

Introduzione alle SDR ...

... e alle trasmissioni accidentali

Alessandro Barenghi

22 maggio 2019

Sommario

Background, ben compreso

- Fondamenti, brutalizzati, di fisica
- Fondamenti, brutalizzati di trattamento segnali
- SDR, breve introduzione all' uso

Cosa può andar storto?

- Emissioni (stupide) intenzionali
- Emissioni non intenzionali
- Forzare la mano: TEMPEST

Disclaimer

Take a deep breath

- Stiamo per vedere il compresso di 35+ CFU
- La compressione non è **priva di perdite**
 - diciamo che la prenderemo un po' qualitativa
- La fisica che vedremo è quella classica (no approccio quantistico)
- Fourier, Maxwell, Gauss, Lorenz, Shannon: perdonatemi.

Campo elettrico, campo magnetico

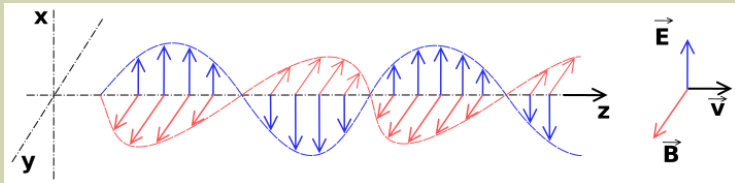
.. in una slide

- Campo Elettrico (CE): generato da una carica (e.g., elettrone)
- Campo Magnetico (CM): non ha un singolo generatore (no monopoli)
- Maxwell-Faraday: $\nabla \times \mathbf{E} = -\frac{\partial \mathbf{B}}{\partial t}$
 - Variare il (flusso di) CM fa variare il CE
- Ampère: $\nabla \times \mathbf{B} = \mu_0 \left(\mathbf{J} + \varepsilon_0 \frac{\partial \mathbf{E}}{\partial t} \right)$
 - Variare il CE o spostare cariche fa variare il CM
- N.B. CE e CM esistono anche nel vuoto

Onde elettromagnetiche

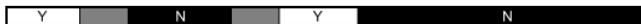
.. in una slide

- Una variazione di CE causa una variazione di CM
- ... che causa una variazione di CE, che causa una variazione di CM ...
- C'è una continua, mutua variazione di CE e CM nello spazio!
- Il fenomeno, autosostentante è un'onda elettromagnetica
 - Si propaga, nel vuoto, alla velocità della luce (per def.)



Spettro EM, tutto

Penetrates Earth's
Atmosphere?



Radiation Type
Wavelength (m)

Radio
 10^3

Microwave
 10^{-2}

Infrared
 10^{-5}

Visible
 0.5×10^{-6}

Ultraviolet
 10^{-8}

X-ray
 10^{-10}

Gamma ray
 10^{-12}

Approximate Scale
of Wavelength



Buildings

Humans

Butterflies

Needle Point

Protozoans

Molecules

Atoms

Atomic Nuclei

Frequency (Hz)



10^4

10^8

10^{12}

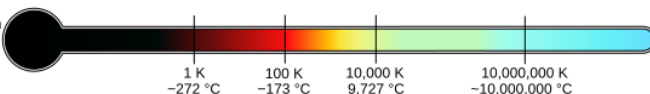
10^{15}

10^{16}

10^{18}

10^{20}

Temperature of
objects at which
this radiation is the
most intense
wavelength emitted



1 K
-272 °C

100 K
-173 °C

10,000 K
9,727 °C

10,000,000 K
~10,000,000 °C

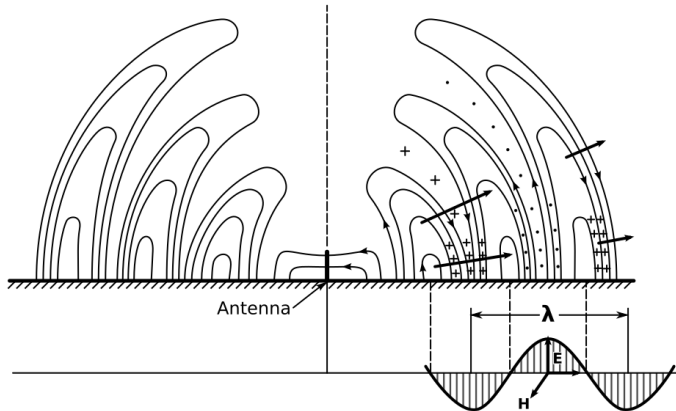
Antenne

.. in una slide

- Generiamo un CE di intensità variabile tra due conduttori
 - genererà a un CM di intensità variabile ... generando un'onda
 - mi basta “pompare” le cariche con un generatore di CA
- Metto due conduttori sul percorso di un'onda EM
 - se li oriento bene, il CM entrante genera CE tra loro,
 - essendo conduttori, il CE sposta le cariche in loro
- Due conduttori con una resistenza tra loro sono un'antenna!
 - L' antenna “trasmette” e “riceve” naturalmente, non è monodirezionale

Dipolo in funzione

Dipolo, visto di lato



Dipolo, visto da sopra

Attenuazione, direzionalità

Attenuazione del segnale

- L'onda EM emessa da un antenna si attenua
 - Naturalmente: perde intensità come $\left(\frac{c}{4\pi df}\right)^2$
 - A causa di ostacoli, mezzo non vuoto, riflessioni

Antenne direzionali

- Cambiare la forma dell'antenna cambia che forma ha il CE/CM generato
- Possiamo concentrare (moltissima del) l'energia emessa in una direzione: otteniamo un'antenna direzionale (e.g. Yagi-Uda)
 - questo vuol dire solo che l'antenna non emette/riceve in altre direzioni, non che aumenta l'energia emessa

Giocare con la natura

... con un'agenda ben precisa

- Le onde EM in una certa porzione dello spettro:
 - è suff. una quantità di energia ragionevole per generarle
 - si propagano quasi indenni attraverso a buona parte di quello che sono gli oggetti con cui interagiamo
 - possono essere ricevute con antenne di dimensioni ragionevoli
 - possiamo scegliere tempo ed energia impiegata per generarle
- Possiamo inviare/ricevere informazione con esse!
 - E' sufficiente accordarsi su un senso dato alle variazioni di tempo ed energia

Modulazione

Come trasmettere?

- Obiettivo: trasmettere un'informazione da un punto all' altro
 - Informazione continua, e.g. voce
 - Informazione discreta: simboli binari
- Come? Generando un'onda EM, variandone i parametri
 - L'onda di cui variamo i parametri è detta portante
 - L'informazione è detta modulante
- Quali parametri?

Interludio

Un diverso modo di vedere la realtà

- Solitamente, pensiamo a un segnale nel dominio del tempo
 - un valore per ogni istante di tempo che passa
- Qualcuno, nel 1822, ebbe un'idea diversa



Nuove basi

Fenomeni periodici

- Serve un modo lucido di vedere cosa succede quando abbiamo sovrapposizioni di onde diverse
- Intuizione di Fourier: **tutti** i fenomeni a energia finita si possono scomporre come somma di fenomeni periodici
- Rappresentiamo un segnale che ci piace come una funzione del tempo t

Trasformata di Fourier - 1

Trasformata di Fourier

Alcuni fatti

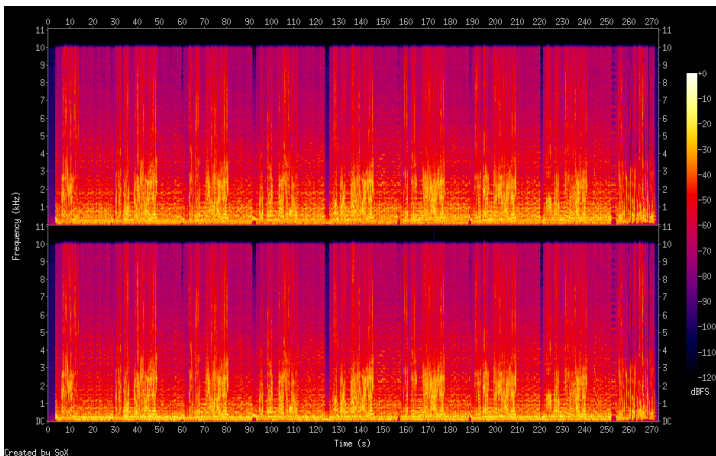
- Ogni componente della trasformata corrisponde ad una sinusoide ad una data frequenza
 - Ampiezza e fase sono i due parametri classici legati ad una sinusoide
 - E' possibile sintetizzarli in un numero complesso legato alla sinusoide dalla relazione di Eulero
 - Si può vedere la trasformata come una sequenza di numeri complessi
- L' effetto di più onde sovrapposte è semplicemente di avere più componenti complesse non nulle

Spettrogramma

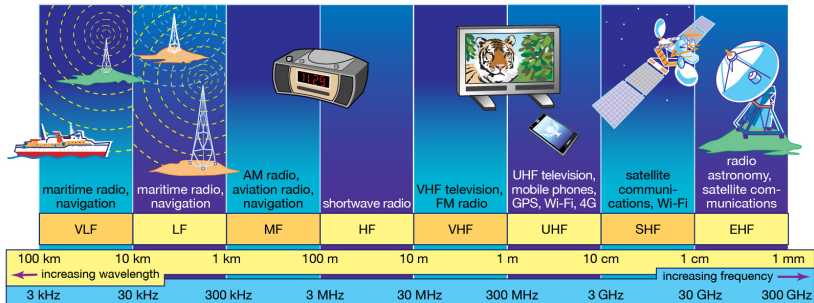
Una rappresentazione visiva

- E' utile avere una rappresentazione visiva di un fenomeno la cui trasformata di Fourier varia nel tempo
- La rappresentazione più comune è lo spettrogramma o diagramma a cascata
- Si ottiene:
 - segmentando il segnale nel tempo
 - calcolando la trasformata di ogni segmento
 - rappresentando il modulo di ogni elemento della trasformata come una riga/colonna di pixel in un immagine

Spettrogramma



Usi umani dello spettro EM

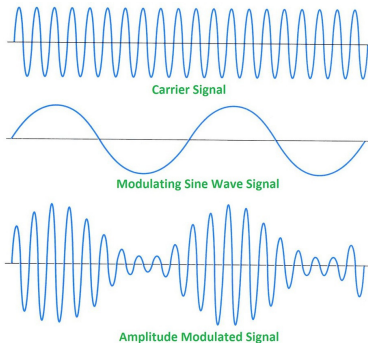


© 2013 Encyclopædia Britannica, Inc.

Modulazioni – Ampiezza

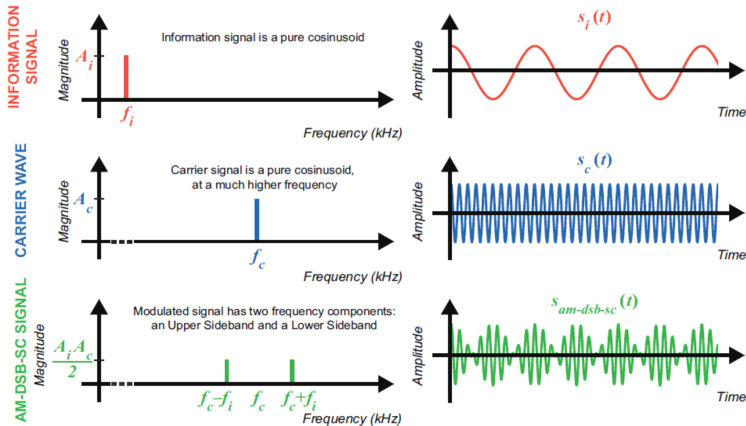
Modulante continua: $\sin(x)$

- Codifico l'informazione variando l'ampiezza della portante



Modulazioni – Ampiezza

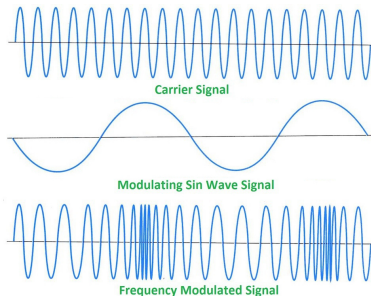
Trasformata di Fourier



Modulazioni – Frequenza

Modulante continua: $\sin(x)$

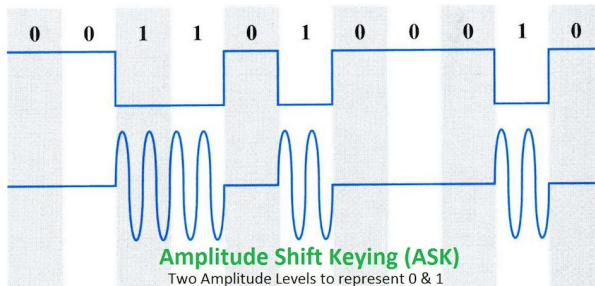
- Codifico l'informazione variando la frequenza della portante



Modulazioni – Amplitude Shift Keying

Modulante discreta

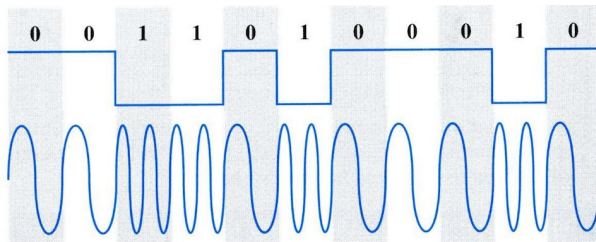
- Codifico l'informazione variando l'ampiezza della portante



Modulazioni – Frequency Shift Keying

Modulante discreta

- Codifico l'informazione variando la frequenza della portante



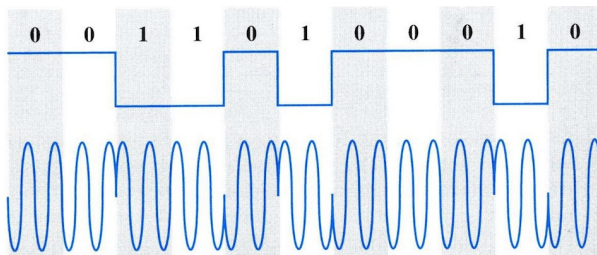
Frequency Shift Keying (FSK)

Two frequencies to represent 0 & 1

Modulazioni – Phase Shift Keying

Modulante discreta

- Codifico l'informazione variando la fase della portante



Phase Shift Keying (PSK)

Or called BPSK, uses two phases to represent 0 & 1

Consummè di SP

Filtraggio

- Trasformo il segnale, scarto delle componenti, antitrasformo
- Tolgo ciò che non mi interessa (rumore, altre trasmissioni)

Campionamento e discretizzazione

- Il segnale è continuo vs. ho un computer che calcola su numeri discreti
 - Se campiono il segnale a $2\times$ la frequenza di quello che mi interessa “non perdo nulla”
 - Se discretizzo i valori che il segnale assume nel tempo abbastanza fitti, “non me ne accorgo”

Equipaggiamento economico

Software Defined Radios

- Tipicamente, il ricevitore agisce sul segnale
 - 1 traslandolo da un intorno della portante ad un intorno dello 0
 - 2 opzionalmente discretizza, in tempo ed ampiezza
 - 3 elabora e decodifica il segnale
- Un ricevitore radio ^a, aveva sia la parte di ricezione che quella di elaborazione del segnale in hardware
 - per ragioni di efficienza, e di *costo*
- E' ora possibile fare il punto 3 completamente in software!

^afino a meno di 10 anni fa

RTL2832U

(ab) Usare un ricevitore TV digitale

- Caso emblematico: Realtek produce l' RTL2832U, un ricevitore per digitale terrestre economico
- Talmente economico che non ha nulla di specializzato per la ricezione del DVB-T, il ricevitore è generico!
- Tramite reverse engineering dei driver, si scopre che è possibile accedere al segnale grezzo ricevuto



RTL2832U

Come funziona

- L' RTL2832U effettua i seguenti passi
 - Sposta una porzione di componenti di frequenza dall' intorno di una f_c prefissata, in un intorno dello zero
 - Campiona (=discretizza nel tempo e in ampiezza) il segnale risultante
- Il campionatore consente di estrarre informazione per una banda di circa 2.4 MHz
- In buona parte dei modelli la f_c va da ≈ 24 MHz a 1.7+ GHz
 - Alcuni modelli funzionano bene anche off-spec e consentono di ricevere fino a 50 kHz

Software disponibile

gqrx

- gqrx è un plotter per t.d.F. + waterfall con integrato demodulatore
- buon punto d' inizio, fire-and-forget, consente di salvare dati grezzi ed estratti

gnuradio

- Banco di strumenti di signal processing
- Interfaccia a blocchi a-la simulink
- Richiede un po' di background di DSP

Aspetti legati alla sicurezza AFT!

Trasmissioni in chiaro

- Alcuni sistemi si basano sulla “speranza che nessuno ascolti”
 - oh well...
- Se tra due conduttori c'è una d.d.p. variabile, questi “trasmettono” la variazione
 - non è detto che io voglia trasmettere quel segnale :P
- Cosa succede se illumino con un' onda EM dei conduttori con piccole d.d.p.?
 - succede che le variazioni si “modulano” sulla mia onda :)

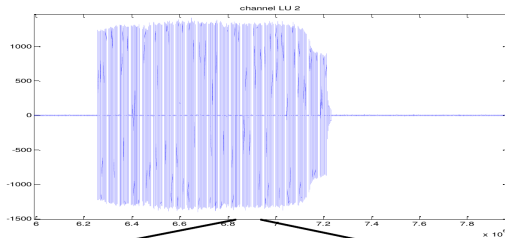
Segreti al vento

Apricancello e campanelli

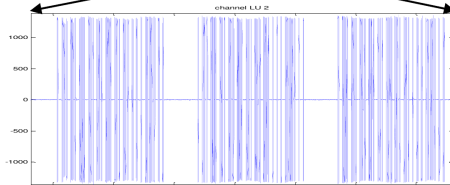
- Non è insolito per (vecchi) apricancello e campanelli trasmettere in ASK una sequenza presunta segreta
- La porta si apre/suona il campanello se la sequenza è corretta
- Es.: <http://tiny.cc/alt36y>, <http://tiny.cc/nmt36y>



Risultato?



The entire transmission. 21 packets are observable, and its length is about 1MSamples, which means its of the length of 1 second.



A zoom-in on 3 packets

(Tele-?)Video

Trasmissioni accidentali

- Spostare cariche in conduttori (e.g. cavo dati) genera un CM
- Non è necessariamente nostra intenzione che questo trasmetta un segnale!
 - Apparatati commerciali vengono certificati (e.g. da FCC) come non disturbanti la quiete degli apparati vicini
 - Nonostante questo, l' emissione non è nulla
- Caso emblematico: cavi video e monitor
 - I pixel sono trasmessi sequenzialmente su cavo e visualizzati in sequenza a monitor
 - L' onda emessa dal cavo/monitor dipende dai colori dei pixel!

(Tele-?)Video

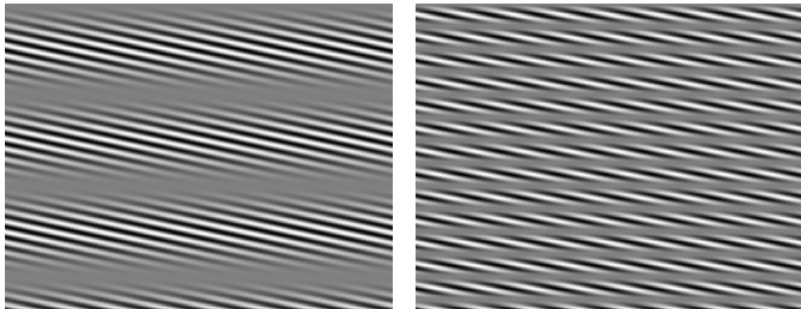


Figura: Figure che fanno trasmettere un fischio a 300 e 1200 Hz modulato su portante a 1 MHz se visualizzate su un monitor 1280x1024@ 85Hz

Funziona su LCD?

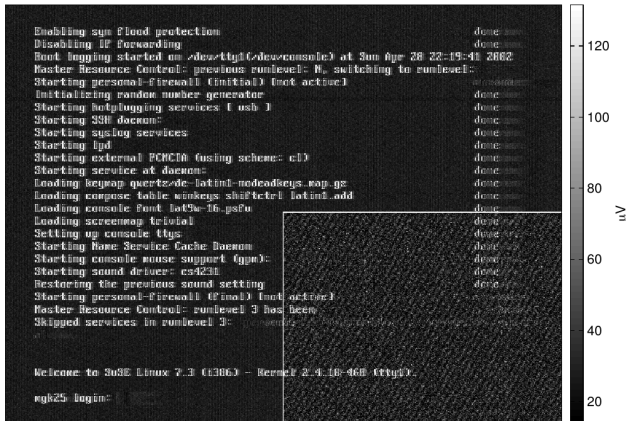


Figura: Ricezione a 3m di distanza delle emissioni di un Toshiba 440CDX post boot. Causa delle emissioni: 30cm di cavo da video a scheda madre

The quick brown fox jumps over the lazy dog
It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries.

However, interference is not the only problem caused by electromagnetic radiation. It is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in the case of digital equipment this possibility constitutes a problem, because remote reconstruction of signals inside the equipment may enable reconstruction of the data the equipment is processing.

This problem is not a new one; defence specialists have been aware of it for over twenty years. Information on the way in which this kind of "eavesdropping" can be prevented is not freely available. Equipment designed to protect military information will probably be three or four times more expensive than the equipment likely to be used for processing of non-military information.

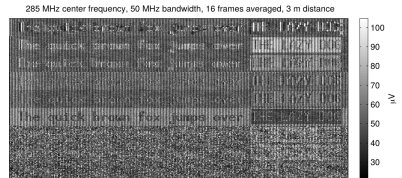
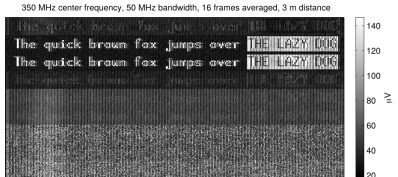
Excerpt from Rix van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286. I
!P!111! (0)++.../0123456789:;<?@AB CDEFGHIJKL MNOPQRST UVWXYZV1" 2
"abcdefghijklmnopqrstuvwxyz{|}~!"P!111! (0)++.../0123456789:;<?@
AB CDEFGHIJKL MNOPQRST UVWXYZV1" "abcdefghijklmnopqrstuvwxyz{|}~!"
vsnack.txt lines 1-26/26 (END)

Figura: Stesso hardware, ricezione attraverso 3 pareti di cartongesso, 10m

Contromisure? Cambiare i colori ai font :)

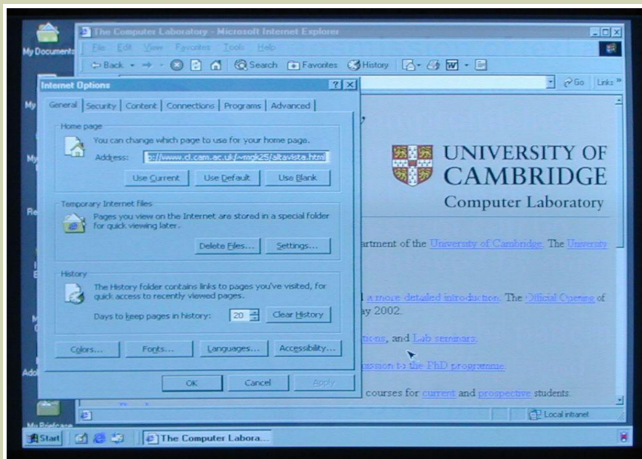
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG
The quick brown fox jumps over	THE LAZY DOG

A video ↑
Ricevuto →



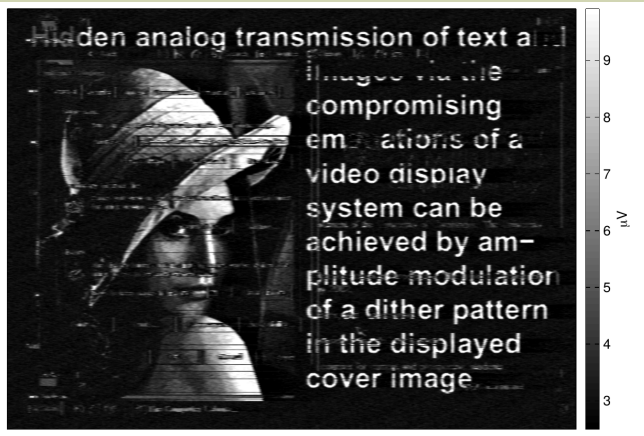
Covert² Channels

Cosa viene ricevuto quando visualizzo questo?



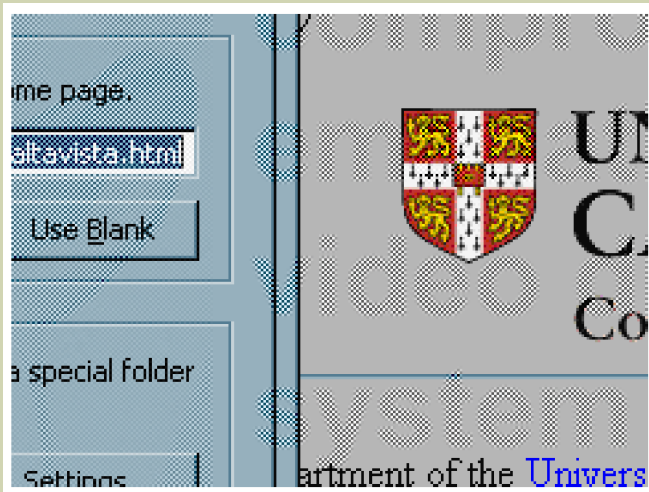
Covert² Channels

Questo!



Covert² Channels

Modulazione AM, con creatività



Analisi di consumo

RSA - Square and Multiply

```
s = m;  
for (i =  $\lceil \log_2(d) \rceil - 1; i \geq 0; i \leftarrow i - 1$ ) do  
    s = s2;  
    if di-1 == 1 then  
        s = s * m;  
    end  
end
```

- Calcolo di $m^d \bmod n$
- La moltiplicazione in rosso viene eseguita solo se l' i -esimo bit di chiave è a 1 $\rightarrow$ diversi consumi $\rightarrow$ diverse emissioni EM

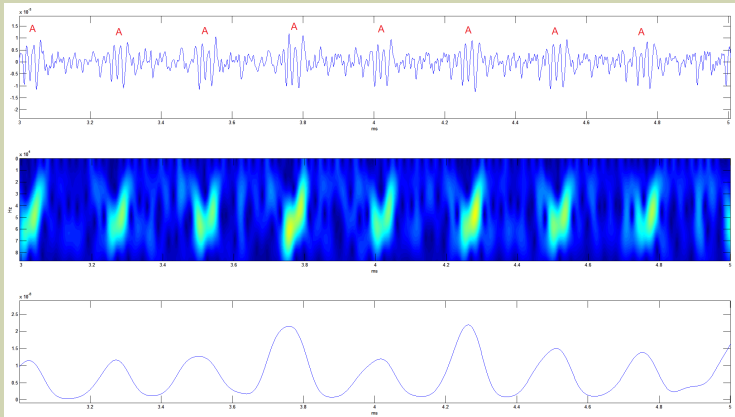
Analisi di consumo

Setup economico per misure



Analisi di consumo

Risultati



Extra Sources

Link utili

- Signal identification wiki
<https://www.sigidwiki.com/wiki/Category:HF>
- Tesi di PhD di Markus Kuhn: <https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf>
- Analisi EM di RSA :
<https://www.cs.tau.ac.il/%7Etromer/mobilesc/>
- *Trasmettitore* SDR:
<https://osmocom.org/projects/osmo-fl2k/wiki>

Credits

- Voci di Wikipedia riguardanti gli argomenti
- <https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/>
- <http://tiny.cc/1qt36y>