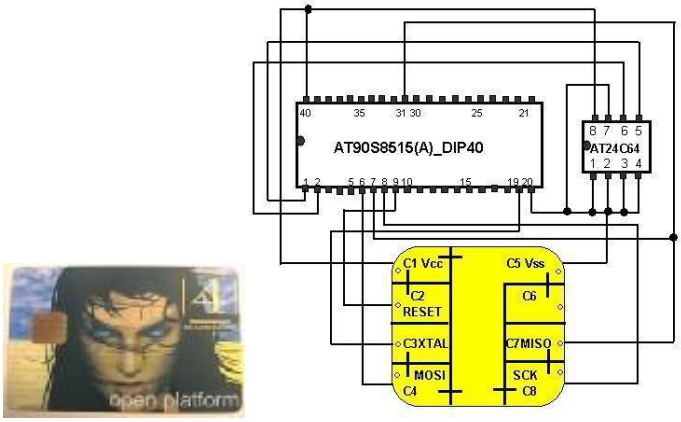
- **Green card**

Contiene al suo interno un pic 16F877, un pic completamente riprogrammabile e dotato di molta memoria, e una EEPROM 24LC128 programmabile con il millenium compatible Silver card.

- **Pink card**

E’ una wafer card equipaggiata con un microprocessore ATMEL AT90S2343 ed una EEPROM 24LC16.

Funcard 4



E’ costituita da un processore ATMEL AT90S8515 e da una EEPROM 24LC256

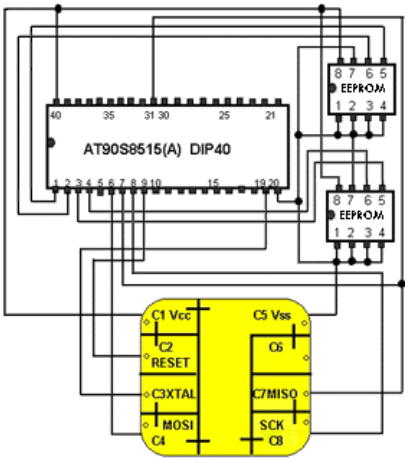
- **Funcard 5**

E’ costituita da un processore ATMEL AT90S8515 e da una EEPROM 24LC512

- **Funcard 6**

La funcard 6 monta un processore AT90SC8515 e una grandissima EEPROM 24LC1024. Inoltre questa funcard è compatibile con i file di tutte le smart card precedenti (fun 2/3/4/5).

- **Funcard 7**



Una card molto potente che monta un processore ATMEL 8515 e una EEPROM 24C2048 con 2048 byte di memoria (1024x2).

- **Titanium card**

La titanium card si programma esclusivamente con lo smartmouse. Ha una RAM da 1024 byte ed una EEPROM da 32K. Usa un sistema operativo per interfacciarsi con le varie periferiche (OS) che si può aggiornare via software. La versione più recente è OS 1.06. I file che vengono caricati in questa card devono essere compatibili con la versione di OS installata nella card stessa. Se vengono caricati dei dati non compatibili con il sistema operativo installato, la card, nella maggior parte dei casi perde l'ATR, cioè un codice necessario per il riconoscimento della card da parte dei programmatori. Se questo dovrebbe accadere la card sarebbe irrimediabilmente danneggiata e quasi impossibile da recuperare. E' programmabile ad una frequenza di clock di 3.57 Mhz.

- **Platinum card**

La platinum card e l'equivalente del doppio della titanium card. Infatti ha una memoria EEPROM da 64K, il doppio rispetto alla titanium (32K). Questo permette alla card di contenere molti più dati.

- **Knot card**

E' la card più potente al mondo ed ha il doppio della potenza di una comune titanium ed ha un sistema operativo (OS) proprietario, lo knotOS.

Tutte queste schede sono composte da un circuito stampato che collega una memoria eeprom ed un pic (microprocessore), per poi terminare, dall'altro lato della scheda, con i contatti, che replicano fedelmente quelli di una smart card originale.
Le schede si differenziano fra loro per l'hardware che montano e, di conseguenza, per la memoria a disposizione "on board".
Ognuna di queste schede ha un corrispettivo plastico, ovvero una scheda con chip integrati, in modo che essi non siano fisicamente estraibili dal supporto: si tratta di supporti meno versatili, ma certamente esteticamente più accurati.
Escludendo il logo della Pay-TV non presente su Gold Card, Silver Card e Purple Card (rispettivamente), queste sono indistinguibili ad occhio nudo da una scheda originale.
Che siano in formato plastico o meno, sui pic di tutte le carte vengono caricati i software che emulano le smart card originali, mentre sulle eeprom occorre caricare i codici operativi veri e propri.

6.6.1 Programmare le Smart-card

Per programmare un smart card abbiamo bisogno di un programmatore.
Alcuni dei programmatori più usati sono:

- **Smartmouse**, un programmatore molto diffuso che serve a programmare smart card più avanzate, come le titanium card o le platinum card. E' molto economico e si interfaccia col PC tramite un collegamento seriale.

Inoltre può essere "settato", tramite un Jumper, a due frequenze, 3.57 Mhz e 6 Mhz, ed ha un'alimentazione esterna, con un trasformatore o una batteria a 9V. Il software per l'utilizzo è il "titanium cardprogger"

- **Smallprog**, un programmatore di Silver card (o piccard2).

Programma le EEPROM 24LC16/32/64 wafercard e piccard2. La EEPROM va programmaa separatamente nel caso delle wafer card, staccandola dalla card e inserendola nell'apposito zoccolo.
Funziona con un'alimentazione da 9V tramite un trasformatore, e si collega al PC tramite cavo seriale. Il software per l'utilizzo è "IC prog".

- **Funprog gold,** un programmatore di Atmelcard (funcard).

Programma diversi tipi di funcard sia su zoccoletto che assemblate. Si interfaccia col PC tramite collegamento seriale, e si alimenta direttamente dalla porta del PC. I software per l'utilizzo di questo programmatore sono "funpron 244" e "fun magic".

- **ProgEeprom ISO**, un programmatore che permette di programmare la Eeprom direttamente sulla wafer card o comunque sulle wafer card dotate di ponticelli, senza estrarre la Eeprom dalla basetta.

Per tutti gli altri tipi di wafer card è necessario estrarre la eepron ed inserirla nello zoccoletto del programmatore. Le Eeprom che possono essere programmate da questo programmatore sono24LC16/32/64/128/256.

- **Millennium,** un programmatore molto potente, capace di programmare pic ed Eeprom sia su slot ISO che su zoccoletto. Questo programmatore ha un suo processore di

gestione per programmazioni più sicure. Si alimenta con un trasformatore esterno da 12V sia continua che alternata. E' inoltre in grado di programmare il pic 16F84A. Il software per utilizzare questo programmatore è "FX prog".

- **Card Maestro,** uno dei programmatori più potenti al mondo che supporta svariati tipi di smart card (wafer card, funcard, gold card, sim card). Questo programmatore ha un processore interno da 8 bit che controlla i dati trasmessi alla smart card, rendendo così sicura la programmazione. Inoltre con un solo tasto può passare istantaneamente da JDM a Phoenix/smartmouse (per la programmazione di funcard) a I2C (per programmare le sim card). Per funzionare ha bisogno di una tensione di 12V ad una corrente di almeno 100mA. Si interfaccia col PC tramite un collegamento seriale. I software per utilizzare questo tipo di programmatore sono: "Ic-prog" e "chipcat"

Infinity USB, un programmatore di nuova generazione che a differenza di tutti gli altri programmatori si interfaccia col PC tramite collegamento USB 2.0 garantendo così una programmazione rapida e sicura, grazie al processore interno da 24Mhz. Riconosce automaticamente il tipo di smart card inserita e si adatta alle sue caratteristiche e può programmare la maggior parte delle smart card esistenti in commercio. Inoltre ha la possibilità di essere aggiornato via software.

Studi effettuati sulle diverse smart card e possibile approfondire l'argomento a scopo di studio su (28).

6.7 I motivi del successo della pirateria

La storia della crittologia insegna che si susseguono periodi (anche interi secoli) in cui hanno la meglio i crittografi o coloro che vogliono mantenere un segreto e altri in cui prevalgono i crittoanalisti o coloro che vogliono svelare un segreto. (29)
La crittologia moderna, dall'introduzione del DES, avvenuta nel 1977, ad oggi, ha visto la netta prevalenza dei primi grazie alla scoperta di crittosistemi molto forti come lo stesso DES o l'RSA.
I sistemi per l'accesso condizionato, in particolare quello della tv a pagamento, costituiscono un'eccezione a causa di deficienze tecnologiche e strategie di gestione inadeguate.
Sia il **Common Scrambling Algorithm (CSA)** che i sistemi di codifica non sono stati resi pubblici dalle aziende che li hanno sviluppati e le sole conoscenze disponibili sono state fornite, in maniera non ufficiale, da coloro che li studiano.
Questa scelta è stata motivata col non voler fornire informazioni ai pirati e col mantenimento del segreto industriale, ma induce a ritenere che tali crittosistemi non siano poi così forti.
Questo alla luce del principio di Kerckhoffs, alla base di tutta la crittografia moderna, secondo cui la sicurezza di un sistema dipende dalla segretezza delle chiavi e non dell'algoritmo.
In ottemperanza a tale principio, tutti gli attuali crittosistemi sono pubblici e possono essere sottoposti a studi che ne evidenziano le eventuali debolezze permettendo di eliminarle.
Il non rendere pubblici i sistemi per l'accesso condizionato della tv a pagamento li ha posti in una situazione singolare in cui essi sono forzati senza che le società che li hanno realizzati sappiano ufficialmente con quali tecniche e, quindi, senza possibilità di apportare modifiche per rafforzarli.
La documentazione non ufficiale di cui disponiamo, fa ritenere che, alla luce delle attuali tecnologie elettroniche ed informatiche, la crittografia delle tv a pagamento sia effettivamente debole in quanto prevalentemente basata su chiavi a 64 bit.
Ricordiamo che il DES, che aveva una chiave di 64 bit di cui solo 56 effettivi ed 8 di controllo, nel 1999, è stato violato con un attacco di forza bruta impiegando meno di ventiquattro ore anche se con macchine dedicate e ingenti risorse di calcolo.
La potenza di calcolo degli attuali PC e la possibilità di distribuire un attacco di forza bruta su molte macchine operanti in parallelo consentono di rompere un simile cifrario in modo molto semplice, rapido e poco costoso.
Le ControlWord, che sappiamo avere una lunghezza di 64 bit dalla documentazione ufficiale del DVB, non sono soggette a questo tipo di attacco in quanto modificate con una frequenza altissima. Invece le ServiceKey vengono cambiate con una frequenza molto bassa e rimangono attive per un tempo che va da uno a trenta giorni.
Peraltro, i sistemi più evoluti prevedono ServiceKey di 128 bit ma le emittenti, per scelte che non sono note (forse per problemi tecnici), non sempre si avvalgono di tale possibilità.
Inoltre, sebbene in letteratura non vi sia riscontro, sembra ragionevole ritenere che le ServiceKey siano generate con algoritmi pseudo casuali e relativi semi, ambedue noti ai pirati.
Questo permetterebbe di definire le chiavi future con largo anticipo senza dover ricorrere a tecniche più complesse o dispendiose come un attacco di forza bruta.
La smart card costituisce un punto debole dell'intero sistema per l'accesso condizionato in quanto soggetta ad attacchi di varia natura che ne consentono la lettura e, addirittura, anche la scrittura.

L'evoluzione tecnologica ha sicuramente aumentato la sicurezza delle smart card ma non al punto da renderle immuni da intrusioni.
Una ricerca ha evidenziato che tutti i cifrari finalisti del concorso per la definizione dell'Advanced Encryption Standard, il nuovo cifrario simmetrico standard che ha sostituito il DES, mostrano una vulnerabilità più o meno accentuata ad attacchi effettuati con la recente e sofisticata tecnica dell'analisi di potenza.
La cosa assume aspetti ancora più significativi se si considera che uno dei requisiti richiesti ai candidati all'AES era proprio quello dell'implementazione sicura su smart card.
Le attuali tecnologie per la progettazione e realizzazione di smart card non sembrano poter garantire la sicurezza necessaria a mantenere un segreto su vasta scala.
Un'altra debolezza dei sistemi per l'accesso condizionato delle tv a pagamento è costituita dalla possibilità di rilevare costantemente il flusso cifrato in ingresso al decoder e il corrispondente decifrato in uscita dal decoder con un semplice analizzatore logico o **logger.**
Considerato che si possono rilevare un numero a piacere di coppie testo cifrato-testo in chiaro, sarebbe possibile effettuare un attacco di tipo matematico-statistico con testo (in chiaro o cifrato) scelto.
In realtà, questa tecnica viene utilizzata per analizzare il traffico tra la smart card ed il suo lettore e definire in maniera dettagliata tutte le interazioni esistenti tra i due dispositivi.
Manchevolezze nella gestione del sistema per l'accesso condizionato da parte delle emittenti possono favorire le azioni di cracking.
Il sistema non è costituto soltanto dai vari dispositivi e dai relativi software ma prevede anche operazioni, opportunamente pianificate, da attivare periodicamente o al verificarsi di determinati eventi.
Il cambio delle chiavi, la disattivazione di trick card mediante Electronic Counter Measure o la sostituzione delle smart card sono parte integrante del sistema e devono essere realizzate nei modi e nei tempi previsti in modo da prevenire o eliminare rapidamente la visione abusiva.
Non sempre le emittenti mettono in atto tali azioni in quanto non sono disposte a sopportarne i relativi costi, tempi e sforzi organizzativi.
Il cambio delle ServiceKey avviene con una frequenza molto bassa che può arrivare addirittura a trenta giorni e la sostituzione delle smart card viene in genere effettuata solo quando il sistema è stato completamente forzato da tempo.
Il cambio di smart card comporta la modifica della UserKey e di tutti gli algoritmi di decifratura delle chiavi e rende quindi inservibili la gran parte delle conoscenze eventualmente acquisite dai pirati sul sistema di codifica.
Per questo motivo le smart card dovrebbero essere cambiate anche quando lo stesso risulti ancora integro.
Come per tutti i sistemi elettronico - informatici, un'ulteriore possibilità di attacco è costituita dalla presenza di bug nella progettazione e realizzazione dell'hardware o del software del sistema per l'accesso condizionato.
In genere, questi errori sono sfruttati per forzare la lettura e la scrittura della smart card.
Va infine ricordato che la visione abusiva può essere facilitata dalla natura stessa del sistema di trasmissione o di quello per l'accesso condizionato.
La tv via satellite, che è la più soggetta agli attacchi, prevede una trasmissione di tipo simplex ossia unidirezionale dalla stazione emittente ad ogni singolo ricevitore.
La mancanza di un segnale di ritorno nel protocollo di comunicazione non rende possibile l'identificazione e la conseguente disattivazione delle trick card.

Inoltre un serio rafforzamento di una codifica potrebbe richiedere il cambio del decoder o della CAM con costi considerevoli non sempre sopportabili.

6.8 Proposte per combattere la pirateria.

La pirateria delle tv a pagamento costituisce un'attività illegale molto diffusa che comporta gravi perdite finanziarie ed occupazionali.
L'Unione Europea, gli Stati che vi appartengono e gli operatori del settore hanno effettuato alcuni interventi di natura legislativa e tecnica che non sembrano aver intaccato il fenomeno, visto il suo espandersi.
L'insuccesso di questa azione ed il previsto aumento del numero di tv a pagamento, a seguito del passaggio al digitale terrestre, fanno ritenere necessari ulteriori interventi.

- Il primo è di natura squisitamente culturale.

I soggetti danneggiati dalla pirateria dovrebbero promuovere iniziative che portino a considerare la visione abusiva "inaccettabile" sia dal punto di vista legale sia finanziario.
Attualmente, quest'opera di sensibilizzazione, che ha valenza anche per altri generi di pirateria (software, musica, film), viene svolta di rado e con poca convinzione; il problema emerge, quasi sempre in maniera sensazionalistica, solo quando viene sgominata un'organizzazione di pirati o introdotta, aggiornata o forzata una codifica, senza che questo comporti significative ricadute in termini educativi o di presa di coscienza.
Quella culturale è una strada molto lunga che richiede tempi considerevoli ma, al di là di ogni retorica, è l'unica a garantire risultati consolidati e duraturi.
Non si potrebbe spiegare altrimenti quanto accade in Scandinavia, dove il numero di abbonati alle tv a pagamento rimane molto alto pur in presenza di una pirateria in grado di offrire la visione abusiva di tutti i bouquet degli operatori locali senza alcuna interruzione temporale.

- Il secondo è di natura legislativa.

L'Unione Europea, sotto la spinta delle società di tv a pagamento, ha emanato nel 1998 la direttiva 98/84/EC sulla protezione legale dei servizi basati sull'accesso condizionato, in cui le attività e i sistemi che consentono la visione abusiva vengono dichiarati illegali.
In Italia, la direttiva è stata definitivamente recepita con la legge n. 2442 del 15 gennaio 2003 [Leg03] che ha integrato il decreto legislativo n. 373 del 15 novembre 2000.
Le leggi emanate a seguito della direttiva nei Paesi appartenenti all'UE hanno consentito di smantellare le piccole organizzazioni di pirati e di chiudere i siti Internet residenti su server, situati negli stessi Stati, che distribuivano software e chiavi.
Le grandi organizzazioni, invece, hanno continuato ad operare e a gestire siti in Paesi non appartenenti all'Unione Europea (in particolare dell'Europa dell'Est e dell'ex Unione Sovietica) dove la materia non è regolamentata.
Un'azione legislativa parziale, promossa solo da alcuni Paesi, non sembra in grado di combattere la pirateria.
Un'armonizzazione legislativa che consideri illegale la visione abusiva nel maggior numero di Paesi o, meglio ancora, in tutto il mondo, rimane la sola strategia per ridurre in maniera significativa il fenomeno.

- L'ultimo intervento riguarda l'aspetto tecnico.

Abbiamo ampiamente dimostrato che l'attuale sistema per l'accesso condizionato non è in grado di garantire sicurezza ma, al momento, non sono disponibili alternative più efficaci.
Le proposte di sistemi per l'accesso condizionato più o di tecniche per la scoperta di "traditori", ossia di utenti autorizzati che rendono pubbliche le chiavi per consentire la visione abusiva ad altri, [Tre03] non hanno ancora trovato attuazione.

Pertanto le uniche soluzioni proponibili riguardano il potenziamento e la corretta gestione dell'attuale sistema per l'accesso condizionato.
In primo luogo va adottata una crittografia forte a 128 bit invece degli attuali 64.
L'AES, che, come abbiamo visto, è a rischio di forzatura quando implementato su smart card, potrebbe però essere un buon candidato in quanto pubblicamente riconosciuto resistente ad attacchi di forza bruta e di tipo matematico/statistico.
In secondo luogo, le emittenti dovrebbero mettere in atto tutte le operazioni programmate per la corretta gestione del sistema per l'accesso condizionato, come il cambio molto frequente (più volte al giorno) delle ServiceKey e quello periodico (ogni sei-dodici mesi) delle smart card.

6.8.1 I successi contro la pirateria

Di seguito sono riportati alcuni articoli.
Tratto dalla cronaca del "Corriere della Sera" 1 ottobre 2004. Primo caso in Europa: è successo a Castelfiorentino (Fi). Pirata «satellitare» clona Sky.
Programmi cifrati, sportivi e porno a cento euro. Eutelsat aveva escluso ogni falla ma si è dovuta ricredere

Eurobird TM, uno dei satelliti gestiti dalla Eutelsat (Ap)

BRESCIA - Primo e unico caso in Europa di pirateria satellitare. Una emittente televisiva con tecnologie molto sofisticate è stata scoperta appropriarsi di frequenze per irradiare **programmi cifrati, sportivi o di pornografia.** È stata individuata anche la rete di clienti delle smart-card, vendute a cento euro ciascuna, al termine di una indagine tra l'Italia e la Francia durata circa un anno. Anziche duplicare le smart-card, il gestore della truffa era riuscito a clonare il segnale di Sky

È il primo caso di furto di trasmissioni televisive realizzato in Europa attraverso tecnologie raffinate, quello scoperto dalla Guardia di Finanza di Brescia - Brigata di Salò - a seguito dell'indagine coordinata dal sostituto procuratore Paolo Savio della Procura di Brescia. Le Fiamme gialle hanno scoperto una vera stazione clandestina di segnali satellitari situata nel centro storico di Castelfiorentino, in provincia di Firenze. Il titolare M.S., di 50 anni - un «genio» in questo settore, come è stato definito - rubava, decodificava e poi demoltiplicava i segnali del satellite hotbird 1, gestito dalla società Eutelsat di Parigi.

Dalla sua emittente parallela e nominata Dataservice e Dataservice 2, proponeva un palinsesto con partite del campionato di calcio di serie A e B e anche film di recente produzione recando un danno economico a Sky Tv, Rai Sat e Rai Sport. Informata del furto, in un primo momento, la società francese Eutelsat aveva escluso qualsiasi ipotesi di falla nel sistema. Successivamente, gli stessi ideatori di hotbird hanno dovuto ricredersi davanti all'evidenza. Il danno creato alla società è stato quantificato in circa 2 milioni di euro.

Le trasmissioni che il fiorentino «rubava» al satellite erano quelle destinate alla Turchia. Con un elicottero dotato di personale tecnico altamente specializzato, sorvolando la zona di Castelfiorentino è stato individuato il punto di partenza delle onde radiotelevisive oggetto di

indagine. L'emittente pirata era posta nel locale mansarda di un immobile in cui hanno sede a sezione locale dei Ds e anche l'Arcicaccia. La prima è addirittura zona di passaggio obbligato per accedere al piano superiore dove aveva sede l'emittente pirata. Individuati i locali tutto il materiale tecnico presente è stato sottoposto a sequestro preventivo. Le indagini della guardia di Finanza di Brescia - partite dalla Procura di Brescia un anno fa per una segnalazione anonima relativa ad una Smart Card per decodificare le trasmissioni audiovisive ad accesso condizionato - stanno ora proseguendo per individuare la rete di clienti.

I risultati dell'operazione denominata «Cielito lindo» sono stati illustrati dal procuratore capo di Brescia Giancarlo Tarquini, dal sostituto procuratore Paolo Savio, dal comandante provinciale delle Fiamme Gialle Attilio Iodice insieme ai vertici della Brigata di Salò e al presidente dell'Associazione per la protezione delle opere e dei servizi cifrati AEPOC, Jean Grenier, che peraltro è lo stesso ideatore del sistema Hotbird. Il genio informatico creatore del sistema pirata è stato denunciato a piede libero per violazione della legge sul diritto d'autore e per ricettazione.

«Nessuno può sottovalutare la piaga della pirateria e il caso di questa emittente fiorentina scoperto dalla Guardia di Finanza di Brescia dà la misura di quanto sia grave e preoccupante il fenomeno» commenta Sky in una nota. Si tratta, secondo Sky, di «una piaga che viene spesso sottovaluta nel nostro paese e verso cui non è possibile abbassare il livello di guardia. Quella individuata oggi è una nuova modalità che si aggiunge alla lunga lista di marchingegni pirata diffusi nel nostro paese. Una ulteriore conferma di come la sicurezza delle trasmissioni cifrate sia una condizione fondamentale per lo sviluppo dell' industria culturale del nostro paese. Ancor più in un momento in cui il mercato della pay tv si sta aprendo a nuovi operatori e il problema della pirateria diventa cruciale per garantire un' evoluzione competitiva di questo mercato e la tutela degli investimenti di tutti i diversi fornitori di contenuti a pagamento».

27-05-2005 (tratto dal sito : www.poliziadistato.it)

Milano:operazione “Sat war” della Polizia Postale di Milano contro le violazioni del diritto d'autore.

La Polizia Postale e delle Comunicazioni di Milano, nell'ambito di un'indagine finalizzata al contrasto delle violazioni in materia di diritto d'autore e sulla base di una denuncia della società SKY Italia srl, ha eseguito ventidue perquisizioni locali che hanno consentito di sequestrare 139.000 euro, 1300 smart card, 1200 decoder, numerosi dati relativi agli utenti che hanno acquistato decoder e smart card e una pagina web usata per pubblicizzare un'illecita attività di distribuzione di decoder e smart card di SKY. L'indagine ha permesso di scoprire una gruppo criminale che ha procacciato abbonati e distribuito decoder e smart card per il sistema cifrato di una Pay Tv, per trasmettere in particolare eventi sportivi del campionato di serie A e B e Champions League, eventi per i quali Sky Italia srl detiene i diritti in esclusiva per il territorio italiano. Questa attività fraudolenta era pubblicizzata e incrementata, attraverso un sito internet registrato con dati fittizi presso AlterVista.org, da uno degli indagati nel quale venivano specificate le modalità di pagamento degli abbonamenti attraverso bonifico bancario, attraverso bollettino su conto corrente postale oppure ricarica tramite carta di credito ricaricabile.

Figura 28: operazioni anti-pirateria

CAPITOLO 7: Il digitale terrestre in Italia

L'attivazione della televisione digitale terrestre in Italia deriva dal processo di attuazione delle raccomandazioni comunitarie in merito al passaggio dalla tradizionale televisione analogica terrestre alla televisione digitale terrestre.
Per l'Italia il termine ultimo previsto per la conversione da televisione analogica terrestre a televisione digitale terrestre (il cosiddetto switch-off), e quindi il termine ultimo per aggiornare gli impianti, era il 31 dicembre 2006, ma il Consiglio dei Ministri nel dicembre 2005 ha rinviato la cessazione del servizio analogico alla fine del 2008. Il 15 luglio 2006, durante la seconda Conferenza Nazionale sul Digitale Terrestre svoltasi a Napoli, Rai, Mediaset e Telecom Italia Media hanno presentato "Tivù", la piattaforma unica per il digitale terrestre, un progetto con cui i tre maggiori concorrenti del settore si impegnavano a fornire nuovi contenuti gratuiti su piattaforma digitale. L'allora ministro delle comunicazioni Gentiloni (Governo Prodi II) aveva anche indicato come data realistica per la chiusura della TV analogica il 2012, data ultima imposta dall'Unione Europea per il passaggio definitivo al digitale.

7.1 Panorama legislativo attuale

La Commissione Europea richiede che la conversione da televisione analogica a televisione digitale sia completata entro il 2012 in tutti i Paesi membri dell'Unione Europea.
L'introduzione della tecnologia digitale per le trasmissioni televisive da terra partì in via sperimentale, sull'esperienza degli altri Paesi europei, a Torino durante il primo governo Prodi. Successivamente con la legge 66/2001 si stabilì:

- termine dello switch-off il 31 dicembre 2006;
- il 40% della capacità trasmissiva di ciascun mux privato dovrebbe essere affittato a terzi (al momento Telecom e Mediaset rispettano questo parametro, la RAI no, non essendo tenuta a farlo).

Nel 2003 venne emanata la legge Gasparri, legge di riordino del sistema televisivo italiano, in cui sono stati imposti due tipi di limiti alle emittenti sul digitale terrestre:

- Si è confermato il tetto del 40% da affittare a terzi;
- Si è introdotto il Sistema Integrato delle Comunicazioni (Sic), secondo cui i ricavi di ciascuna emittente possono arrivare al massimo al 20% dei ricavi totali facenti parte del Sic, calcolato dall'antitrust.

La Gasparri se da una parte rispetta il principio del 20% introdotto dalla Corte Costituzionale, dall'altra parte, con l'introduzione del Sic, ha elevato il totale su cui quel 20% viene calcolato, consentendo per legge ulteriori possibilità di crescita per gli attori che attualmente ricoprono una posizione dominante sul mercato televisivo analogico italiano.
Il Sic è stato quantificato a giugno 2006 in 22 miliardi di €, con un massimo di 4,4 miliardi per azienda.
È bene precisare però che i servizi PPV non rientrano nel limite del 40% se le trasmissioni hanno una durata massima di 24 ore settimanali. Tant'è che Mediaset, con 5 canali PPV, e Telecom, con 7 canali PPV, possono trasmettere eventi pay, catalogati come "servizi della società dell'informazione" dall'antitrust italiano, non rispettando il limite del 40%.

7.2 Transizione da analogico a digitale

In Italia il mercato televisivo si può prestare a molte interpretazioni. Sui ricavi c'è un oligopolio in cui tre aziende, Rai-Mediaset-Sky si spartiscono poco più di 2 miliardi di euro per ciascuno. In particolare la Rai ha la sua fonte di sostentamento per il 50% nel canone e per il restante 50% nella pubblicità. Mediaset e Sky hanno ricavi derivanti sia da pubblicità (soprattutto la prima) sia da abbonamenti e PPV. Si deve altresì sottolineare che

nell'analogico terrestre Rai e Mediaset si spartiscono oltre il 90% dei ricavi pubblicitari totali, di cui il 40% va alla tv pubblica, il restante a Mediaset, ed hanno insieme l'85% degli ascolti.
Alla fine del 2005 la Commissione Europea ha avviato uno studio propedeutico all'emanazione di una procedura d'infrazione nei confronti dell'Italia con l'accusa di aiuti di Stato. Tale accusa è stata mossa per il finanziamento statale di 220 milioni di euro per l'acquisto dei ricevitori per il digitale terrestre. Sono anche sorte delle polemiche perché un'azienda amministrata da Paolo Berlusconi la Solari.com srl, fratello dell'allora premier, è stato uno dei distributori di decoder (con una quota minima del 2% del mercato). Nel 2006, la stessa commissione ha aperto un'indagine a proposito del problema delle frequenze tv (nel mirino l'acquisizione da parte di Mediaset delle frequenze di Europa Tv, proprietaria del canale sportivo analogico Sportitalia), ma non è emerso niente di illegale. L'Antitrust ha però esteso i tetti esistenti del DVB-T al DVB-H, in particolare obbligando le emittenti che trasmettono su cellulare a lasciare il 40% dei propri canali a terzi e obbligando a usare le frequenze solo per la TV sui cellulari.
Il 19 luglio 2006 la Commissione Europea aveva inviato al governo Prodi una lettera di avviso formale in cui si chiedono chiarimenti in merito alla riforma del sistema televisivo, su cui si sospettavano incompatibilità con le norme europee in materia di concorrenza, nelle parti in cui si danno restrizioni alla fornitura di servizi nel settore delle trasmissioni televisive. Infatti la legge Gasparri, se da una parte dovrebbe favorire l'aumento del pluralismo permettendo alle tv locali di unirsi in network interregionali, dall'altra non interviene sulla (presunta) posizione dominante di Rai e Mediaset. A tal proposito, il 12 ottobre 2006 è stato presentato un nuovo disegno di legge che mira a ridimensionare Rai e Mediaset spostando una rete analogica a testa (si parla di Rete quattro e Raidue, scartata Raitre che garantisce l'informazione regionale) solo sul digitale terrestre, in cui l'azienda milanese sta investendo milioni grazie anche alla pay-per-view; questo, secondo il ministro Gentiloni (centrosinistra) dovrebbe aumentare la concorrenza nel mercato televisivo italiano.
A gennaio 2007 l'Italia ha ricevuto una sanzione per gli incentivi all'acquisto sui decoder per il digitale terrestre, ritenuti non in regola con la neutralità tecnologica tra sistemi di trasmissione. Nello stesso anno il Governo Prodi ha varato nell'ultima finanziaria per il 2007 una nuova campagna di incentivi ma solo per l'acquisto di tv flat con tuner digitale terrestre integrato (apparecchi non molto diffusi). Tali incentivi sono delle detrazioni di imposta pari al 20% del prezzo d'acquisto, fino ad un massimo di 200 euro. Essi sono stati riproposti anche nella Finanziaria 2008.
Il 18 luglio 2007, Bruxelles chiede all'Italia di correggere alcune discriminazioni della Gasparri sul passaggio dall'analogico al digitale entro 2 mesi, altrimenti scatta un altro deferimento alla Corte di Giustizia Europea e una multa giornaliera di 300-400 mila euro fino a quando non saranno sanate le anomalie. Il governo, vista la lentezza dell'iter, ha chiesto una proroga, ma la UE l'ha respinta.

GLOSSARIO

Alta Definizione

L'immagine televisiva tradizionale è formata da 625 linee di definizione. Nell'Alta Definizione, il numero di linee viene raddoppiato, offrendo una qualità d'immagine e un livello di dettaglio superiori, vicini a quelli offerti dalla pellicola cinematografica. Analogico Tecnicamente, è il sistema in cui il segnale viene elaborato in forma continua, l'opposto di un segnale digitale. Si tratta del sistema utilizzato tradizionalmente per diffondere i programmi tv via terrestre. Via satellite, esistono decine e decine di emittenti che trasmettono in modalità analogica. Questo standard verrà in futuro soppiantato da quello digitale, economicamente più conveniente per le emittenti e più versatile per gli utenti.

ATR (Answer To Reset)

Messaggio inviato da una Smart Card nella comunicazione con il CAM. L'ATR indica il tipo di card, protocollo di comunicazione e altre informazioni di base che vengono usate per determinate i parametri per le comunicazioni tra la card ed il dispositivo di interfaccia.

BBS

Acronimo di Bullettin Board Service, ovvero forum di discussione. Programma residente sul server, che permette di ospitare messaggi, informazioni e dati dei visitatori di un sito Web.

BROADCAST

Un broadcast è una particolare trasmissione dove i destinatari sono tutti i nodi raggiungibili.

CAM

Conditional Access Module (modulo d'accesso condizionato). Si tratta, nei sistemi digitali, della circuitazione di decodifica necessaria a ricevere i canali cifrati. Può essere un modulo estraibile, come nel caso dei CAM Irdeto o di quelli conformi allo standard Common Interface, o di un chipset integrato direttamente sulla piastra madre del ricevitore. Canone Importo versato da ciascun utente al Service Provider per fruire dei servizi offerti.

Cas - Sistemi per l'accesso condizionato

Il sistema che controlla l'accesso a servizi, programmi ed eventi da parte dell'abbonato.

Cass - Conditional Access SubSystem

Parte dell'apparato ricevente preposta alle operazioni di decifratura per la messa in chiaro dei servizi.

Control word

La chiave principale utilizzata nel processo di codifica/decodifica.
Decoder Apparecchio necessario per decodificare programmi televisivi cifrati.

Demultiplexer

Dispositivo in grado di estrarre, da una sequenza continua di dati, blocchi

indipendenti da indirizzare ognuno verso la propria destinazione.

Descrambling
Processo inverso allo scrambling, atto a ricostruire il segnale originale.

Digitale
Sistema di trasmissione numerico basato sul campionamento di immagini e suoni. In Europa viene utilizzato lo standard DVB (Digital Video Broadcasting), che prevede la compressione del segnale attraverso il sisema MPEG2.

Down Link
Percorso del segnale dal transponder del satellite a Terra.

DVB
Acronimo di Digital Video Broadcasting: è lo standard di trasmissione digitale adottato in Europa, ed è basato sul sistema di compressione MPEG-2.

Electronic Counter Measure
Comandi inviati dalle emittenti nel tentativo di mettere fuori uso le card pirata, e consistenti in un cambio di chiavi imprevisto o nella cancellazione della EEPROM.

Entitlement Control Message
Messaggio che porta con sè le informazioni per decodificare un canale cifrato (Pay TV o Pay-Per-View).

Eeprom
Acronimo di Electrically Erasable Programmable Read-Only Memory,è la memoria a sola lettura cancellabile elettricamente, presente sulle card.

Entitlement Management Message
Messaggio di gestione che il provider invia alle card per impostarne e aggiornarne alcuni valori.

ETSI (European Telecommunications Standards Institute)
Organizzazione che stabilisce gli standard per le telecomunicazioni.

Free To Air
I canali digitali irradiati in modalità "free to air" sono quelli privi di codifiche, diffusi "in chiaro". Possono essere ricevuti con qualsiasi set-top box digitale, anche privo di modulo d’accesso condizionato.

Geostazionario
Un satellite geostazionario ha un tempo di rivoluzione attorno alla terra pari al tempo di rotazione della terra stessa.

GPS
Abbreviazione di Global Positioning System, si tratta di un sistema mediante il quale un idoneo apparato é in grado di rilevare le proprie coordinate geografiche, in qualunque punto della terra esso si trovi .
Installazione
Il montaggio e il puntamento di un sistema di ricezione via satellite.

Interlacciato

è un sistema di scansione di immagini video che prevede la divisione delle linee di scansione in due parti, dette campi o semiquadri, suddivisi in linee pari e dispari. Questa tecnica permette una qualità di trasmissione migliore senza bisogno di aumentare la larghezza di banda. Un televisore in standard PAL, per esempio, visualizza 50 semiquadri al secondo (25 pari e 25 dispari). Un quadro completo, quindi, viene tracciato 25 volte al secondo. Nonostante le dichiarazioni di molti produttori di abbandonare la scansione interlacciata, questa tecnica rimane di largo utilizzo ed è prevista nei nuovi standard televisivi, come DV, DVB (comprese le estensioni per l'alta definizione) e ATSC.

IRD (Integrated Receiver Decoder)

Ricevitore con decodificatore integrato. Larghezza di banda Gamma di frequenze occupate da un segnale.

LNB

Acronimo di Low Noise Block converter, ovvero convertitore a basso rumore. E' l'elemento sul quale vengono convogliati i segnali riflessi dalla parabola, la cui funzione è quella di amplificarli e convertirli ad una gamma di frequenze inferiori, per poterli poi trasferire al ricevitore attraverso un cavo coassiale.

Microcontroller

Piccolo dispositivo dotato di capacità di calcolo (CPU).

Modem

Acronimo di MOdulatore - DEModulatore: è l'apparecchio che converte un'informazione digitale in un segnale analogico, per consentire la sua trasmissione attraverso la comune rete telefonica. Nella tv digitale viene utilizzato per collegare il ricevitore al Centro Servizi della pay tv alla quale ci si è abbonati, per consentire l'utilizzo di sistemi di PayPerView.

M.O.S.C.

Modified Original Smart Card, é riferito alla modifica illegale di una smart card con regolare abbonamento.

MPEG2

Sistema digitale di compressione dell'informazione, basato sull'eliminazione degli elementi di ridondanza e su alcuni potenti algoritmi in grado di ridurre sensibilmente la dimensione del dato finale. Sviluppato da un gruppo di ricerca internazionale (il Motion Picture Expert Group, da cui l'acronimo MPEG), è il sistema utilizzato per la compressione dei dati digitali che compongono i segnali DVB.

MPK

Master private key, è la chiave identificativa di ciascun utente e non varia nel tempo.

Multicrypt

Sistema che consente di inserire, in un ricevitore digitale, diversi moduli d'accesso condizionato grazie ad un'interfaccia di tipo Common Interface.

Multiplexer
Dispositivo che consente l'uso di un singolo canale di dati per trasmettere due o più canali di dati.

Parabola
E' il cuore di un sistema di ricezione per la tv via satellite. Tecnicamente, si tratta di una superficie di forma parabolica costruita con materiali in grado di riflettere i segnali ricevuti verso il convertitore. Il suo guadagno varia in funzione del diametro: maggiori saranno le dimensioni, migliore sarà la qualità del segnale ricevuto.

Pay Per Channel
Singolo canale che richiede l'abbonamento per accedere alla sua visione.

Pay Per View
Un servizio offerto dalla pay tv, attraverso il quale è possibile "acquistare" un singolo evento.

Pay Tv
Televisione a pagamento: tutti i programmi di una pay tv sono codificati, e per poterli "decodificare" è necessario pagare un canone di abbonamento.

Pic (microprocessore)
Microprocessore, presente nelle smart card, che consente di elaborare le informazioni contenute nella memoria eeprom.

Reset
Inviato dalla PayTV, provoca il resettaggio della smartcard presente nel decoder, reimpostandola ai valori predefinit (DEFAULT).

Ricevitore
Si tratta dell'apparecchio utilizzato per sintonizzare e memorizzare le diverse emittenti ricevute dalla parabola. Può essere di tipo analogico o digitale.

Scart
Tipo di presa con 21 pin per il collegamento dei dispositivi audio/video come videoregistratori, ricevitori, lettori DVD, decoder e televisori. Attraverso i connettori Scart possono transitare sia segnali in videocomposito che in RGB o in Y/C (Super VHS).

Scrambling
Processo atto a codificare, per mezzo di variazioni continue, la forma del segnale trasmesso, al fine di renderlo inintellegibile.

Service Key (Authorization Key)
Chiave operativa di livello intermedio utilizzata nelle gerarchie di chiavi a più livelli.

Service Provider (SP)
Entità che è in grado di offrire servizi di vario genere, nel nostro caso la pay-tv.

Subscriber Management System

Combinazione di hardware e software che memorizza informazioni sugli utenti di un Sistema,fatture,pagamenti,ecc. .

Smart card

E’ la "tessera", da inserire nei decoder, digitali ed analogici, per abilitarli alla decodifica di un segnale codificato. All’interno della smart card c’è un piccolo chip, sul quale sono memorizzati i dati relativi all’abbonamento sottoscritto, necessari per decodificare il segnale.

Transponder

Il dispositivo, posto su un satellite, in grado di ricevere i segnali dalle stazioni terrestri e di ritrasmetterli verso Terra.

Uplink

Percorso del segnale dalla Terra al satellite.

Video On Demand

Sistema che consente all’utente di scegliere, attraverso l’utilizzo del telecomando, l'evento che desidera acquistare in Pay Per View.

Indice delle figure

Bibliografia

1. **ETSI.** *Digital Video Broadcasting (DVB) - framing structure, channel coding and modulation for cable systems.* s.l. : ETSI, 1994.

2. *La televisione digitale terrestre in Italia.* **M.Cominetti.** 1, 2002, Vol. Elettronica e Telecomunicazioni.

3. **Wikipedia.** wikipedia. [Online] http://it.wikipedia.org/wiki/Televisione_digitale_terrestre.

4. **Bagnardi, Nicola.** [Online] http://bagnardi.com/DVB_Frame.html.

5. **Benoit, Hervé.** *Manuale della televisione digitale - MPEG-1 - MPEG-2 - principi del sistema DVB .* s.l. : Hoepli. 978-88-203-3227-2.

6. —. Digital Television : Satellite, Cable, Terrestrial, IPTV, Mobile TV in the DVB Framework Third Edition. [Online] 2008. http://books.google.it/books?id=xwMZw4UewuUC&printsec=frontcover&dq=Digital+Television+:+Satellite,+Cable,+Terrestrial,+IPTV,+Mobile+TV+in+the+DVB+Framework&source=bl&ots=ah_idrA8vF&sig=fM0oGDwARBvsMqv1eIER_tGuhb4&hl=it&ei=IIwfTJTSKYH8_AaUk4WfDQ&sa=X&oi=b.

7. **ETSI.** *Digital broadcasting systems for television, sound and data services; framing structure, channel coding and modulation for digital terrestrial television.* s.l. : http://www.dvb.org/technology/dvbt2/a122.tm3980r5.DVB-T2.pdf, 1997.

8. **Wikipedia.** http://it.wikipedia.org/. *wikipedia.* [Online] http://it.wikipedia.org/wiki/Forward_Error_Correction.

9. **Experience, Sat.** Sat Experience. *Sat Experience.* [Online] http://library.thinkquest.org/C0122280/italian/standard1.htm.

10. *Valutazione in laboratorio delle prestazioni del sistema DVB-T.* **A.Bertella, B.Sacco, M.Tabone.** 1, s.l. : Elettronica e Telecomunicazioni, 2002.

11. **wikipedia.** wikipedia . [Online] http://it.wikipedia.org/wiki/DVB-T.

12. *Digital video broadcasting over satellite (DVB-S): a system for broadcasting and contribution applications.* **M.Cominetti, A.Morello.** s.l. : International Journal on Satellite Communications, 2000.

13. *Il sistema europeo (DVB-S) per la diffusione televisiva da satellite.* **M.Cominetti, A.Morello.** 3, 1994, Vol. Elettronica e Telecomunicazioni.

14. **ETSI Digital Video Broadcasting (DVB).** wikipedia. [Online] http://it.wikipedia.org/wiki/DVB-S.

15. **DVB-MHP.** *DVB-MHP.* [Online] http://www.mhp.org/.

16. **Wikipedia.** Sistema di accesso condizionato. *Sistema di accesso condizionato.* [Online] http://it.wikipedia.org/wiki/Sistema_di_accesso_condizionato.

17. **Review, EBU Technical.** Functional model of a conditional access system. *Functional model of a conditional access system.* [Online] 1995. http://www.ebu.ch/en/technical/trev/trev_266-ca.pdf.

18. **Ho, Tong.** Digital Video Broadcasting Conditional Access Architecture. *Digital Video Broadcasting Conditional Access Architecture.* [Online] http://www.cs.sjsu.edu/~stamp/CS265/projects/papers/dvbca.pdf.

19. **Namba, Dr. Seiichi.** http://www.nhk.or.jp. *nhk.or.jp.* [Online] Broadcast Technology, 2002 n°12. http://www.nhk.or.jp/strl/publica/bt/en/le0012.pdf.

20. **Ralf-Philipp Weinmann, Kai Wirt.** Analysis of the DVB Common Scrambling Algorithm. *Analysis of the DVB Common Scrambling Algorithm.* [Online] Ottobre 12, 2004. http://www.cdc.informatik.tu-darmstadt.de/~kwirt/csa.pdf .

21. **Wei Li, Dawu Gu.** http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4402690. *http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4402690.* [Online] Department of Computer Science and Engineering Shanghai Jiao Tong University Shanghai 200240, China.

22. **Wirt, Kai.** http://eprint.iacr.org. [Online] Technical University Darmstadt Department of Computer Science Darmstadt, Germany. http://eprint.iacr.org/2004/289.pdf.

23. **Fu-Kuan Tu, Chi-Sung Laih, Hsu-Hung Tung.** On key distribution management for conditional access system on pay-TV system. [Online] http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=754430.

24. **ESKICIOGLU, AHMET M.** A Prepositioned Secret Sharing Scheme for Message. *A Prepositioned Secret Sharing Scheme for Message.* [Online] http://www.sci.brooklyn.cuny.edu/~eskicioglu/papers/CMS2001.pdf.

25. **Tecchi, Elena.** http://www.cs.unibo.it. [Online] 2007. http://www.cs.unibo.it/~margara/page2/page6/page25/assets/Smart%20Card.pdf.

26. **Massimiliano, Gioia Sergio - Leone Marco - Natella.** [Online] http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-0304/TV_Satellitare/index.htm.

27. **Candilio, Gioacchino.** La pirateria della televisione a pagamento in Europa: storia, aspetti tecnici e proposte. [Online] http://www.ciberspazioediritto.org/articoli/candilio.pdf.

28. [Online] http://web.tiscali.it/galassirino/smart.htm.

29. **Scalzo, Gaetano Lo.** [Online] 2007-2008. http://www.ippari.unict.it/wikippari/storage/users/87/87/images/154/Progetto%20Sicurezza%201%20-%20La%20tv%20satellitare.pdf.