ECS455: Chapter 4

Multiple Access

4.3 DS/SS

spread spectrum (SS)

FH/SS

Dr.Prapun Suksompong

prapun.com/ecs455

Office Hours:

BKD, 6th floor of Sirindhralai building

Tuesday	**14:20-15:20**
Wednesday	**14:20-15:20**
Friday	**9:15-10:15**

Spread spectrum (SS)

- Historically spread spectrum was developed for *secure* communication and *military* uses.
- **Difficult to intercept** for an unauthorized person.
- Easily **hidden**.
  - Can even hide below the noise floor during transmission
  - For an unauthorized person, it is **difficult to even detect their presence** in many cases.
- **Resistant to** narrowband **jamming** and interference.

[Goldsmith, 2005, Ch 13]

Spread spectrum (SS)

- Provide a measure of immunity to distortion due to multipath propagation.
  - In conjunction with a RAKE receiver, can provide coherent combining of different multipath components.
- Asynchronous multiple-access capability.
- Wide bandwidth of spread spectrum signals is useful for location and timing acquisition.
- Applications
  - **Cordless phones**.
  - The basis for both 2nd and 3rd generation **cellular systems** as well as 2nd generation wireless LANs (**WLAN**).

[Goldsmith, 2005, Ch 13]

Spread spectrum: Definition

Def:

Spread spectrum refers to any system that satisfies the following conditions [Lathi, 1998, p 406 & Goldsmith, 2005, p. 378]:

① BW expansion

1. The spread spectrum may be viewed as a kind of modulation scheme in which **the modulated (spread spectrum) signal bandwidth is much greater than the message (baseband) signal bandwidth.**

② code and message are independent

2. The **spectral spreading** is performed by a **code** that is **independent** of the message signal. ← Unlike FM, where the spectrum is also spread but by the message itself.
   - This same code is also used at the receiver to despread the received signal in order to recover the message signal (from the spread spectrum signal).
   - In secure communication, this code is known only to the person(s) for whom the message is intended.

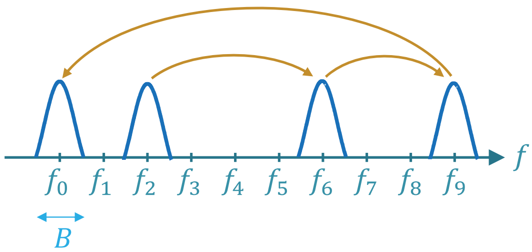
[R. Pickholtz, D. Schilling, L. Milstein, "Theory of Spread-Spectrum Communications - A Tutorial," IEEE Trans. Commun., Vol. 30 , pp. 855-884, May 1982.]

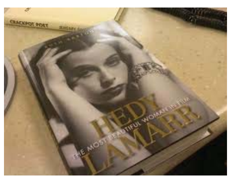
SS: Processing Gain and BW Sharing

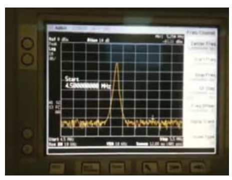
- Increase the bandwidth of the message signal by a factor **N**, called the **processing gain** (or bandwidth **spreading factor**).
  - In practice, N is on the order of **100-1000**. [Goldsmith, 2005, p 379]
    - $N = 128$ for IS-95 [T&V]
  - Wasteful? No
- **Bandwidth Sharing**: Although we use much higher BW for a spread spectrum signal,
  - **Multiplexing**: we can also multiplex large numbers of such signals over the same band.
  - **Multiple Access**: many users can share the same spread spectrum bandwidth without interfering with one another.
    - Achieved by assigning different code to each user.
    - Frequency bands can be reused without regard to the separation distance of the users.

Two forms of spread spectrum

1. **Frequency Hopping** (FH)
   - Hop the modulated data signal over a wide BW by changing its carrier frequency
   - BW is approximately equal to NB
     - N is the number of carrier frequencies available for hopping
     - B is the bandwidth of the data signal.
   - The most celebrated invention of frequency hopping was that of actress **Hedy Lamarr** and composer George Antheil in 1942







2. **Direct Sequence** (DS)

Hedy Lamarr

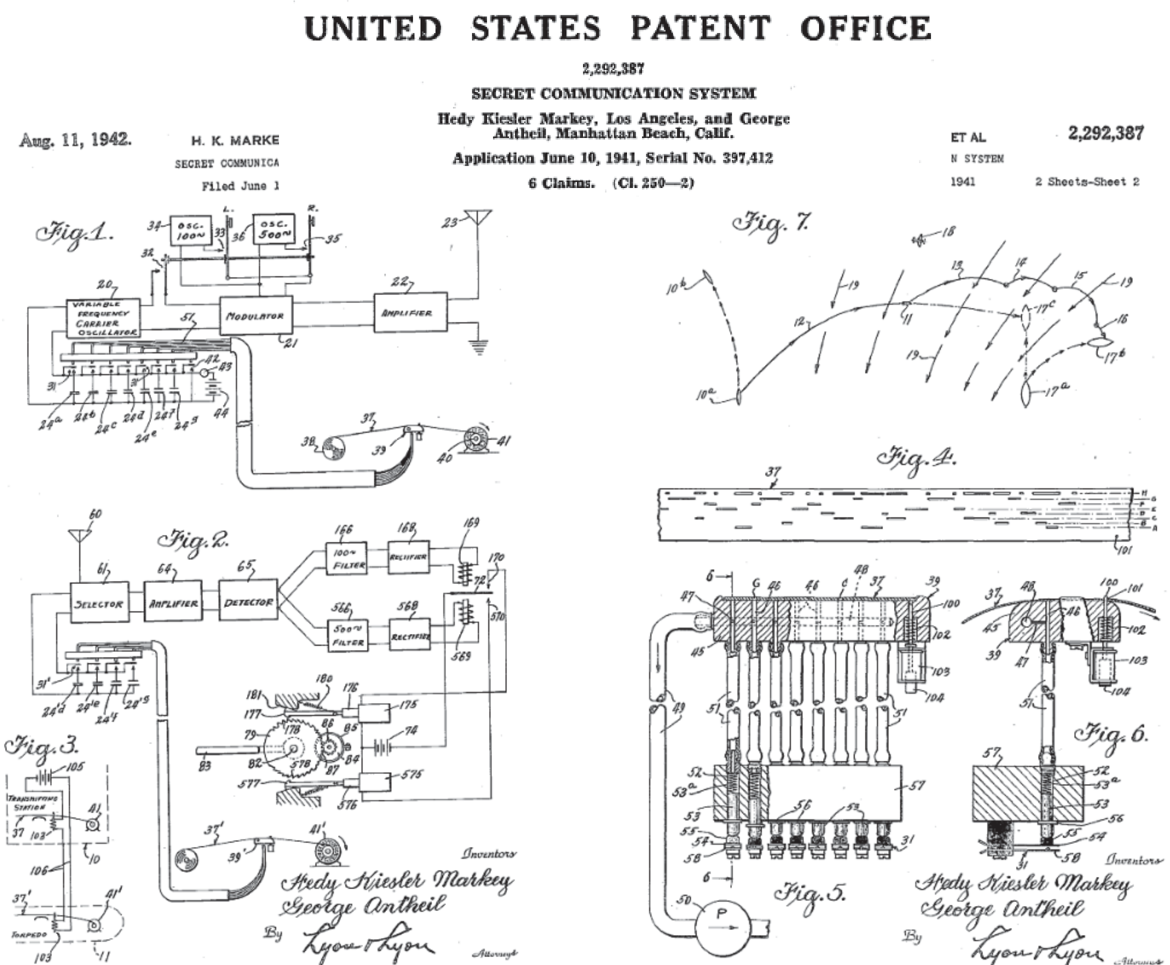
- In 2015, Google honoured Hedy Lamarr with a Google Doodle on her 101st birthday.

[https://www.google.com/doodles/hedy-lamarrs-101st-birthday]

Hedy Lamarr

[http://www.smh.com.au/technology/sci-tech/google-honours-hedy-lamarr-inventor-of-technology-behind-wifi-and-bluetooth-20151109-gku3w8.html]

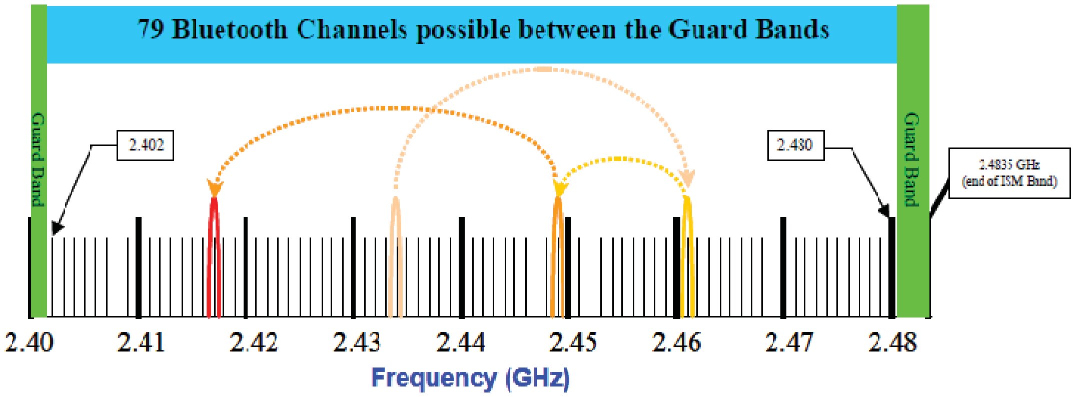
Hedy Lamarr



[http://www.google.com/patents?vid=USPAT2292387]

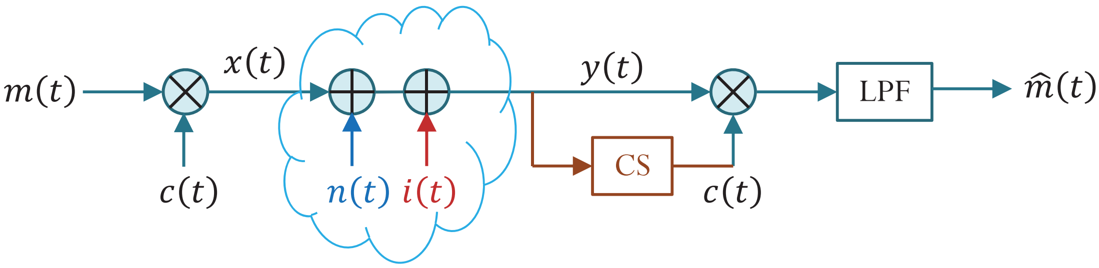
FHSS Example: Bluetooth

- The band at 2.4 GHz is divided into 79 channels.
- A Bluetooth device, hops frequency at a rate of 1600 hops per second, randomly selecting a channel of 1 MHz to operate.

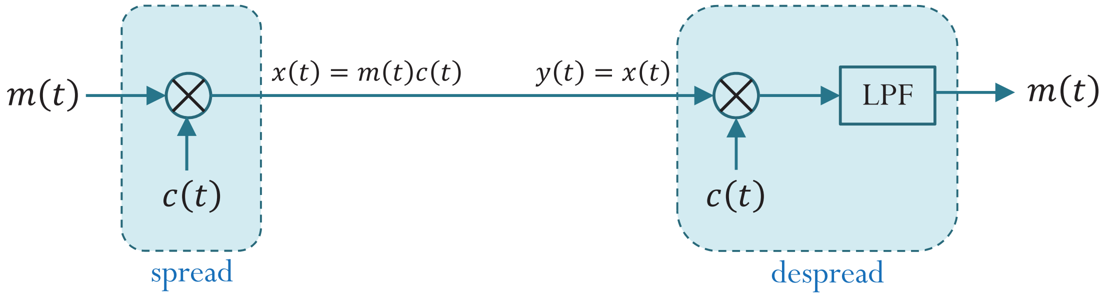


[https://sites.google.com/site/nearcommunications/adaptative-frequency-hopping]

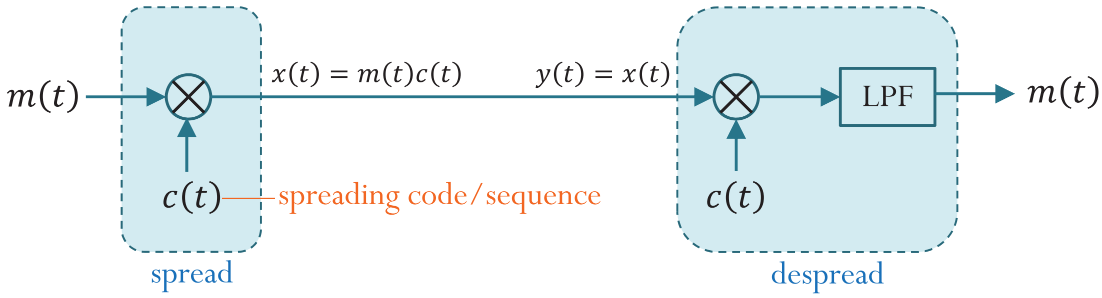
DS/SS System



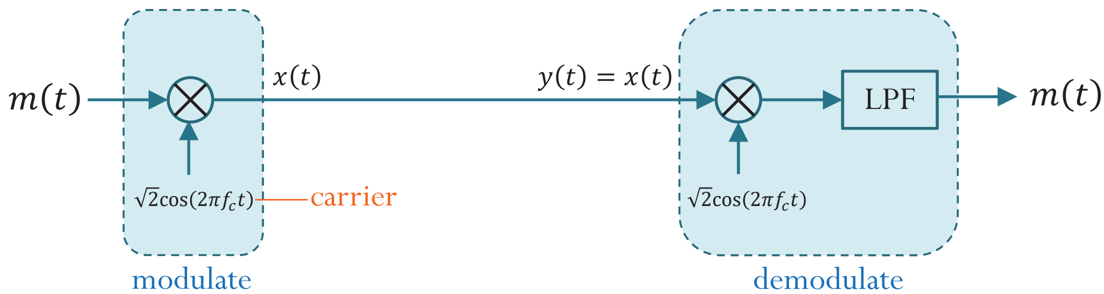
DS/SS System: The Basic



DS/SS System: The Basic



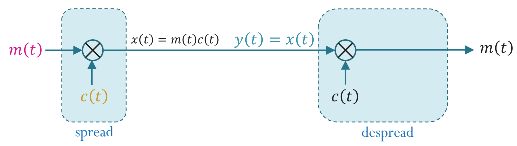
Compare with ECS332's modulation:



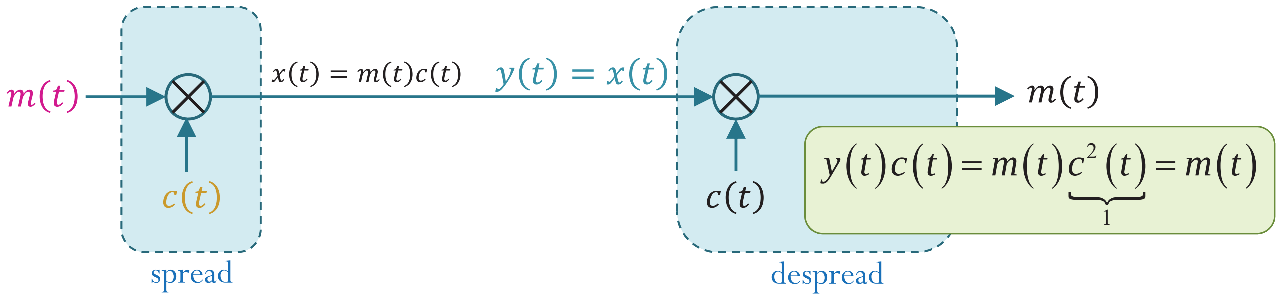
DS/SS System (Con't)

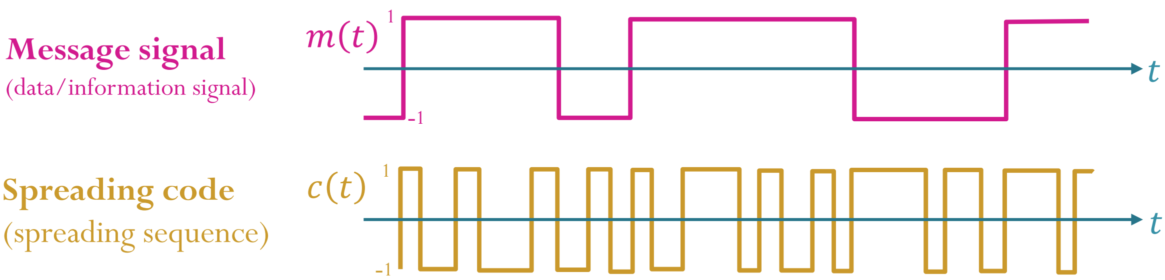
Observe that…

- To be able to perform the despreading operation, the receiver must
  - **know** the **code** sequence $c(t)$ used at the Tx to spread the signal
  - **synchronize** the codes of the received signal and the locally generated code.
- The process of detection (despreading) is **identical** to the process of spectral spreading.
  - Recall that for DSB-SC, we have a similar situation in that the modulation and demodulation processes are identical (except for the output filter).



DS/SS System: Signals

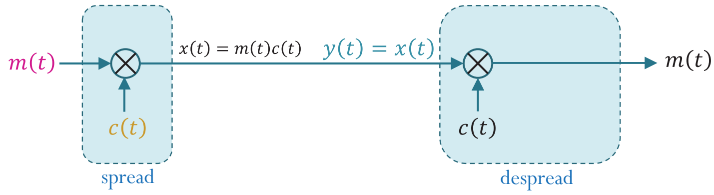


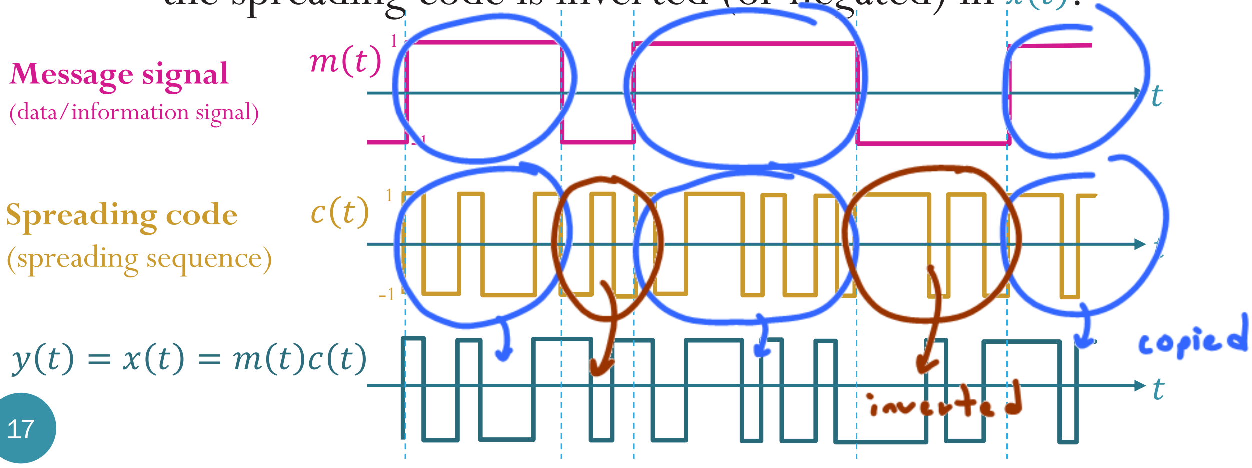


- We assume polar signals.
  - In particular, we assume $c^2(t) = 1$.

DS/SS System: Signals

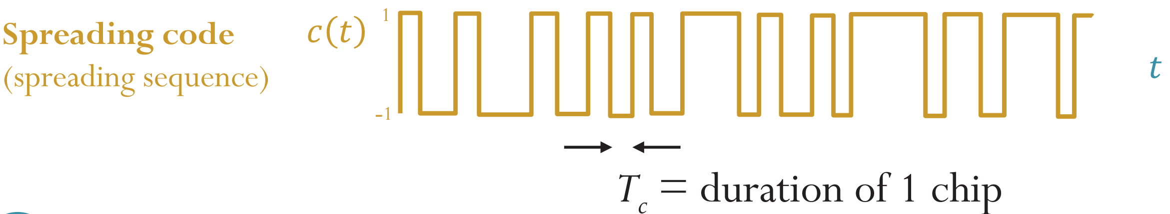
- During the time that $m(t) = 1$, the spreading code is non-inverted in $x(t)$.
- During the time that $m(t) = -1$, the spreading code is inverted (or negated) in $x(t)$.





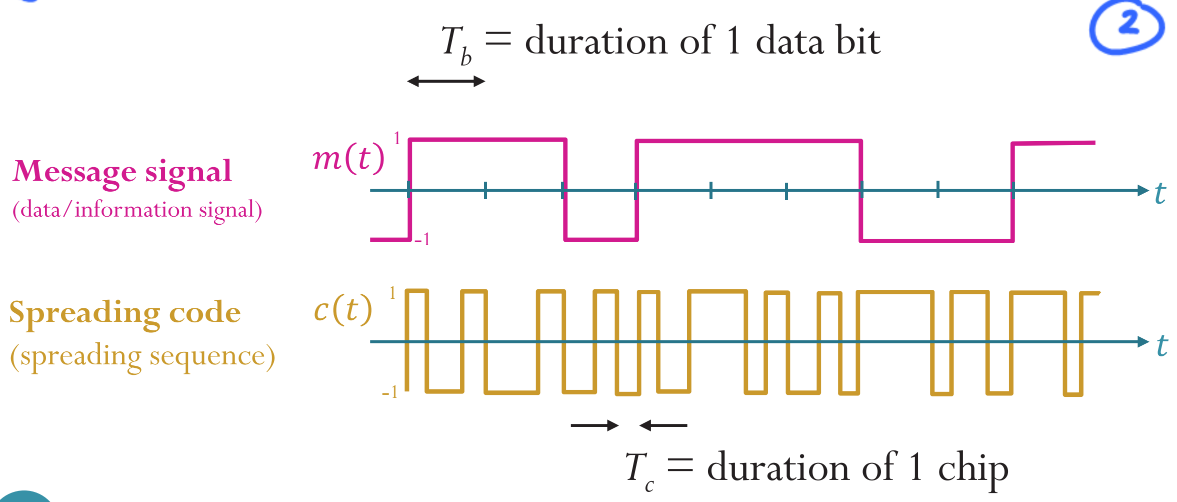
DS/SS: Spectral Spreading Signal $c(t)$

- The spreading code $c(t)$ is design to be **pseudorandom**
  - **Appear** to be **unpredictable**
  - Can be generated by **deterministic** recipe (hence, pseudorandom)
    - This will be studied in the next section.
- Each rectangular pulse in $c(t)$ is called a **chip**.
- The bit rate of $c(t)$ is then known as the **chip rate**.



DS/SS System: Signals

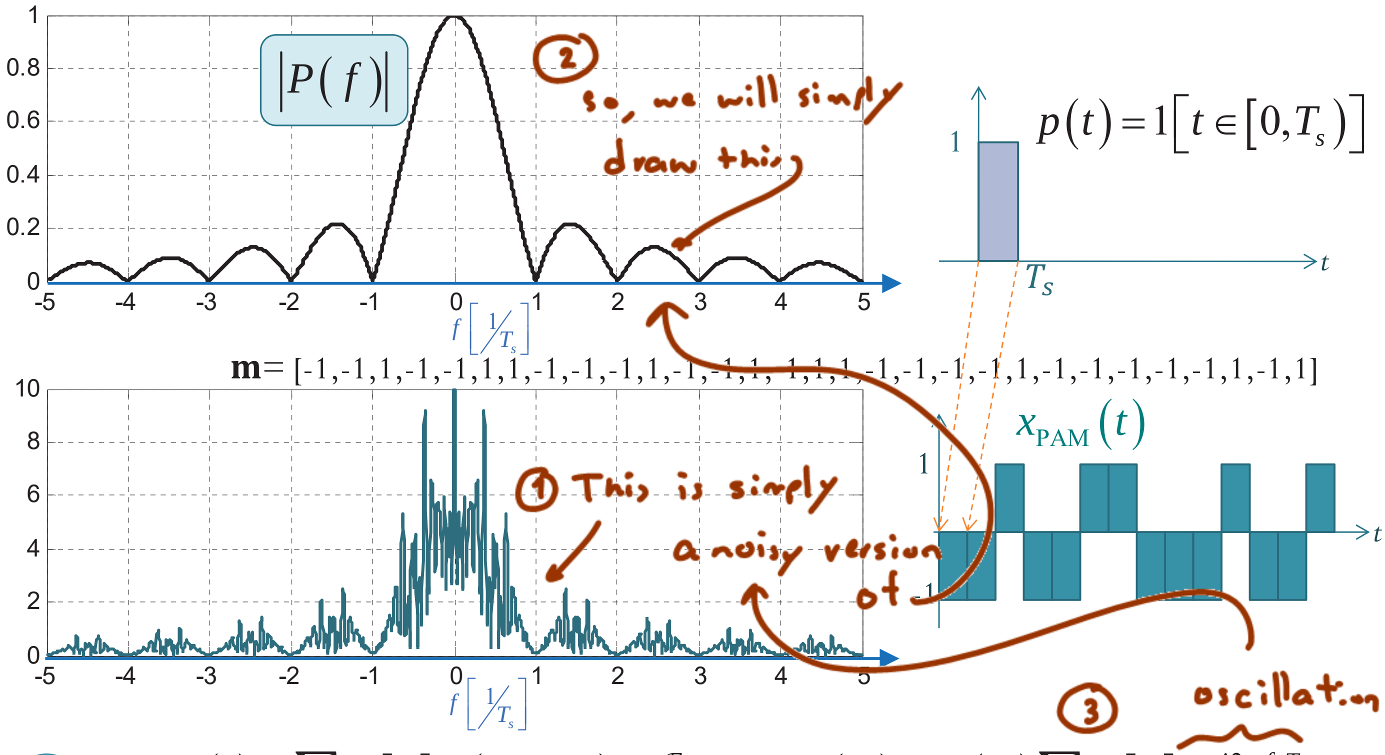
- The bit rate of $c(t)$ is chosen to be much higher then the bit rate of $m(t)$.
- In fact, by definition, the spreading factor $N = \frac{T_b}{T_c}$.



ECS332 2016 ch. 7 Lect F.53 p.117

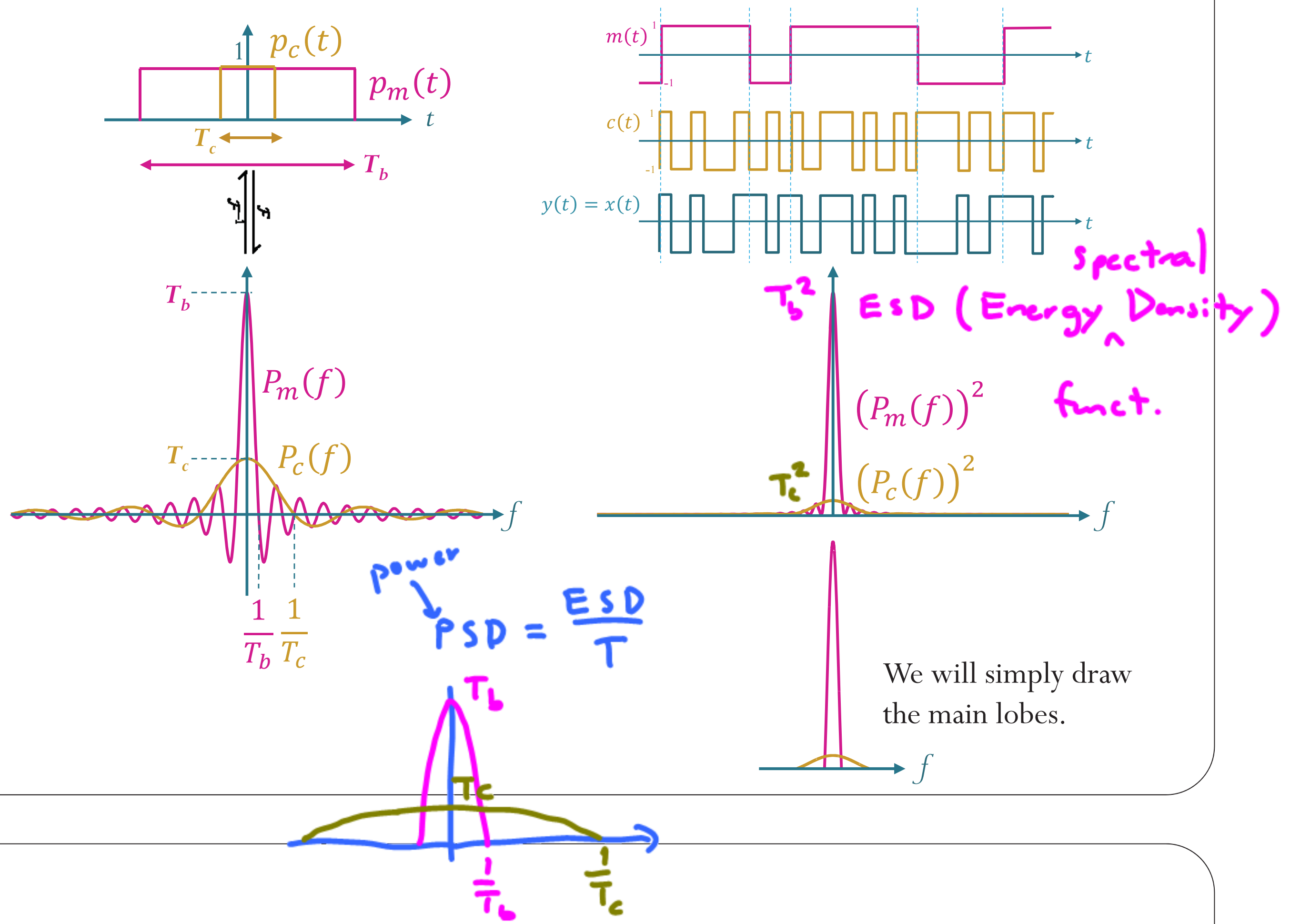
2015 ch. 6 slides p. 89-94 → Exam 2 : Q11

Review: Spectrum of PAM signal



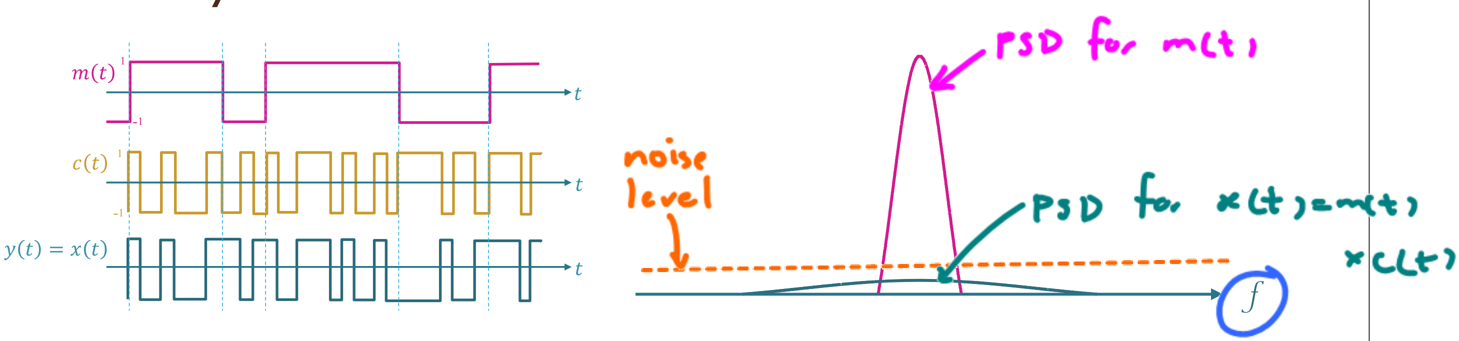
$$x_{\text{PAM}}(t)=\sum_n m[n]\,p(t-nT_s)\xrightarrow{\mathcal{F}}X_{\text{PAM}}(f)=P(f)\sum_n m[n]\,e^{-j2\pi f n T_s}$$

Frequency-Domain Analysis



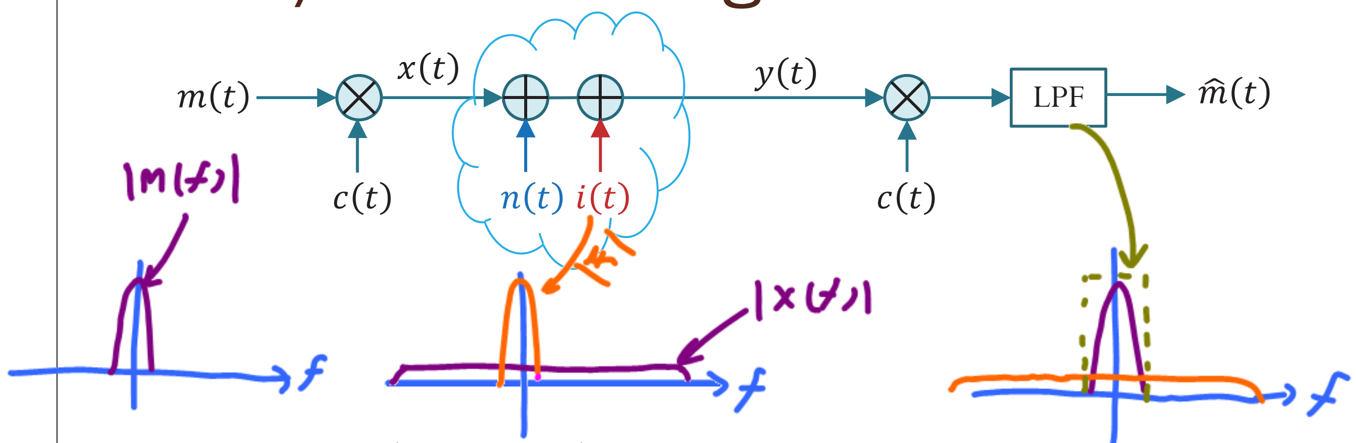
We will simply draw the main lobes.

DS/SS: Secure Communication



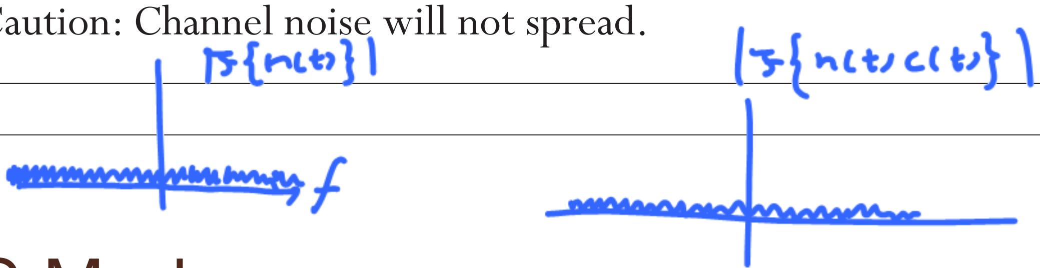
- As N increases, the peak of $X(f)$ is reduced.
- Secure communication
  - Signal can be detected only by **authorized** person(s) who **know** the pseudorandom code used at the transmitter.
  - Signal spectrum is spread over a very wide band, the signal's **spectral level is very small**, which makes it easier to hide the signal within the noise floor

DS/SS: Jamming Resistance

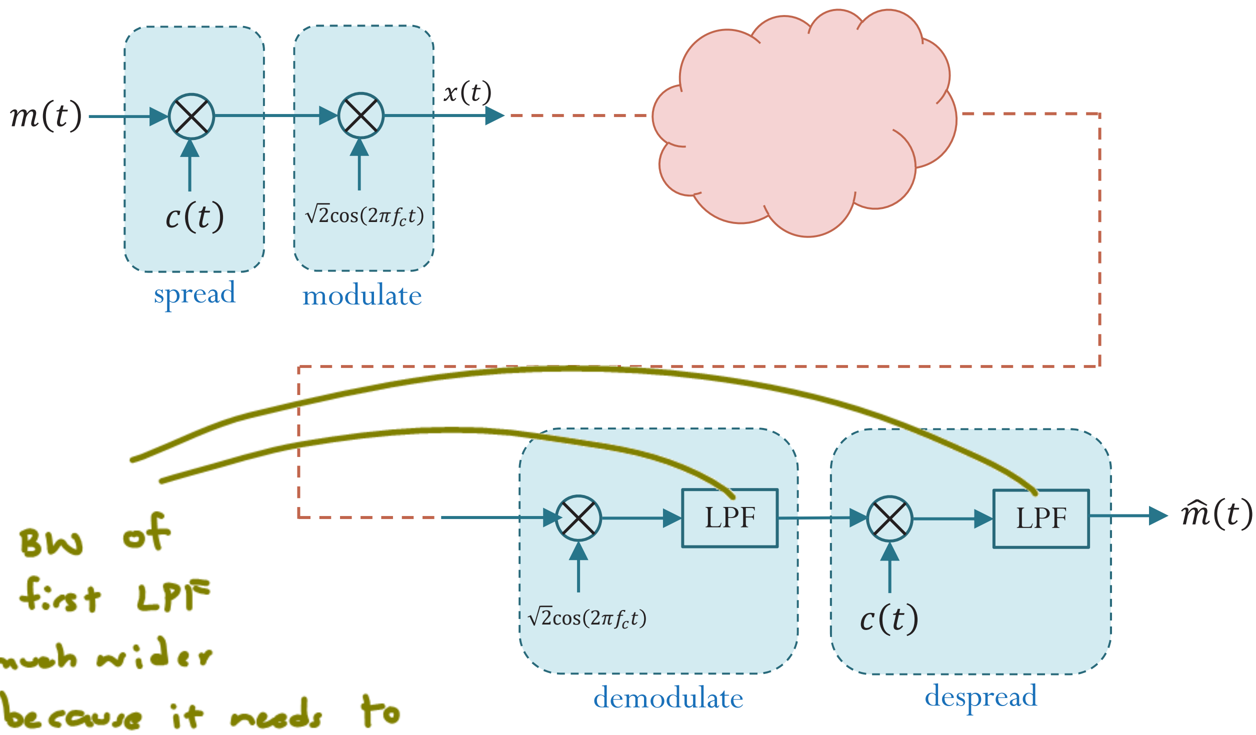


$$y(t)c(t)=\big(x(t)+i(t)\big)c(t)=m(t)c^2(t)+i(t)c(t)=m(t)+i(t)c(t)$$

- Jamming Resistance / Narrowband Interference rejection
  - The decoder despreads the signal $y(t)$ to yield $m(t)$.
  - The jamming signal $i(t)$ is spread to yield $i(t)c(t)$.
  - Using a LPF, we can recover $m(t)$ with only a small fraction of the power from $i(t)$.
- Caution: Channel noise will not spread.



SS Modem



The BW of the first LPF is much wider because it needs to pass the whole spread signal