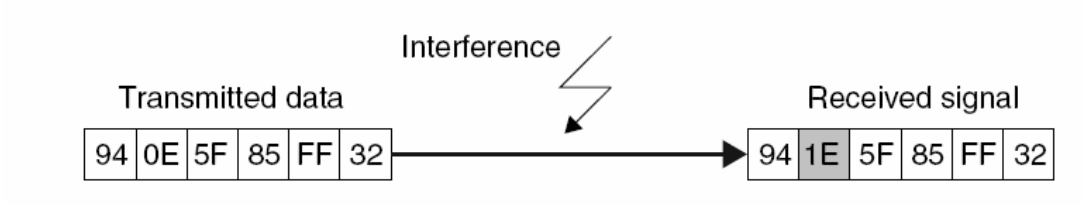
Integrità dei dati

- Il riconoscimento degli errori in trasmissione/ricezione viene effettuato con le

  Procedure di Checksum.
  - Parity check
  - XOR checksum (Longitudinal Redundancy Check)
  - CRC (Cyclic Redundancy Check)



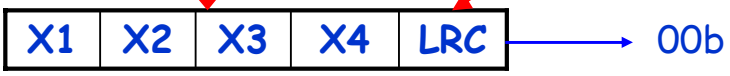
Parity check

- 1 bit di parità ogni 8 bit di informazioni
  - Se stabiliamo "odd parity" il bit di parità assume il valore che fa sì che sui 9 bit ci sia un numero *dispari* di uno
  - Se stabiliamo "even parity" sui 9 bit c'e' un numero *pari* di 1.
- Es: 8bit= A4h = 10100100b
  - se odd parity: parity bit p=0
  - se even parity: parity bit p=1 (=xor di tutti gli 8 bit – 2a2)
- Il bit di parità viene inviato dal trasmettitore ogni 8 bit. Il ricevitore ogni 8 bit calcola il bit di parità e lo confronta con quello ricevuto.
- Possiamo rilevare solo un numero *dispari* di errori su singoli bit:
  - se $P(\#errori=1) = E \ll 1$, allora $P(\#errori>1) \approx E^2$
- Gli errori non possono essere corretti: è necessario ritrasmettere il byte.

XOR sum – LRC
Longitudinal Redundancy Check

- XOR ricorsivo di tutti i byte in un blocco di dati bit a bit
  - es. per 4 byte: LRC = (((X1 xor X2) xor X3) xor X4)
  - trasmettitore

  - ricevitore



  - al ricevitore basta eseguire lo xor ricorsivo di tutti i bit ricevuti. Se il risultato fa zero non ci sono errori
  - ((((X1 xor X2) xor X3) xor X4) xor LRC) = 0
  - MOLTO VELOCE --- NON E' SENSIBILE ALL'ORDINE DEI BYTE

CRC – Cyclic Redundancy Check

- Pensata per grandi blocchi di dati: inizialmente per hard disk
- E' una procedura ciclica. Per ogni nuovo byte si calcola il CRC in funzione del byte stesso e del CRC calcolato per il byte precedente.
- Il CRC è il resto della divisione di una stringa di bit per un "polinomio generatore"

- Poniamo:
  - S stringa di "N" bit
  - G stringa di "M+1" bit (il cosidetto polinomio generatore)
  - C stringa di "M" bit, resto della divisione S/G modulo 2

  - Consideriamo S, G, e C dei polinomi

CRC (II)

- G è un polinomio, nel senso che il valore del bit i-esimo come il coefficiente del termine di grado i di un polinomio. Per es.:
- $10010 = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 \leftrightarrow x^4 + x^1$

- la divisione viene fatta modulo 2. Per capire come funziona vediamo prima una moltiplicazione modulo 2

```
      111 x
     1011
     ----
      111
     111
    000
  111
  ------
  110001
```

E' molto più facile da implementare:

- somme senza carry
- moltiplicazioni x 1 o per 0
- interpretazione in termini moltiplicazione modulo 2 di polinomi: $(x^2+x^1+1)(x^3+x^1+1)=x^5+x^4+1$

CRC (III) - Divisione modulo 2

- Prendiamo l'esempio 110001:111

```
          110001
          111          1
          -----
   XOR    00100
            111        01
            ---
  XOR        111
             111         1
             ---
             000 = RESTO        QUOZIENTE = 1011
```

- Nota: ((A xor B) xor B) = A
- Nel calcolo del CRC ci interessa solo il resto. Quindi basta un hardware dedicato che sappia fare XOR e shift

CRC (IV) – In trasmissione

- Dividiamo modulo 2 Sx^M / G, Q è il quoziente, C è il resto, cioè

  $Sx^M = Q\,G + C$

- C è il CRC, ed è l'unica quantità che ci interessa
- Vediamo l'esempio a lato:
- S=10100011 (N=9)
- G=110101 (M=5)

- Il trasmettitore invia N+M bit:
- prima S e poi C

```
Sx^M      10100011000000
G          110101
          ------
           0111011
            110101
           -------
            00111010
              110101
             -------
              00111100
                110101
               -------
                001001000
                  110101
                 -------
                  0100010
                   110101
                  -------
                   010111
```

C = 10111 è il crc.

CRC (V) in ricezione

- In ricezione il sistema divide tutti gli N+M bit per G (modulo): se ottiene resto zero il crc è corretto.

- Gli N+M bit sono $Sx^M + C$

- Nota:
- $(Sx^M+C)/G = (QG + C + C)/G = Q$.

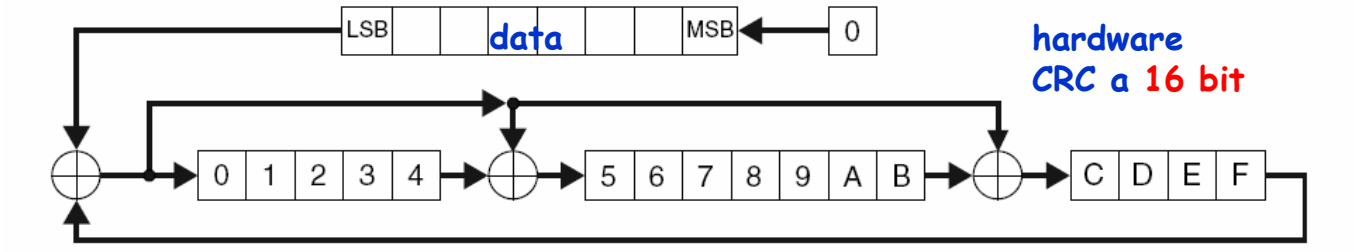
- Nota: C+C=0 (perché facciamo tutto modulo 2).

Esempio:

```
Sx^M + C  10100011010111
G          110101
          ------
           0111011
            110101
           -------
            00111010
              110101
             -------
              00111110
                110101
               -------
                00101111
                  110101
                 -------
                  0110101
                   110101
                  -------
                   000000
```

CRC (VI)

- Importante: trasmettitore e ricevitore DEVONO essere entrambi a conoscenza del polinomio generatore.
- Per un CRC a M bit, la probabilità che due stringhe qualsiasi abbiamo lo stesso CRC è $1/2^M$ (se M=16 → 2^{-16} = 1.5e-5).
- I polinomi generatori più diffusi sono:
  - per il CRC a 16 bit: $x^{16} + x^{12} + x^5 + 1$ (Standard X25)
  - per il CRC a 32 bit: $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^3+x^2+x+1$ (Ethernet standard).



CRC (VII)

- Un aspetto importante del CRC è il fatto che permette di rilevare L bit sbagliati consecutivi, se L < M.
- Poniamo che S e T siano stringhe di N bit che differiscono di L bit consecutivi
- Possiamo definire $D=(S-T)x^M$
- D ha K zeri in testa, poi una stringa E di L bit, e in coda (N-K-L) zeri → $D = Ex^L$

- D = 000000<E>0000000

  K L N-K-L

- E < G, e quindi $D = Ex^L$ non è divisibile per G (il resto non è zero), quindi il CRC non torna.

Procedure multi-accesso (I)

- Spesso molti transponder sono presenti nella regione di interrogazione del lettore. Abbiamo quindi un tipo di comunicazione ASIMMETRICA tra lettore e transponder:
  - Quando il lettore trasmette tutti i transponder ascoltano → cioè abbiamo una comunicazione BROADCAST (come la radio, la tv "classica", etc.)
  - Quando i vari transponder trasmettono, e solo il lettore riceve, i vari transponder competono per l'attenzione del transponder: comunicazione MULTI-ACCESSO. La "capacità del canale" viene divisa tra i vari transponder presenti nella regione di interrogazione.
- Sono necessarie procedure ANTI-COLLISIONE per permettere ad ogni transponder di trasferire i suoi dati al lettore senza interferenza mutua (appunto, collisione).
  - I problemi di collisione sono presenti in numerose tecnologie di telecomunicazione: per esempio telefonia cellulare (più terminali cercano di comunicare con la stazione della singola cella)

Tecniche di accesso multiplo (anticollisione)

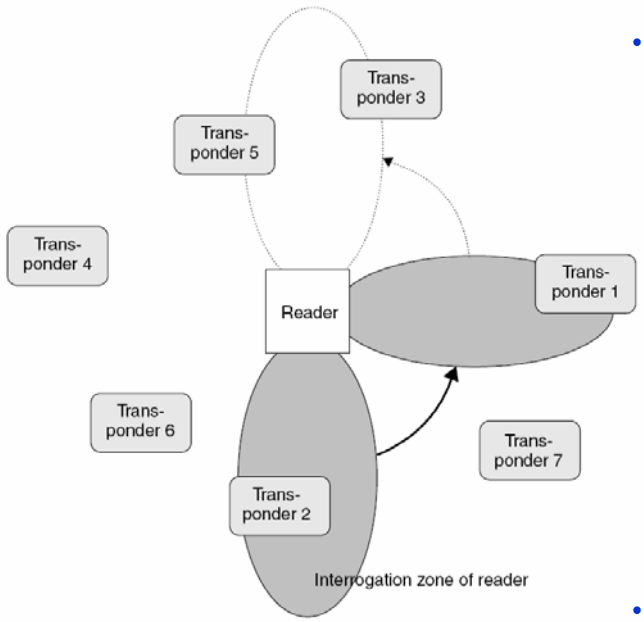
Classificazione "tradizionale"
Accesso multiplo a divisione di:

- spazio – Space (SDMA)
- codice – Code (CDMA)
- tempo – Time (TDMA)
- frequenza - Frequency (FDMA)

DMA = "Division Multiple Access"

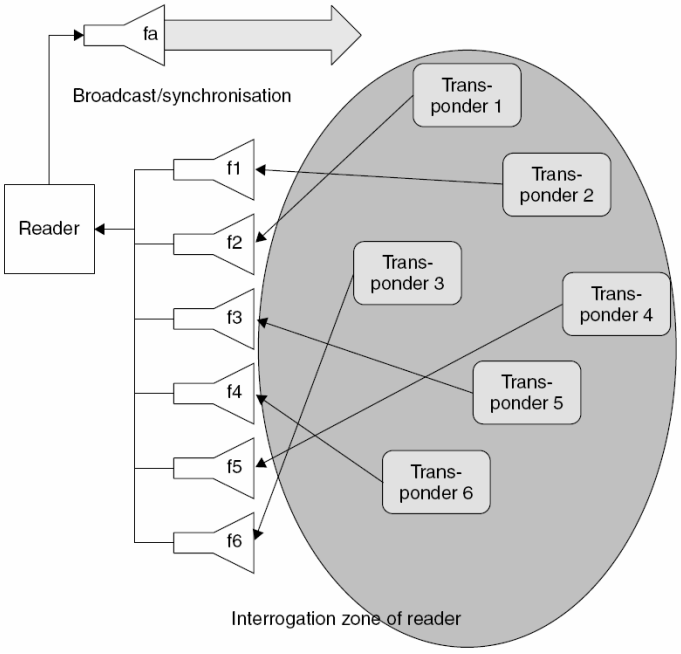
- Di solito queste procedure sono impiegate in casi in cui c'è un flusso di dati ininterrotto a cui viene assegnata una parte della capacità totale del canale.
- I transponder RFID sono invece attivi per periodi di tempo molto brevi con basso duty cycle.
- La capacità del canale deve essere suddivisa solo per il tempo necessario per la trasmissione dei dati.
- E' quindi una trasmissione a pacchetti: tipicamente UN SOLO PACCHETTO per ogni transponder.
- I transponder NON ASCOLTANO gli altri transponder, e quindi non si possono accorgere di una eventuale collisione. Solo il lettore se ne puo' accorgere.
- Quasi tutte le procedure commerciali sono coperte da brevetti.

SDMA
(Space Division Multiple Access)



- Si restringe la regione di interrogazione in modo che non ci sia mai più di un tranponder:
  - riducendo la portata
  - usando un'antenna direttiva per il lettore [ruotata meccanicamente o elettronicamente (phased array) come in un RADAR] (si puo' fare a UHF o microonde)
- Ha il vantaggio che si riesce anche a localizzare spazialmente il transponder

FDMA
(Frequency Division Multiple Access)



- ogni transponder trasmette a una frequenza differente nella banda utilizzabile o modula il backscatter con una diversa sottoportante.
- Il lettore trasmette a una frequenza fissata (downlink e alimentazione) e puo' ricevere su più frequenze contemporaneamente.
- Il lettore è molto costoso,

TDMA
(Time Division Multiple Access)

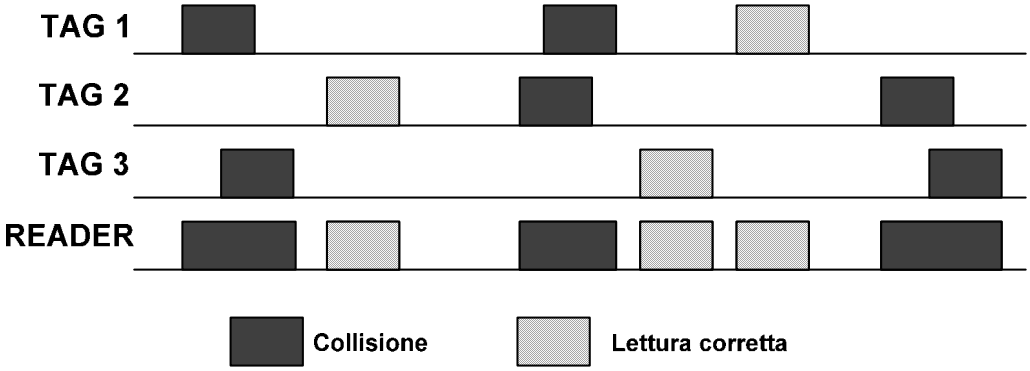
- E' la procedura più diffusa
- I transponder trasmettono in intervalli di tempo differenti
- Abbiamo procedure
  - "transponder driven" – a iniziativa del transponder
  - "interrogator driven" – a iniziativa del lettore
- Le trasponder driven sono asincrone, perché non c'è un agente UNICO che controlli il trasferimento di dati, e stabilisce il "clock" del sistema.
- Sono in generale più lente, e meno intelligenti (non c'e' una "regia").

TDMA – Classificazione (II)

- a iniziativa del transponder (asincrone)
  - transponder spenti dopo la lettura
  - transponder non spenti dopo la lettura
    - a ciclo infinito
    - a scorrimento continuo
- a iniziativa del lettore (sincrone)
  - lista (polling)
    - lista predefinita
    - censo dinamico (dynamic census)
  - ricerca binaria
    - selezione predefinita di un gruppo
    - selezione dinamica di un gruppo

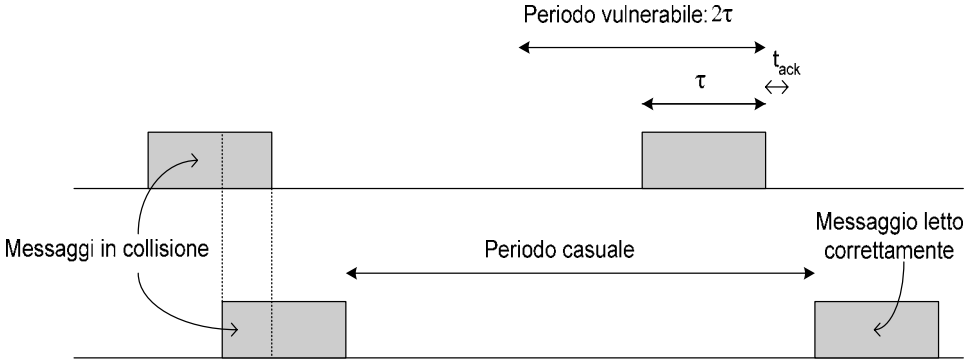
Procedura ALOHA (I)

- Rientra nella categoria a transponder-driven
- Derivata da ALOHANET, la rete radio di trasmissione a pacchetto di dati sviluppata alle Hawaii negli anni 70.
- Ogni transponder trasmette in continuazione un breve pacchetto (contenente ad esempio il proprio numero seriale) a istanti casuali
- Se un pacchetto arriva al reader senza collisioni, viene letto correttamente



ALOHA (II)

- Durata del pacchetto τ — Tempo di osservazione T
- Supponiamo il transponder i-esimo trasmetta in T in media $\nu_i T$ volte:
  - $dp_i = \nu_i dt$ → probabilità che il tag i inizi a transmettere in dt
  - $dp = \sum_i \nu_i dt = \nu dt$ → prob.che un tag inizi a trasmettere in dt
- Calcoliamo la probabilità che il tag i possa trasmettere senza collisioni: è necessario che per un tempo 2τ tutti gli altri transponder non comincino a trasmettere:



ALOHA (III)

- Poniamo N >> 1: se il "silenzio" è durato t, la probabilità che duri altri dt è

$$p(t+dt) = p(t)(1-\nu dt) \rightarrow \frac{dp}{dt} = -\nu p \rightarrow\rightarrow p(t) = \exp(-\nu t)$$

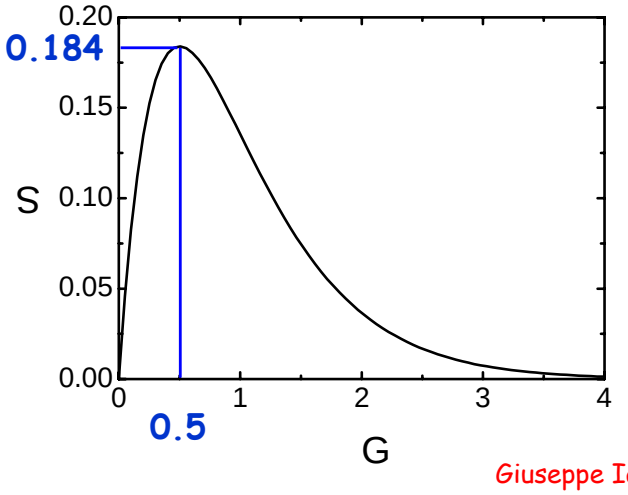
- La probabilità p_0 è: $p_0 = p(2\tau) = \exp(-2\nu\tau)$
- Il numero di tag che possono essere letti in T è in media il prodotto tra i tentativi di trasmissione e la probabilità che ciascun tentativo vada a buon fine:
  $\langle N \rangle = \nu T p_0 = \nu T \exp(-2\nu\tau)$
- Il "carico offerto" (offered load) G è il numero medio di tag che trasmettono contemporaneamente, che si puo' ottenere come rapporto tra la somma dei tempi durante i quali ciascun transponder trasmette e il tempo totale di ascolto:

$$G = \frac{\tau \sum_i \nu_i T}{T} = \nu\tau$$

ALOHA (IV)

- Il throughput S è il numero medio di pacchetti che a un certo istante si stanno leggendo correttamente (0<S<1), e si ottiene come rapporto tra il tempo impiegato a leggere pacchetti corretti (senza collisioni) e tempo totale di ascolto

$$S = \frac{\tau \sum_i \nu_i T p_0}{T} = G p_0 = G \exp(-2G)$$



$$\frac{dS}{dG} = \exp(-2G) - 2G\exp(-2G)$$

- dS/dG = 0 → G=0.5, S= 0.184
- Se G è piccolo, il canale è praticamente inutilizzato
- Se G è grande, ci sono troppe collisioni.

ALOHA (V)

- Tentativi che in media un tag deve fare prima di essere letto

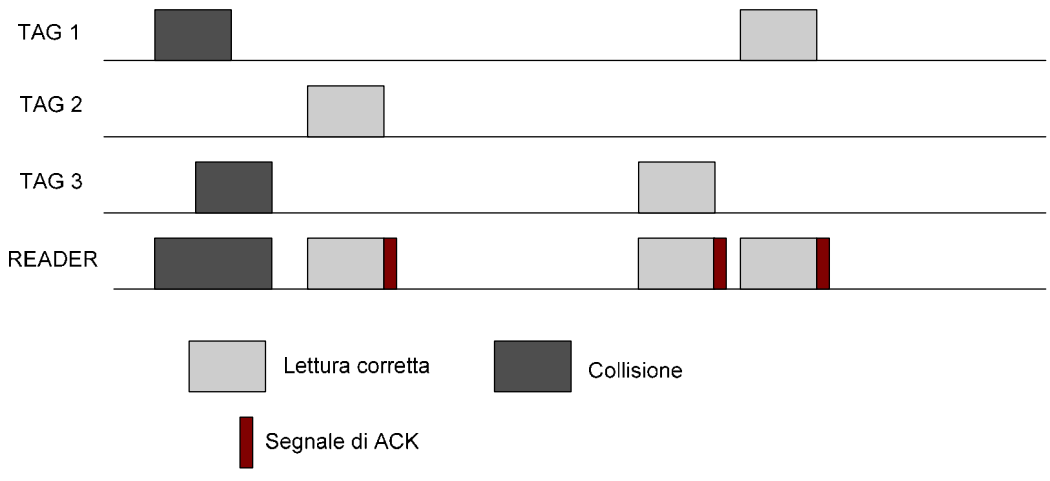
$$p_0^{-1} = \frac{G}{S} = e^{2G}$$

- Tentativi senza successo: $\frac{G}{S} - 1 = e^{2G} - 1$
- tempo medio tra due tentativi di trasmissione: $\frac{M}{\nu} = \frac{M}{G}\tau = L\tau$ dove M è il numero di tag; L = M/G
- Tempo medio di attesa per ogni tag da quando comincia a trasmettere a quando viene letto correttamente

$$E[T_{tag}] = \tau + (e^{2G} - 1)(\tau + L\tau) = \tau\left[1 + \left(\exp\left(\frac{2M}{L}\right) - 1\right)(1 + L)\right]$$

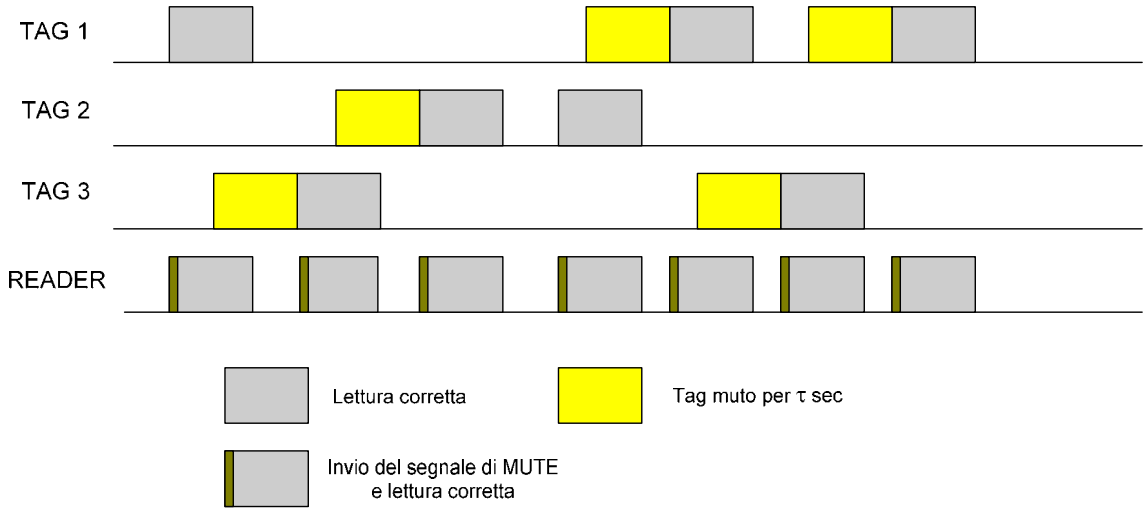
Varianti: ALOHA Switch off

- Dopo che un pacchetto è stato ricevuto correttamente, il lettore trasmette un breve pacchetto di acknowledgment (ACK), e il tag che ha appena finito di trasmettere si disattiva fino a nuovo ordine



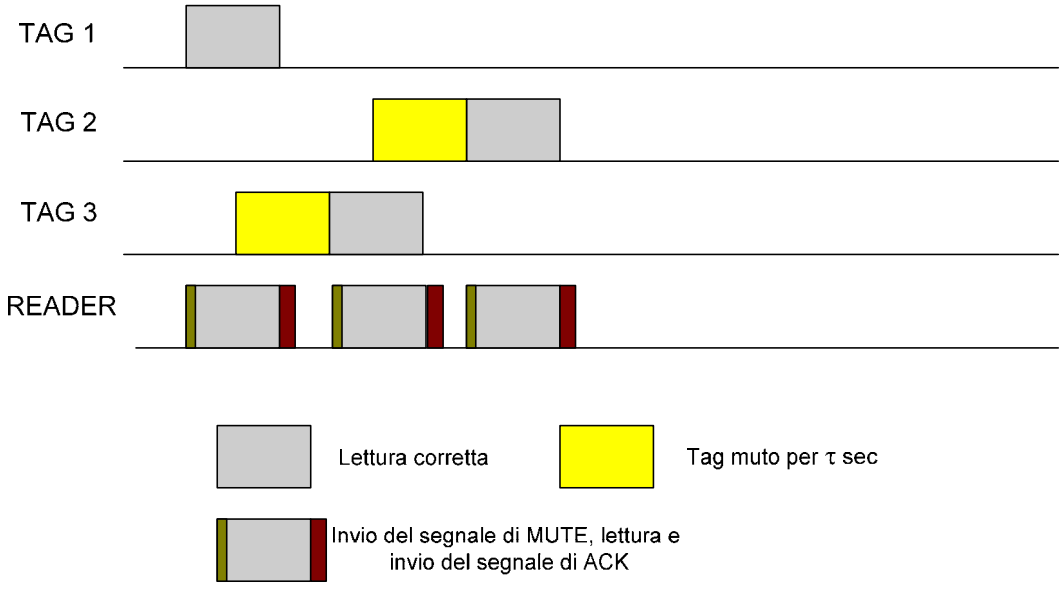
Varianti: ALOHA Fast

- Appena il lettore comincia a ricevere un pacchetto manda un segnale di MUTE: tutti i tag che non stanno trasmettendo evitano di trasmettere per un periodo di mute di durata τ.

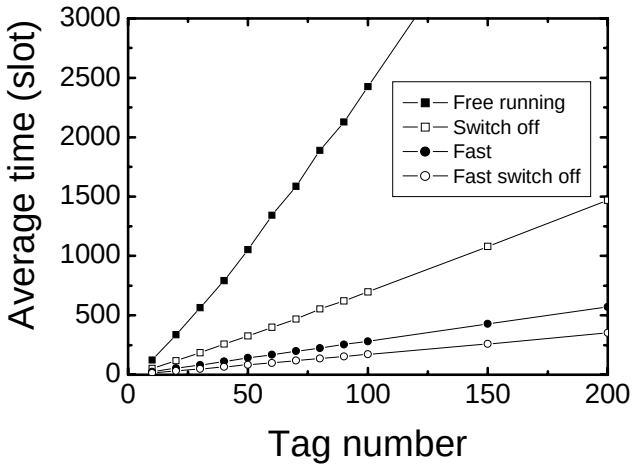


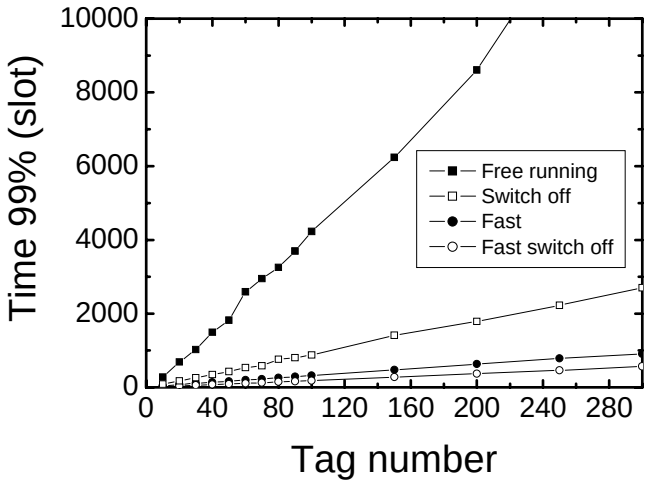
Varianti: Aloha Fast Switch Off

- Il lettore manda sia il segnale di MUTE sia di ACK.



Confronto Prestazioni ALOHA

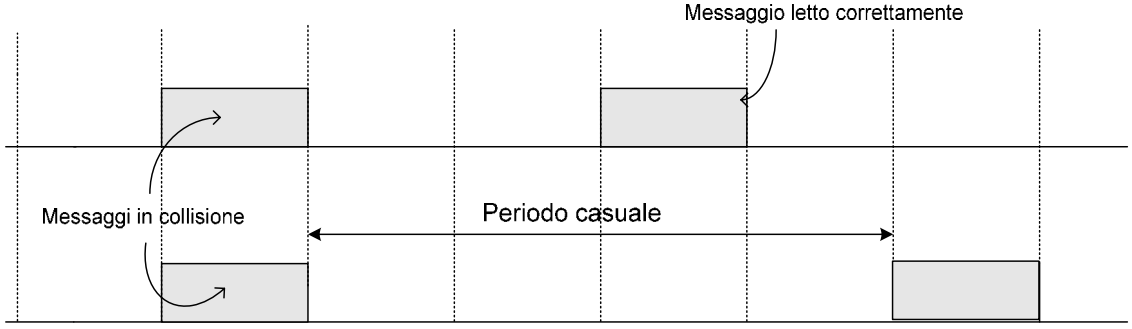




- **Tempo medio di lettura di tutti i tag (in unità di durata di un pacchetto) (per L=16)**
- **Tempo dopo il quale la probabilità di aver letto tutti i tag è il 99%.**

Aloha Slotted (I)

- **I transponder possono cominciare a trasmettere i loro pacchetti solo a istanti di tempo predeterminati, stabiliti dal lettore, che definiscono degli slot**
- **Il periodo di "silenzio" necessario per non avere collisioni è τ e non più 2τ**
- **Abbiamo:** $p_0 = \exp(-\nu\tau) = \exp(-G)$ $\quad S = G\exp(-G)$



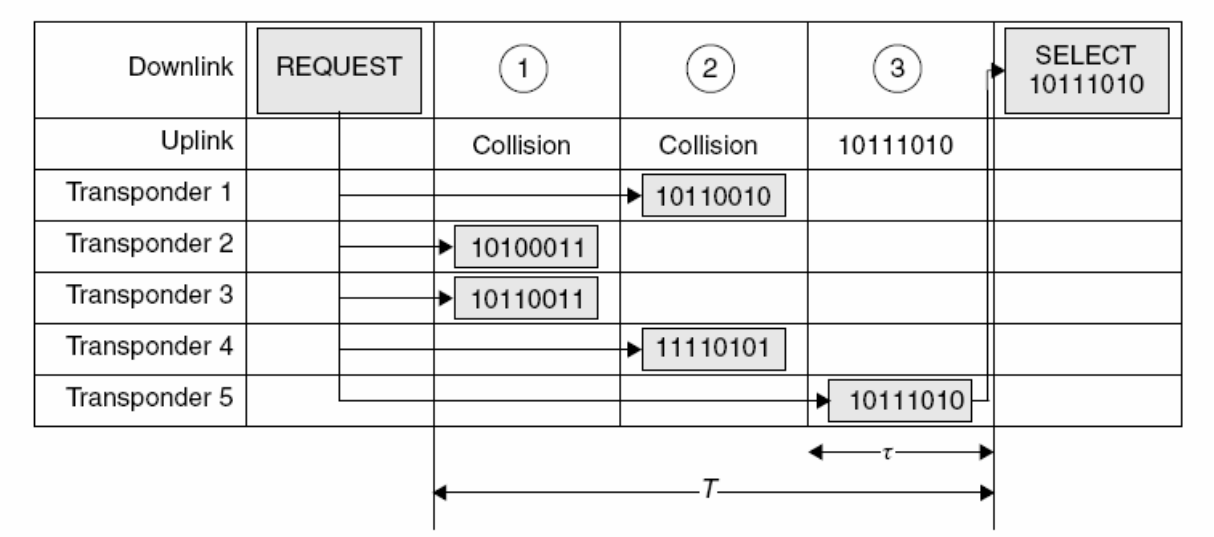
Aloha Slotted (II)

- Calcoliamo il throughput massimo:

$$\frac{dS}{dG} = \exp(-G) - G\exp(-G) = 0 \rightarrow G = 1$$

- per $G=1$ abbiamo $S=e^{-1}=0.368$ (circa il doppio dell'Aloha semplice).
- Per la procedura Aloha slotted, ogni transponder deve avere un unico numero seriale, il lettore deve poter inviare alcuni comandi:
  - REQUEST: il lettore invita i transponder a trasmettere in uno degli slot disponibili
  - SELECT (Serial Number): il lettore seleziona il transponder corrispondente a Serial Number per la comunicazione
  - ... altri comandi di lettura e scrittura ...

Aloha Slotted (III)



- Solo il transpoder 5 viene letto correttamente e selezionato.

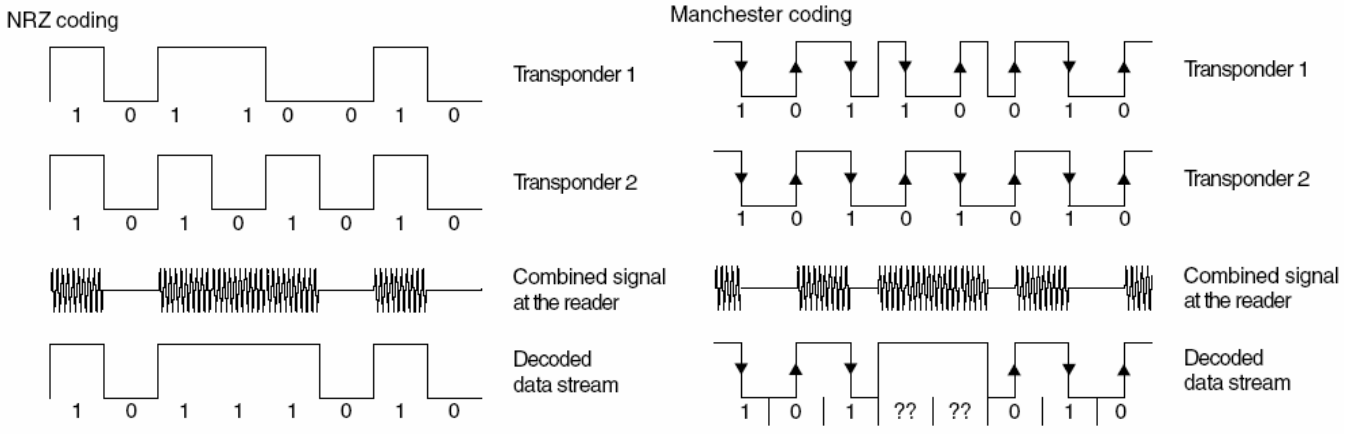
Varianti dell'Aloha Slotted

- **Aloha Slotted Dinamico**
- Con ogni request il lettore trasmette anche il numero di slot disponibili.
- Ogni transponder trasmette su uno degli slot disponibili (a caso)
- Il numero degli slot disponibili viene modificato in modo adattivo:
  - se ci sono troppe collisioni, il numero di slot viene aumentato (per ridurre la congestione di traffico
  - se non ci sono collisioni, il numero di slot viene diminuito (per ridurre il tempo medio di lettura).

- **Aloha Slotted Switch Off**
- Si puo' inserire un comando di switch off per silenziare i transponder che sono stati letti (e ridurre la congestione).

Ricerca Binaria (I)

- Le procedure di ricerca binaria richiedono si usi una codifica che permetta al lettore di riconoscere per quale bit si è avuta una collisione.



- NRZ non permette di sapere a che bit c'è stata collisione
- Manchester permette di sapere a che bit c'è stata collisione

Ricerca Binaria (II)

- Ogni transponder ha un numero seriale unico
- La procedura consente al lettore di selezionare un transponder alla volta
- Il lettore deve sincronizzare tutti i transponder
- Il lettore deve poter inviare alcuni comandi:
  - Request (SN): chiede a tutti i tranponder con numero seriale < SN di transmettere il proprio numero seriale
  - Select (SN): seleziona il transponder con numero seriale SN
  - Comandi di Read/Write/etc. sul transponder selezionato
  - Unselect: deleziona il transponder e lo porta in modalita "mute" in modo che non risponda a "Request" successivi

Esempio Ricerca binaria

Codici presenti:

10110010
10100011
10110011
11100011

1°passo:

Richiesta del reader	11111111
Tag in risposta	10110010 10100011 10110011 11100011
Risultato	1X1X001X

2°passo:

Richiesta del reader	10111111
Tag in risposta	10110010 10100011 10110011
Risultato	101X001X

3°passo:

Richiesta del reader	10101111
Tag in risposta	10100011
Risultato	10100011

4°passo:

Richiesta del reader	10111111
Tag in risposta	10110010 10110011
Risultato	1011001X

5°passo:

Richiesta del reader	10110010
Tag in risposta	10110010
Risultato	10110010

6°passo:

Richiesta del reader	10111111
Tag in risposta	10110011
Risultato	10110011

7°passo:

Richiesta del reader	11111111
Tag in risposta	11100011
Risultato	11100011

Giuseppe Iannaccone - 2005

Ricerca Binaria (III)

- E' assolutamente necessario che la trasmissione dei vari transponder sia sincronizzata.
- Il numero medio L di iterazioni necessarie per leggere N transponder è

$$L = \log_2 N + 1 = \frac{\ln N}{\ln 2} + 1$$

- Si puo' ridurre del 50% il tempo di lettura totale con una Ricerca binaria dinamica:
  - si dimezza il numero di bit trasmessi se si fa in modo che il lettore trasmetta la prima parte del numero seriale (fino al primo bit dove c'è stata collisione) e ogni transponder trasmetta solo i bit restanti

Esempio Ricerca binaria dinamica

Codici presenti:

10110010
10100011
10110011
11100011

1°passo:

Richiesta del reader	ε
Tag in risposta	10110010 10100011 10110011 11100011
Risultato	1X1X001X

2°passo:

Richiesta del reader	10
Tag in risposta	110010 100011 110011
Risultato	101X001X

3°passo:

Richiesta del reader	1010
Tag in risposta	0011
Risultato	10100011

4°passo:

Richiesta del reader	10
Tag in risposta	110010 110011
Risultato	1011001X

5°passo:

Richiesta del reader	10110010
Tag in risposta	(10110010)
Risultato	10110010

6°passo:

Richiesta del reader	10
Tag in risposta	110011
Risultato	110011

7°passo:

Richiesta del reader	ε
Tag in risposta	11100011
Risultato	11100011

Ricerca ad albero casuale (random tree)

- supponiamo ci siano M transponder
- ciascun transponder i estrae un numero casuale ki con distribuzione uniforme tra 1 e B.
- il tempo necessario per spedire un pacchetto è uno slot. B slot formano un frame

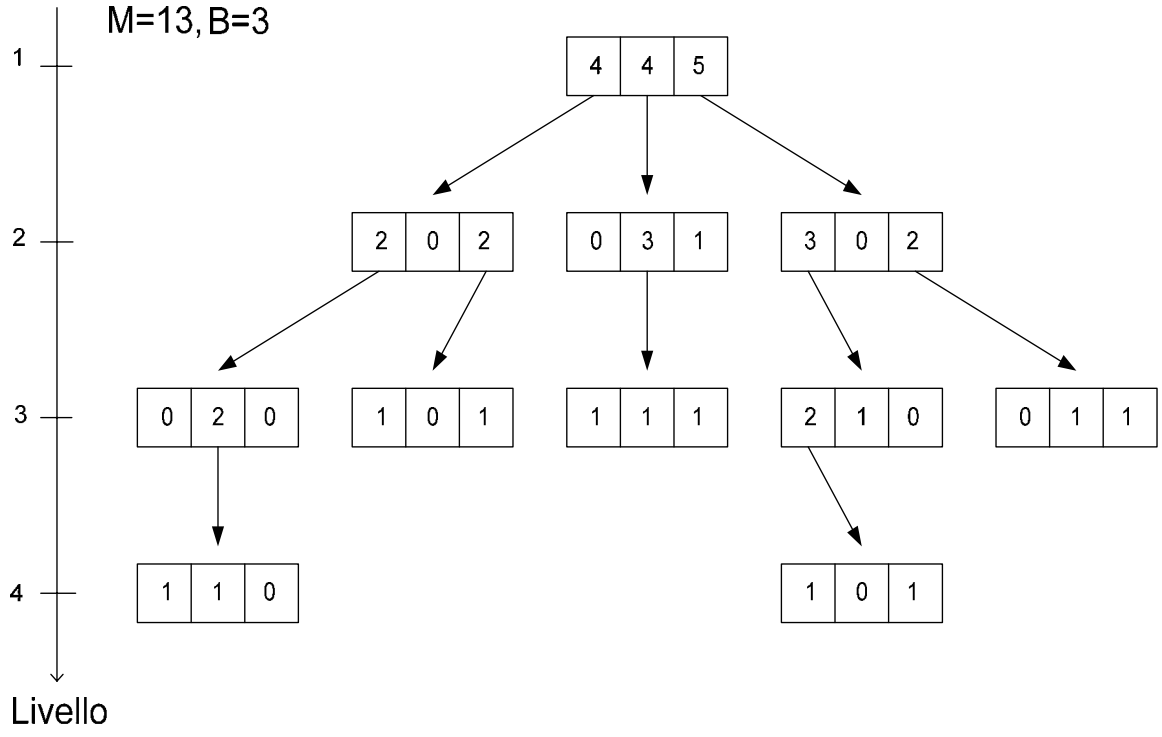
Nel primo frame, ogni trasponder trasmette nello slot ki.

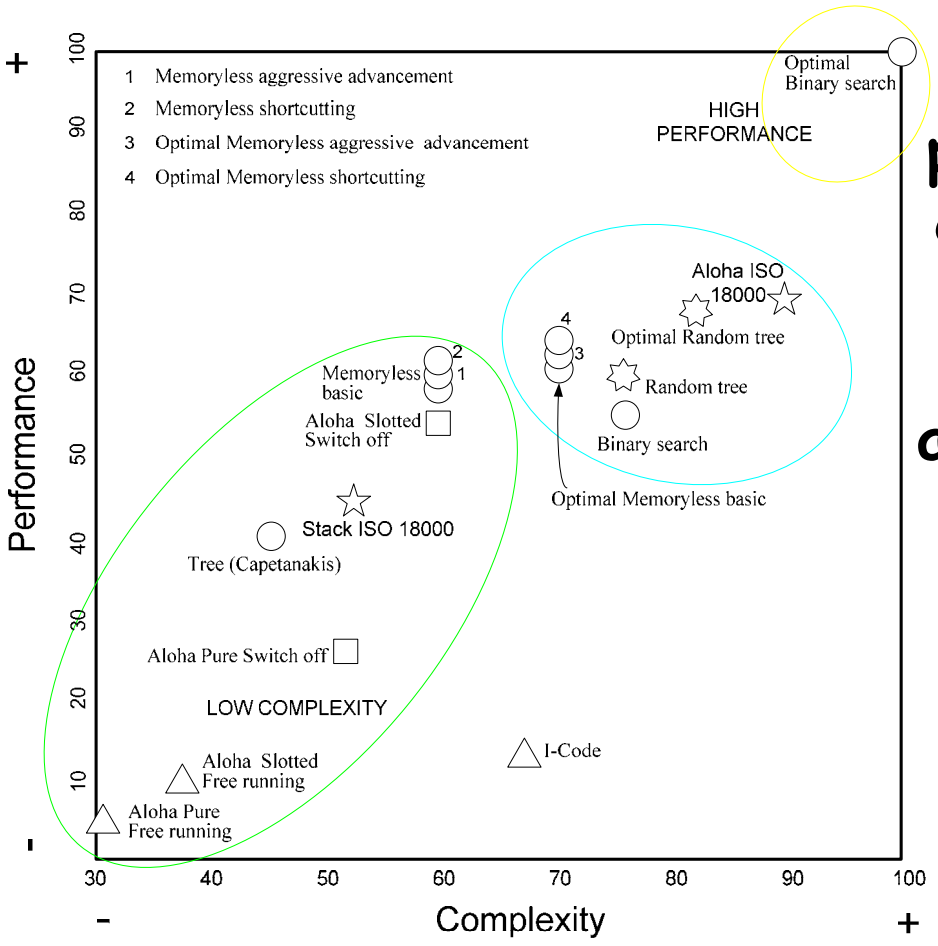
- Il lettore comunica in quali slot c'e' stata collisione.
- Le collisioni sono risolte a partire dal primo slot in cui c'è stata collisione.

Nel secondo frame rispondono solo i tag che hanno trasmesso nel primo slot, generando un nuovo ki tra 1 e B...

- La procedura continua in modo ricorsivo. in questo modo si forma un albero casuale

Ricerca ad albero casuale - esempio





Confronto prestazioni/ complessità per alcuni protocolli anticollisione

Sicurezza dei dati

- La sicurezza dei dati è particolarmente importante per sistemi RFID impiegati per il controllo dell'accesso, per effettuare pagamenti, per applicazionie del tipo biglietteria elettronica
- Sono necessari Protocolli di autenticazione

- Sistemi sicuri di RFID si devono difendere dai seguenti tipi di attacchi:
  - Lettura non autorizzata dei dati, per duplicazione e alterazione
  - Contraffazione del transponder/lettore per accesso non autorizzato o per ricevere un servizio senza pagamento
  - Ascolto della comunicazione (eavesdropping) e registrazione, per contraffare un transponder.
- In tutte le applicazioni sensibili a questi attacchi, è importante considerare la possibilità di inserire procedure di crittografia nella comunicazione tra RFID e transponder.

Autenticazione mutua e simmetrica

"autenticazione" mutua in tre passi ISO 9798-2

- Il transponder deve proteggersi da una lettura/scrittura non autorizzata della propria memoria
- Il lettore deve proteggere l'applicazione che controlla da dati manipolati
- L'autenticazione avviene se i due partecipanti alla comunicazione conoscono una chiave segreta crittografica K. Ogni partecipante controlla che l'altro conosca la chiave secondo una procedura challenge-response. In questo senso l'autenticazione è mutua e simmetrica.

Autenticazione Mutua e Simmetrica

1. Il lettore invia al transponder il comando GET_CHALLENGE
2. Il transponder invia al lettore un numero casuale R1 (challenge)
3. Il lettore genera un numero casuale R2, usando un algoritmo ALG noto calcola la stringa token1 = ALG (R1, R2, K) e lo transmette al transponder (response + challenge)
4. Il transponder conosce l'algoritmo inverso e ricava R1,R2 = ALG^{-1} (token1,K). Se riconosce R1 il lettore e' stato riconosciuto.
5. Il transponder genera un numero casuale R3 da cui ottiene la stringa token2 = ALG (R2, R3, K), che trasmette al lettore (response)
6. Il lettore riceve la stringa, la decritta R2,R3= ALG^{-1} (token2,K): se riconosce R2 l'autenticazione è completa.

Autenticazione mutua e simmetrica

- VANTAGGI
  - le chiavi segrete non sono mai trasmesse. Sono trasmessi solo i numeri casuali crittati (token1 e token2).
  - L'uso di numeri casuali generati sia da lettore sia da transponder impedisce che si possa registrare il segnale di token e poi fare un playback per l'accesso.
  - L'algoritmo di crittazione/decrittazione puo' essere pubblico. Il token is critta/decritta solo se si conosce K.
  - Uno dei numeri casuali (R2,R3) puo' essere usato come chiave casuale (session key) per la trasmissione dei dati successivi.
- SVANTAGGI
  - C'è una chiave unica per tutti i transponder della stessa applicazione.
  - Se l'applicazione è con tanti transponder, abbiamo una potenziale fonte di pericolo (troppi transponder conoscono la chiave).
  - Se la chiave di un transponder viene scoperta, tutto il sistema è vulnerabile.

Autenticazione con chiavi derivate

- In fase di produzione, in ogni transponder è immagazzinata una chiave diversa Kx funzione di una chiave master KM e del numero seriale del transponder ID: Kx = fun (KM,ID). Il lettore conosce KM (il transponder no). fun è pubblica.

1. Il lettore chiede al transponder di inviare l'ID
2. il transponder invia l'ID (in chiaro)
3. il lettore calcola Kx= fun (KM,ID)

a questo punto si torna al caso precedente utilizzando come chiave Kx.

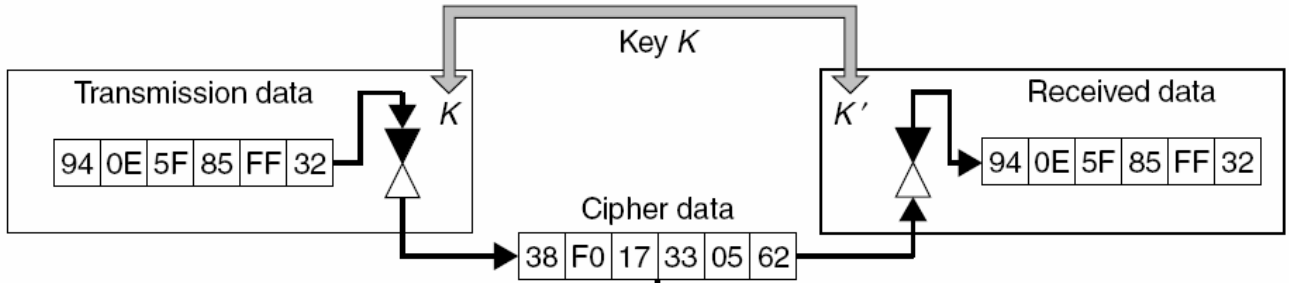
KM è memorizzata solo nel lettore. La Kx di un transponder è inutilizzabile per accedere agli altri.

Trasferimento di dati crittati/cifrati

- Necessità di difendere la comunicazione da
  - Attacchi passivi: ascolto per carpire le informazioni comunicate (eavesdropping)
  - Attacchi attivi: manipolazione dell'informazione che arriva al lettore/transponder
- Prima di essere spediti, i dati vengono crittati usando un algoritmo segreto e una chiave segreta K.
- Il ricevitore, conosce la chiave segreta K' e l'algoritmo ed è in grado di decrittare i dati.
- Se K=K' o ricavabili direttamente l'una dall'altra, si dice che la procedura è a chiave simmetrica
- Se la conoscenza di K è irrilevante per decrittare i dati, si dice che la procedura è a chiave asimmetrica

Cifratura Sequenziale (I)

- In sistemi RFID si usano solo procedure a chiave simmetrica
- Possiamo avere:
  - cifratura sequenziale (un byte alla volta) -stream ciphering
  - cifratura a blocchi (di più byte) – block ciphering
- La cifratura a blocchi richiede capacità computazionali più elevate: nei sistemi RFID si usa la cifratura stream.

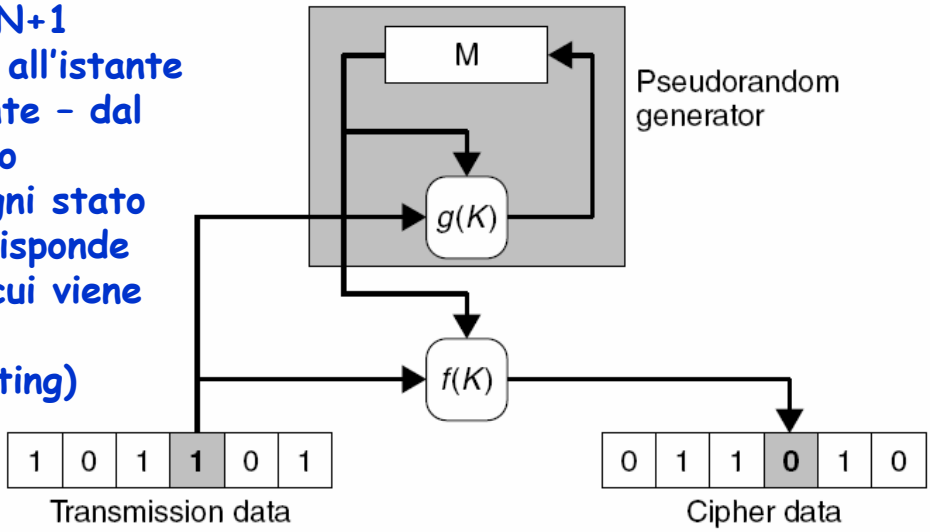


Cifratura sequenziale (II)

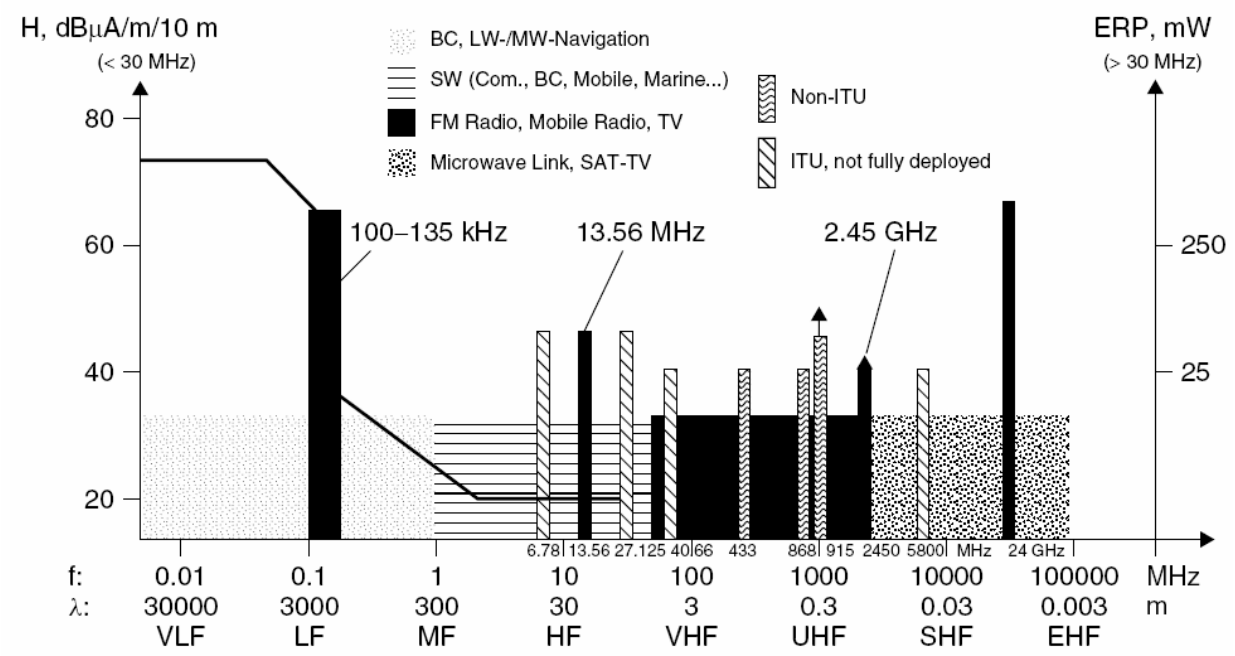
- Ogni byte viene crittato con una chiave diversa
- Il caso ideale è la cifratura Vernam:
  1. Una chiave K viene generata in modo casuale come stringa di bit e viene resa disponibile alle due parti
  2. K viene usata per cifrare i dati (XOR gating bit a bit)
- IMPORTANTE: la chiave deve essere lunga almeno quanto il messaggio e deve essere usata SOLO una volta. In questo modo la sicurezza è garantita se si riesce a trasmettere la chiave in modo sicuro.
- Se la chiave fosse più corta del messaggio, e dovesse essere ripetuta più volte durante la cifratura, sarebbe possibile decrittare il messaggio con procedure di "criptoanalisi".
- La cifratura Vernam in questa forma è sicura ma NON è pratica. (Come si fa a spedire in modo sicuro una chiave lunga quanto il messaggio?).

Cifratura Sequenziale (III)

- La modifica più ragionevole è quindi usare come chiave una stringa di bit pseudocasuale (invece che casuale), usando un generatore pseudocasuale segreto presente sia nel trasmettitore sia nel ricevitore.
- Un generatore pseudocasuale è una macchina a stati, in cui lo stato all'istante N+1 dipende dallo stato all'istante N ed – eventualmente – dal carattere trasmesso all'istante N. Ad ogni stato della macchina corrisponde una carattere con cui viene cifrato il carattere trasmesso (XOR gating)



Regolamentazione delle frequenza



Bande ISM disponibili per sistemi RFID

- **9-125 KHz – Onde lunghe**
  - non è riservato ai servizi ISM: sono presenti i sistemi di navigazione marina e costiera (Loran C, Omega, Decca), segnale orario, servizi radio militari. Portata radio ~ 1000 Km
- **6.78 MHz – Onde Corte**
  - portata ~ 100 Km giorno/transcontinentale note
  - In Francia è utilizzato per sistemi RFID ma non ovunque
- **13.56 MHz – Onde corte (13.553-13.567)**
  - portata transcontinentale
  - banda affollata: Telecomandi, servizi radio, pagers
- **27.125 MHz – Onde corte**
  - Applicazioni industriali, CB in Europa e US (4 W in trasmissione per 30 Km di portata).

Bande ISM disponibili per sistemi RFID

- 40.68 MHz – VHF
  - non ci sono sistemi RFID: telecomandi, televisione (VHF1)
- 433 MHz – UHF
  - Propagazione ottica e assorbimento significativo da edifici
  - Banda affollatissima: Molti sistemi RFID + banda assegnata ai radioamatori (30-300 Km), baby intercom, telecomandi x cancelli, walkie talkie, cuffie wireless, etc ...
- 869 MHz – UHF (868-870)
  - Banda assegnata a short-range devices (anche RFID) in Europa
- 916 MHz – UHF (902-920)
  - In US e Australia (non Europa) è disponibile per sistemi RFID. Molto vicina alle bande dedicate a cellulari (1G) e telefoni cordless

Bande ISM disponibili per sistemi RFID

- 2.45 GHz
  - propagazione ottica e forte assorbimento attraverso edifici
  - trasmettitori per telemetria, wireless lan (WiFi etc.)
- 5.8 GHz
  - servizi di radiolocazione, wireless lan (WiFi)
- 24.5 GHz
  - disponibile, ancora non utilizzata da sistemi RFID

Regolamenti Europei – CEPT/ERC REC 70/03

- **Short Range Devices**

Table 5.2 Short range device applications from REC 70-03

Annex	Application
Annex 1	Non-specific Short Range Devices
Annex 2	Devices for Detecting Avalanche Victims
Annex 3	Local Area Networks, RLANs and HIPERLANs
Annex 4	Automatic Vehicle Identification for Railways (AVI)
Annex 5	Road Transport and Traffic Telematics (RTTT)
Annex 6	Equipment for Detecting Movement and Equipment for Alert
Annex 7	Alarms
Annex 8	Model Control
Annex 9	Inductive Applications
Annex 10	Radio Microphones
Annex 11	RFID
Annex 12	Ultra Low Power Active Medical Implants
Annex 13	Wireless Audio Applications

Regolamenti Europei – CEPT/ERC REC 70/03

Table 5.3 Non-specific short range devices

Frequency band	Power	Comment
6785–6795 kHz	42 dBμA/m @ 10 m	
13.553–13.567 MHz	42 dBμA/m @ 10 m	
26.957–27.283 MHz	42 dBμA/m	(10 mW ERP)
40.660–40.700 MHz	10 mW ERP	
138.2–138.45 MHz	10 mW ERP	Only available in some states
433.050–434.790 MHz	10 mW ERP	<10% duty cycle
433.050–434.790 MHz	1 mW ERP	Up to 100% duty cycle
868.000–868.600 MHz	25 mW ERP	<1% duty cycle
868.700–869.200 MHz	25 mW ERP	<0.1% duty cycle
869.300–869.400 MHz	10 mW ERP	
869.400–860.650 MHz	500 mW ERP	<10% duty cycle
869.700–870.000 MHz	5 mW ERP	
2400–2483.5 MHz	10 mW EIRP	
5725–5875 MHz	25 mW EIRP	
24.00–24.25 GHz	100 mW	
61.0–61.5	100 mW EIRP	
122–123 GHz	100 mW EIRP	
244–246 GHz	10 mW EIRP	

Relevant harmonised standards: EN 300 220, EN 300 330, EN 300 440.

Giuseppe Iannaccone - 2005

Regolamenti Europei – CEPT/ERC REC 70/03

Table 5.4 Railway applications

Frequency band	Power	Comment
4515 kHz	7 dB μA/m @ 10 m	Euroloop (spectrum mask available)
27.095 MHz	42 dB μA/m	Eurobalise (5 dBμA/m @ ±200 kHz
2446–2454 MHz	500 mW EIRP	Transponder applications (AVI)

Relevant harmonised standards: EN 300 761, EN 300 330.

Table 5.5 Road Transport and Traffic Telematics (RTTT)

Frequency band	Power	Comment
5795–5815 MHz	8 W EIRP	Road toll systems
63–64 GHz	t.b.d.	Vehicle — vehicle communication
76–77 GHz	55 dBm peak	Vehicle — radar systems

Relevant harmonised standards: EN 300 674, EN 301 091, EN 201 674.

Table 5.7 RFID applications

Frequency band	Power	Comment
2446–2454 MHz	500 mW EIRP	100% duty cycle
	4 W EIRP	<15% duty cycle; only within buildings

Relevant harmonised standards: EN 300 440.

Giuseppe Iannaccone - 2005