

Tutto ciò che avreste voluto sapere sulle schede telefoniche

Rubrica a cura di Stefano Rossi e Gianfranco Marchese

ospitata da:

Schede Telefoniche.org



 4° - Decodifica e traduzione dei codici

3° - Codifica schede telefoniche Urmet

Ultima revisione del: 01/08/2017 12:33

Tutto quello che avreste voluto sapere sulle schede telefoniche

Decodifica e traduzione dei codici

3-Codifica schede telefoniche Urmet

Come già visto nel paragrafo "Ad occhio nudo", ecco come appare una scheda telefonica se vista per mezzo del lentino magnetico:



A differenza delle normali schede magnetiche, la scheda telefonica presenta la propria banda magnetica spezzata in tre bande, di cui la prima e la terza sono uguali. Perché?

Purtroppo non si hanno informazioni ufficiali a tal riguardo, per cui posso avanzare solo delle ipotesi che non hanno carattere di ufficialità.

All'interno della scheda telefonica sono contenuti dati ma soprattutto soldi! Riuscire a falsificare una scheda telefonica può dare la possibilità al malintenzionato di eseguire telefonate a costo zero a danno della compagnia telefonica. Ecco allora la necessità di trovare un sistema capace di non consentire frodi, tenendo in considerazione due grandi punti deboli:

 Cabine telefoniche: queste sono disseminate lungo tutto il territorio in zone anche remote, prive di sorveglianza. La possibilità che un malintenzionato possa rubare una intera cabina telefonica non è fantascientifica. Considerando che all'interno della cabina c'è tutto la tecnologia necessaria alla decodifica della scheda telefonica l'eventualità potrebbe offrire tutto il necessario per crackare il sistema;

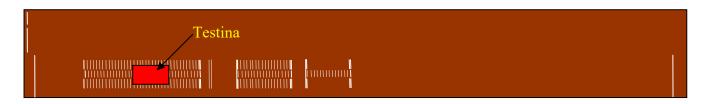
Tutto quello che avreste voluto sapere sulle schede telefoniche

 Schede telefoniche: al suo interno è contenuta l'informazione che consente di potere eseguire telefonate. E' di facile reperibilità e non utilizza tecnologia aliena: una qualsiasi testina potrebbe leggerne il contenuto;

Quindi sia schede telefoniche che cabine possono dare ottimi spunti alla decodifica del sistema. Allora? Il sistema a tre bande sembra essere stato realizzato proprio per questo motivo: i normali scrittori di badge e tessere non possono scrivere una singola traccia spezzata in tre parti, per cui a meno di non disporre di testine di scrittura realizzate ad hoc (quindi non reperibili facilmente in commercio) risulta impossibile poter riprodurre fedelmente la scrittura delle tracce.

E la lettura??

Sebbene la traccia sia spezzata in tre la lettura va eseguita per mezzo di una sola testina, il segnale risultante sarà la somma delle tre bande lette contemporaneamente:



La risultante finale della lettura sarà quindi la somma contemporanea delle singole tracce:

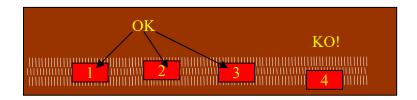
MAGNETISMO = (50% BANDA 1) + (100%BANDA 2) + (50%BANDA 3)

Questa particolare disposizione delle tre bande fa si che anche minimi spostamenti verticali della testina assicurino una corretta lettura: la

Tutto quello che avreste voluto sapere sulle schede telefoniche

traccia centrale verrà sempre letta al 100% mentre le due restanti assicureranno un apporto complessivo pari al 100%.

Provo a schematizzare di seguito:



Nel primo caso la testina si trova in posizione centrale e legge esattamente due metà delle bande superiore e inferiore; nel secondo e nel terzo caso invece la testina si trova posizionata non simmetricamente e occupa porzioni differenti della prima e terza banda: poiché le due bande sono identiche l'apporto totale sarà sempre il medesimo:

- 1) MAGNETISMO = (50% BANDA 1) + (100%BANDA 2) + (50%BANDA 3)
- 2) MAGNETISMO = (25% BANDA 1) + (100%BANDA 2) + (75%BANDA 3)
- 3) MAGNETISMO = (75% BANDA 1) + (100%BANDA 2) + (25%BANDA 3)
- 4) MAGNETISMO = (0% BANDA_1) + (80%BANDA 2) + (100%BANDA 3)

Nei primi tre i casi il risultato sarà sempre lo stesso, indipendentemente dalla posizione verticale della testina poiché la somma delle bande 1 e 3 fa 100%. Nel quarto caso la somma di 1 e 3 fa sempre 100% ma la banda centrale non è del tutto coperta quindi il risultato finale sarà incompleto.

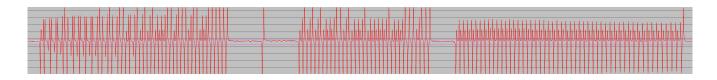
Per i motivi indicati nel capitolo di introduzione, non disponendo (e non volendo disporre) di strumentazione originale URMET è necessario affidarsi a quel che si può trovare regolarmente in commercio, come un lettore per badge.

I lettori in commercio sono progettati per leggere bande magnetiche codificate secondo certi standard definiti dall'ISO. E' possibile utilizzare queste testine per leggere una scheda telefonica ANCHE SE la dimensione della testina possibilmente non è tale da coprire

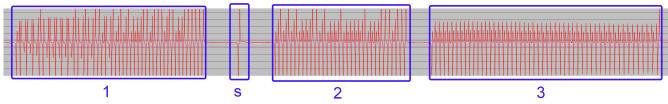
Tutto quello che avreste voluto sapere sulle schede telefoniche

perfettamente quella centrale e due metà di quelle superiore e inferiore: la risultante della lettura contemporanea delle tre bande sarà quindi differente rispetto alla lettura eseguita da strumentazione URMET originale costruita ad hoc.

Posizionando correttamente la testina del badge, analizzando l'output così prodotto per mezzo di un oscilloscopio, ecco cosa otteniamo:

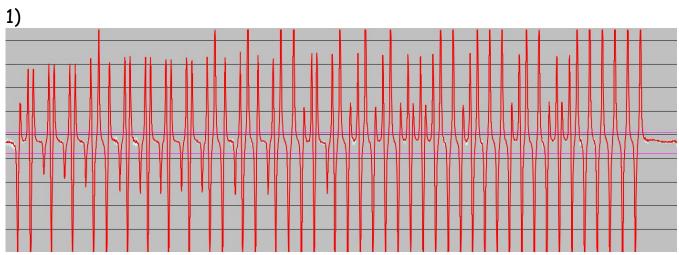


La banda magnetica è evidentemente suddivisa in più sezioni, ognuna rappresenta informazioni differenti, eccetto la sezione "S" che sembra avere l'unica funzione di separare le sezioni 1 e 2:

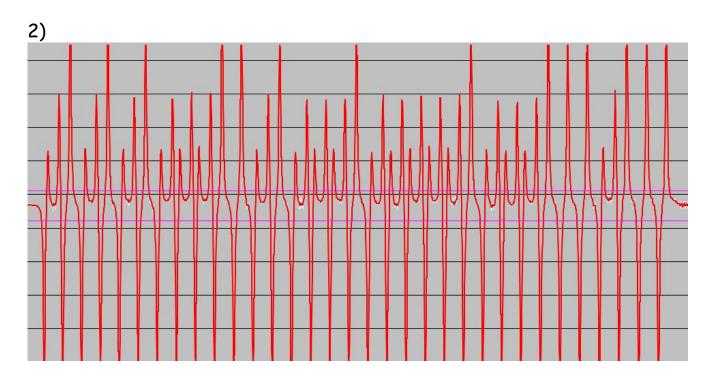


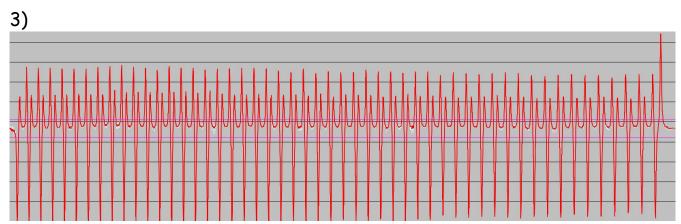
Ogni sezione è contenuta tra una coppia di picchi positivo/negativo che non concorrono ai fini della determinazione dei bit.

Zoomando:



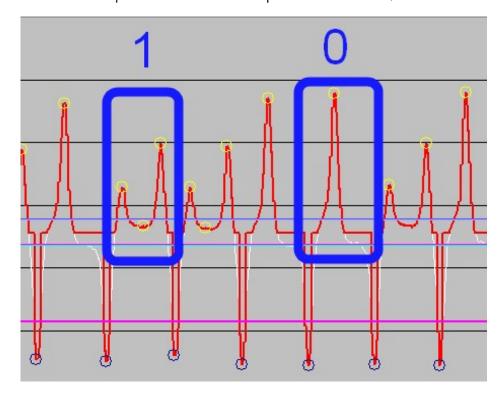
Tutto quello che avreste voluto sapere sulle schede telefoniche





Analizzando attentamente la banda è possibile identificare due tipologie di configurazioni che si susseguono l'una con l'altra (abbiamo identificato in questo modo le modalità con cui viene rappresentata l'informazione binaria). Effettuiamo uno zoom sulla banda ed esaminiamola nel dettaglio:

Tutto quello che avreste voluto sapere sulle schede telefoniche



Innanzitutto, ogni informazione è contenuta tra due picchi negativi che costituiscono in questo modo il clock del segnale. Nello specifico, tra due picchi negativi possiamo trovare due picchi positivi oppure uno solo: se tra due picchi negativi troviamo un solo picco positivo allora abbiamo l'informazione "O", se abbiamo invece due picchi positivi l'informazione rappresentata sarà "1". In questo modo e per tutta la banda della scheda telefonica, vengono immagazzinati i dati, bit dopo bit.

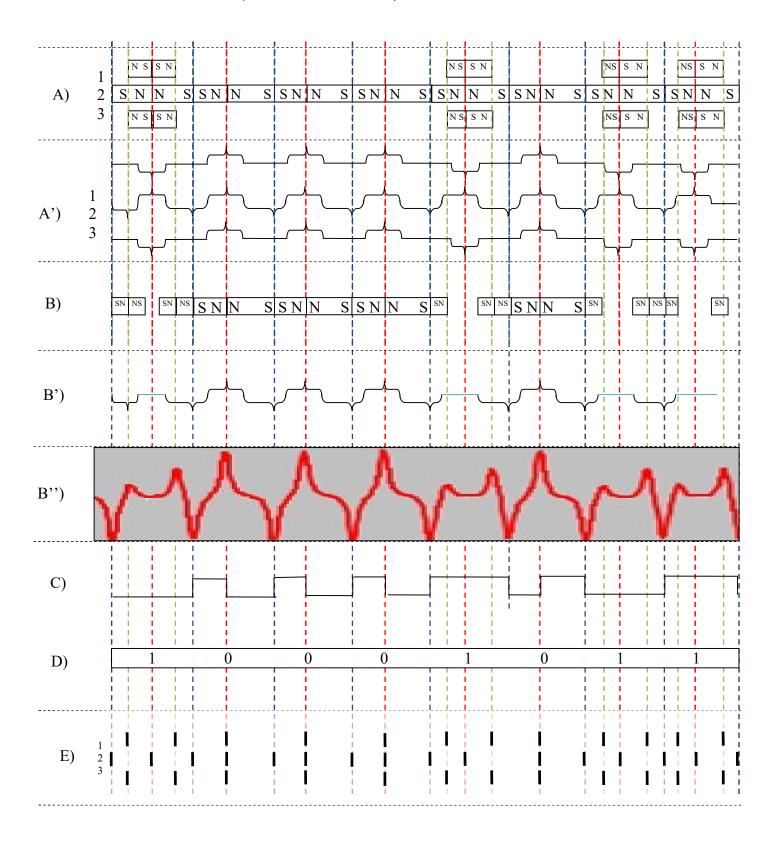
Proviamo ad azzardare il grafico che segue:

- A) Come è magnetizzata la banda magnetica;
- A') La traduzione in Volte delle tre bande magnetiche come se le leggessimo una per una;
- B) La somma delle tre bande magnetiche viste come se fosse una sola banda:
- B') La traduzione in Volts delle tre bande magnetiche lette per mezzo di un'unica testina:

Tutto quello che avreste voluto sapere sulle schede telefoniche

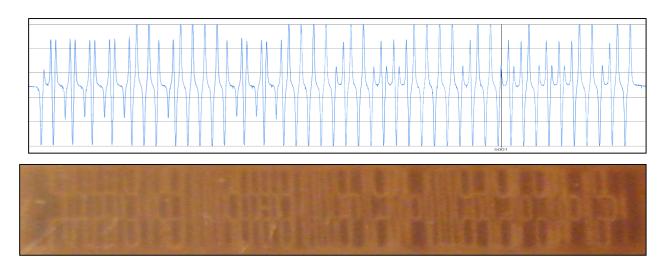
- B") Ciò che viene effettivamente letto dalla testina magnetica. B" è l'unico grafico certo, tutti gli altri sono ipotesi nate sulla base di questo;
- C) Traduzione in onda digitale del genale sinusoidale di B';
- D) Traduzione in bit del segnale;
- E) Come viene vista la banda magnetica al lentino magnetico Arnold.

Tutto quello che avreste voluto sapere sulle schede telefoniche



Tutto quello che avreste voluto sapere sulle schede telefoniche

Di seguito invece mostro la stessa scheda vista al lentino magnetico Arnold e la traduzione in Volts della stessa porzione di banda letta dalla macchinetta



Tutto quello che avreste voluto sapere sulle schede telefoniche

Rubrica ospitata da:

Schede Telefoniche .org

Pagine consigliate





Tutto quello che avreste voluto sapere sulle schede telefoniche

Manleva

Tutto ciò che troverete all'interno di questo documento (foto, informazioni, grafici, notizie, etc) è pubblicato a mero scopo informativo di interesse collezionistico, ottenuto sulla base di deduzioni e studi personali, talvolta ispirati a informazioni reperite verbalmente. Nessuna delle informazioni riportate su tale documento è stata reperita in violazione delle leggi vigenti né mediante l'utilizzo di strumenti dall'uso non consentito o limitato. Nessuna responsabilità viene assunta in relazione sia al contenuto ed all'uso che terzi ne potranno fare.

Nessun contenuto ha carattere ufficiale né tanto meno confermato dalle società telefoniche o da qualsiasi altra società/azienda/ente/persona nominata direttamente o indirettamente all'interno del presente documento.

Gianfranco Marchese, Stefano Rossi e il sito Schetetelefoniche.org, e tutti coloro che sono coinvolti nella stesura del presente documento, non si assumeranno responsabilità derivanti da un uso non corretto di quanto scritto su di esso, tra cui, a mero titolo esemplificativo e non esaustivo:

- materiali contenuti in siti/documenti di terzi raggiungibili/reperibili direttamente/indirettamente da indicazioni/link contenuti nel presente documento;
- errori, inesattezze ed omissioni che tuttavia sono sempre possibili. Si declina, pertanto, qualsiasi responsabilità per errori, inesattezze ed omissioni eventualmente presenti nel sito;

Pertanto gli scriventi non saranno tenuti in nessun caso, per qualsiasi titolo, a rispondere in ordine a danni, perdite, danneggiamento di beni inclusi i dati, o altre perdite economiche o commerciali, pregiudizi di qualsiasi genere che terzi potranno subire a causa del contatto intervenuto con questo documento, oppure a seguito dell'uso di quanto nello stesso pubblicato, anche se informati della possibilità di tali danni, o se tali danni siano prevedibili.

Il presente documento non costituisce testata giornalistica; non ha, comunque, carattere periodico ed è aggiornato secondo la disponibilità e la reperibilità dei materiali (dei provvedimenti, degli articoli e dei materiali ivi contenuti). Pertanto, non può essere considerato in alcun modo un prodotto editoriale ai sensi della L. n. 62 del 7.03.2001.