ECS455: Chapter 4

Multiple Access

4.4 DS/SS

Dr.Prapun Suksompong
prapun.com/ecs455

Office Hours:
BKD 3601-7
Monday 9:20-10:20
Wednesday 9:20-10:20

Spread spectrum (SS)

- Historically spread spectrum was developed for *secure* communication and *military* uses.
- **Difficult to intercept** for an unauthorized person.
- Easily **hidden**. For an unauthorized person, it is difficult to even detect their presence in many cases.
- **Resistant to jamming**.
- 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.

[Goldsmith, 2005, Ch 13]

Spread spectrum: Applications

- First achieve widespread use in **military** applications due to
  - its inherent property of *hiding the spread signal below the noise floor* during transmission,
  - its resistance to narrowband jamming and interference, and
  - its low probability of detection and interception.
- The narrowband interference resistance has made spread spectrum common in **cordless phones**.
- The basis for both 2nd and 3rd generation **cellular systems** as well as 2nd generation wireless LANs (**WLAN**).
  - The ISI rejection and bandwidth sharing capabilities of spread spectrum are very desirable in these systems

[Goldsmith, 2005, Ch 13]

Definition:

Spread spectrum conditions

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

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.**

BW expansion

2. The **spectral spreading** is performed by a **code** that is **independent** of the message signal.

c(t)

code and message are independent

- 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.]

Spread spectrum (2)

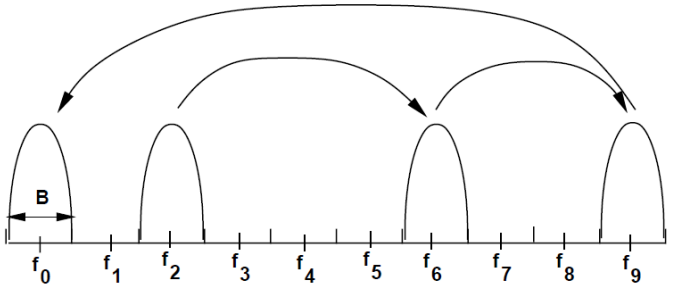
- Increase the bandwidth of the message signal by a factor **N**, called the **processing gain** (or bandwidth spreading factor).
  - In practice, *N* is on the order of **100-1000**. [Goldsmith, 2005, p 379]
    - N = 128 for IS-95 [T&V]
  - Wasteful?
- Although we use much higher BW for a spread spectrum 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.

Spread Spectrum (3)

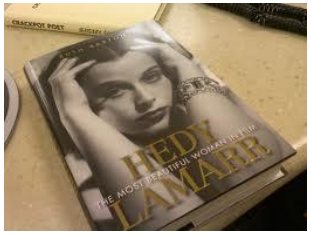
Two forms of spread spectrum (SS)

1. **Frequency Hopping** (FH) FH/SS

   - 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) DS/SS

UNITED STATES PATENT OFFICE

2,292,387

SECRET COMMUNICATION SYSTEM

Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.

Application June 10, 1941, Serial No. 397,412

6 Claims. (Cl. 250—2)

Aug. 11, 1942. H. K. MARKE ET AL 2,292,387

SECRET COMMUNICA N SYSTEM

Filed June 1 1941 2 Sheets-Sheet 2

Fig. 1.

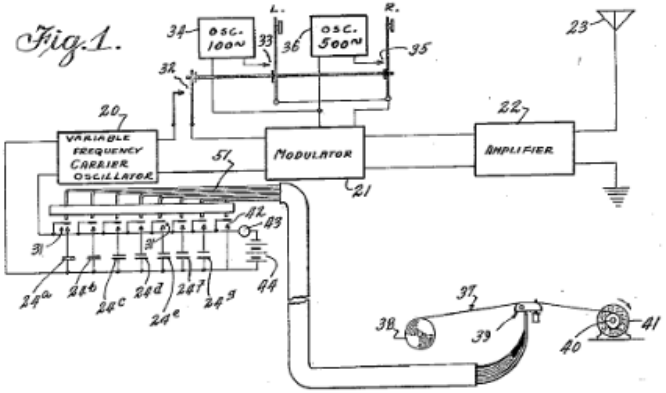


Fig. 2.

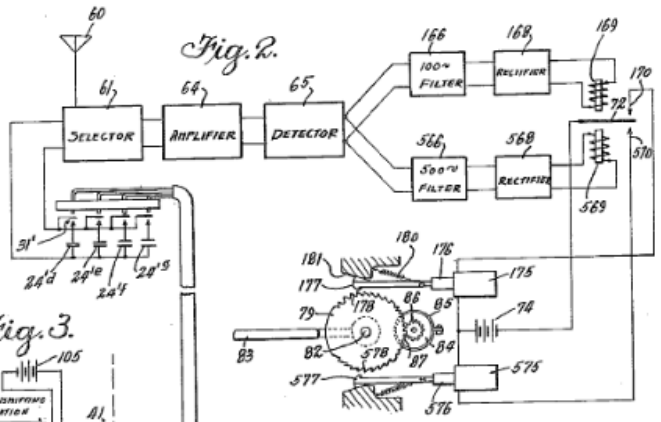


Fig. 3.

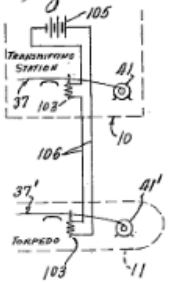


Fig. 7.

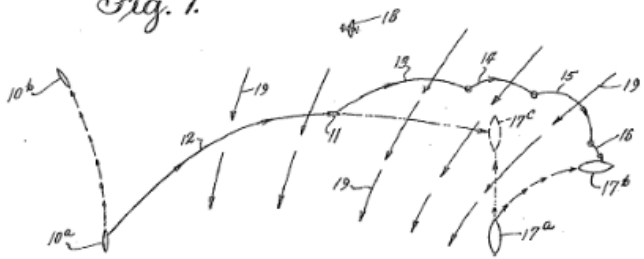
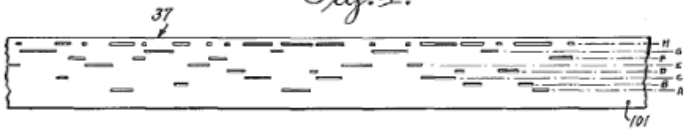


Fig. 4.



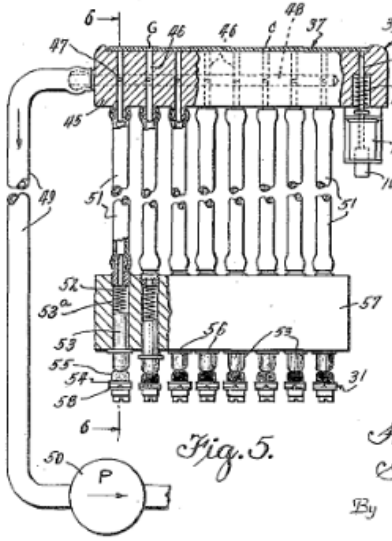


Fig. 5.

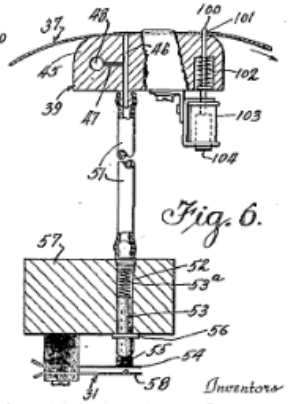
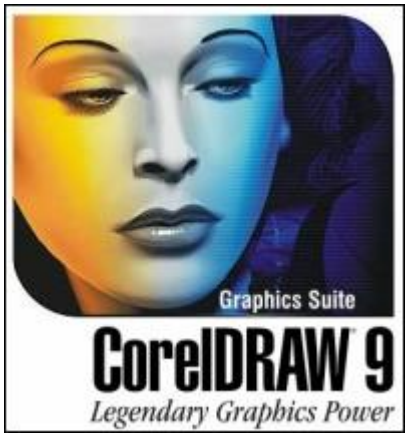


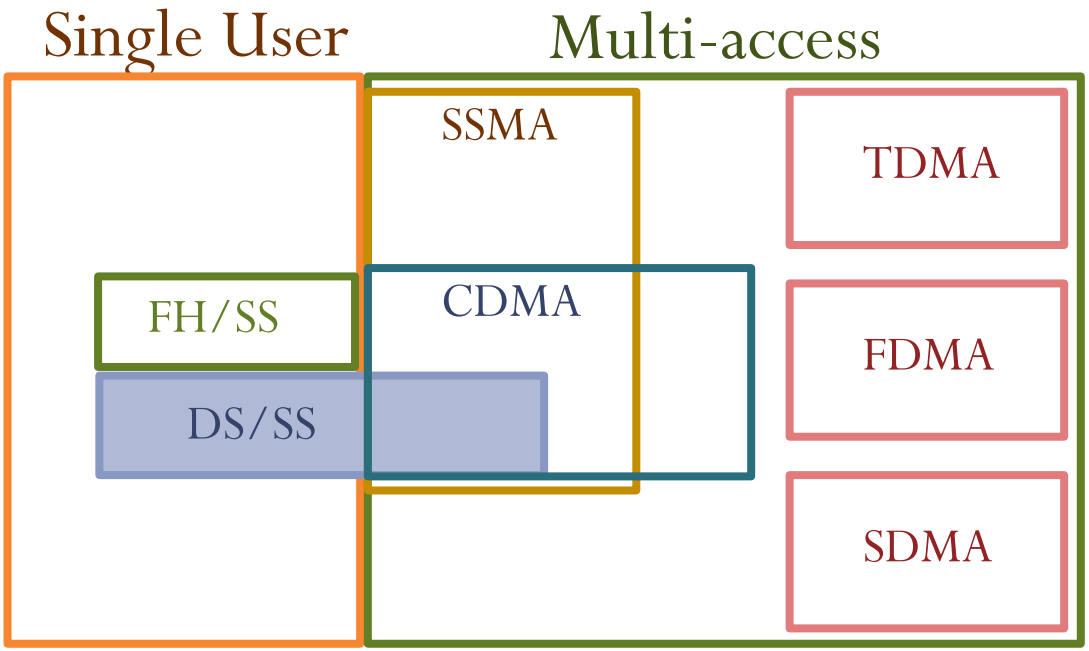
Fig. 6.

Inventors
Hedy Kiesler Markey
George Antheil
By Lyon & Lyon
Attorneys

For several years beginning in 1997, the boxes of CorelDRAW's software suites were graced by a large Corel-drawn image of Hedy Lamarr.

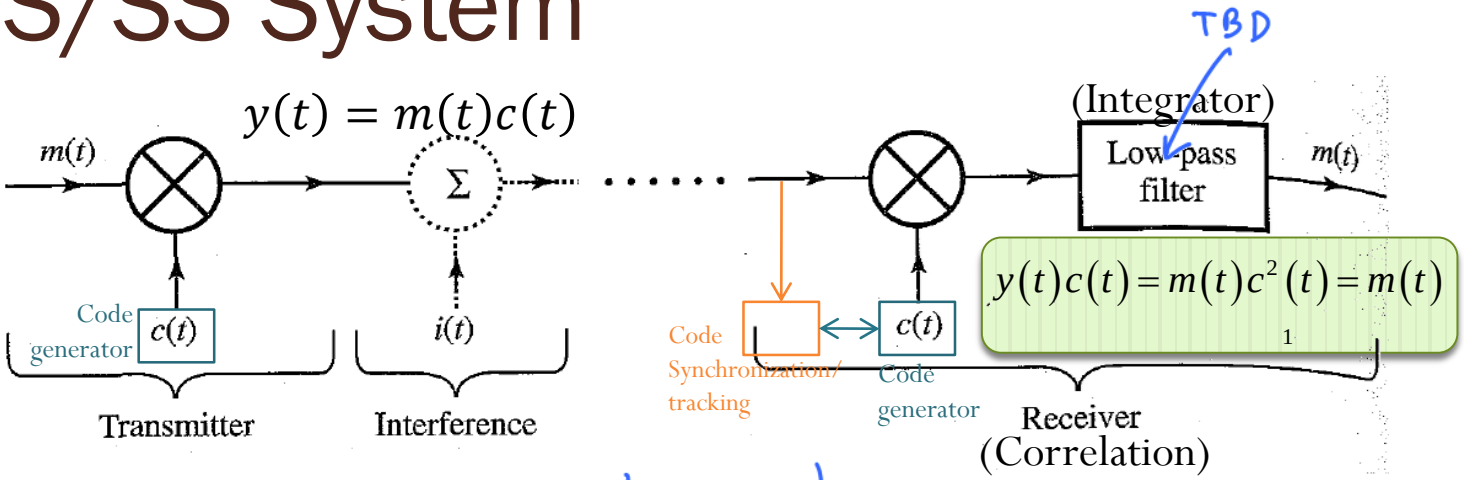


SSMA, CDMA, DS/SS

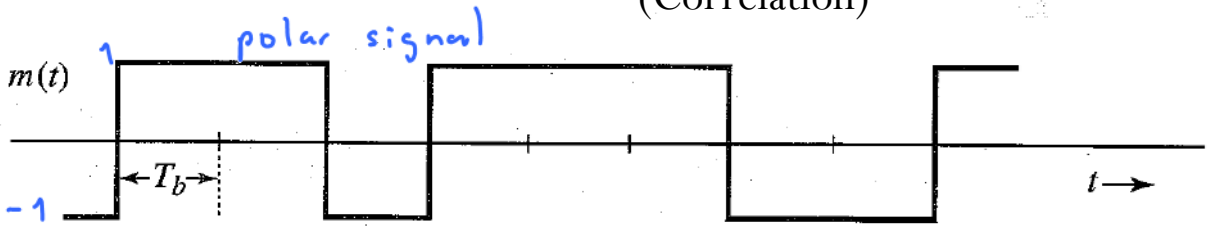


Useful even for single user!

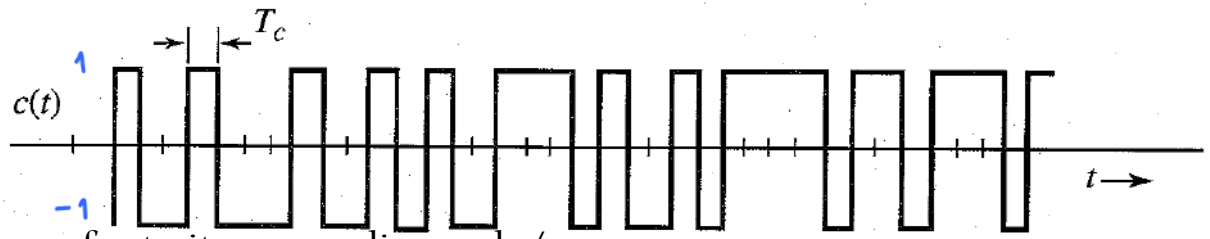
DS/SS System



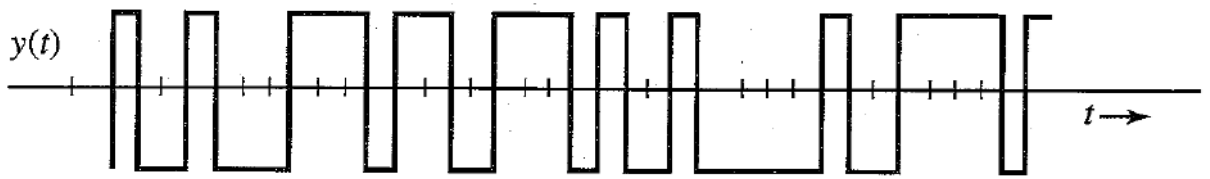
Message signal
(data/information signal)



Pseudonoise (PN) sequence. (Think of this as a pseudorandom carrier).



Here, we refer to it as spreading code/sequence.



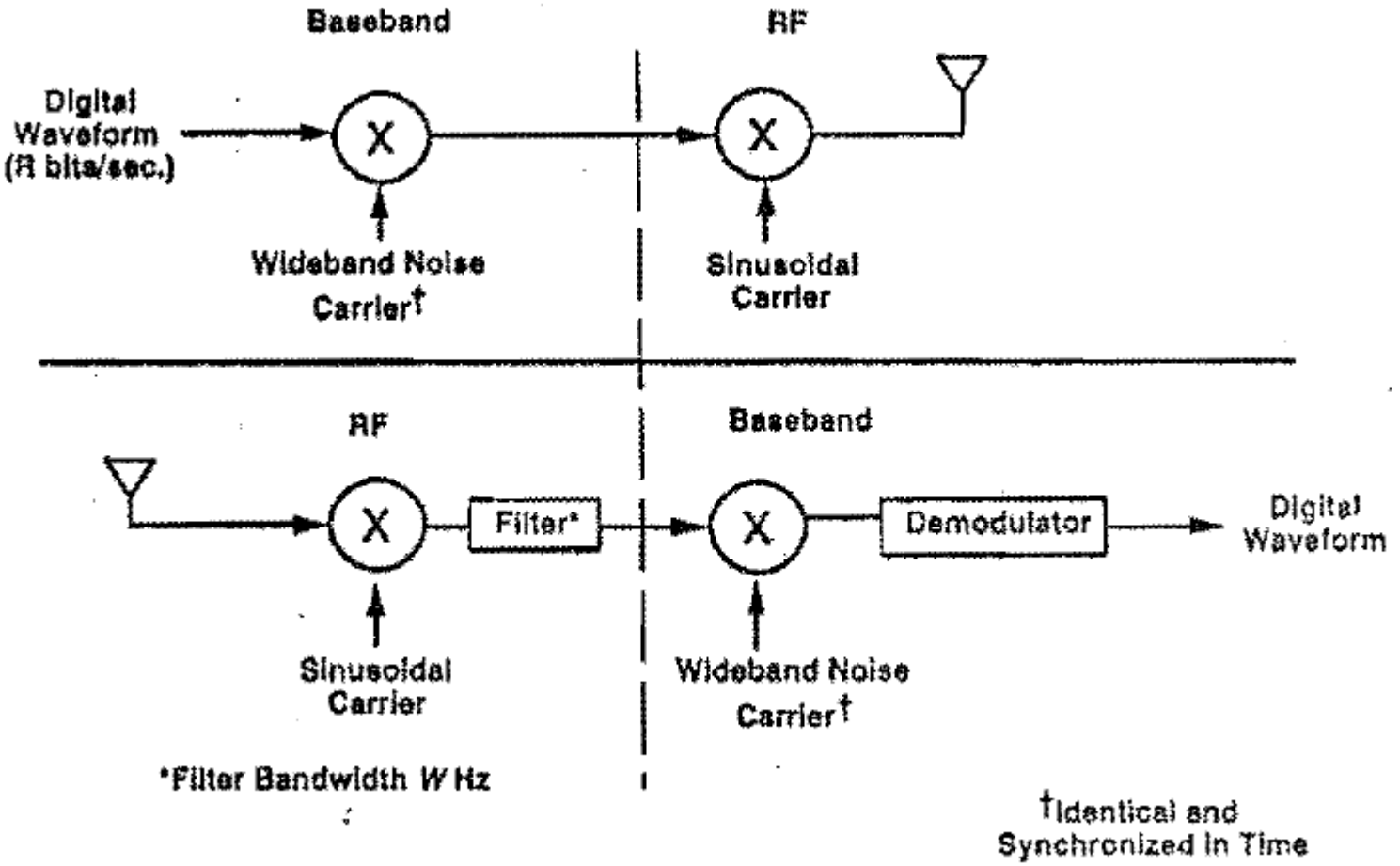
$$N = \frac{T_b}{T_c}$$

DS/SS System (Con't)

Observe that…

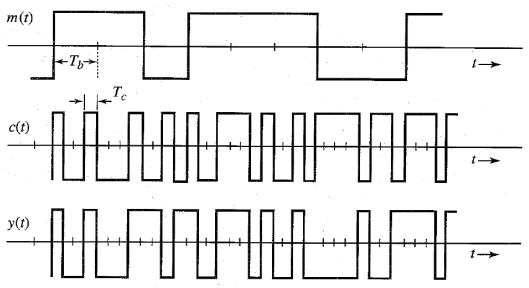
- To be able to perform the despreading operation, the receiver must
  - **know** the **code** sequence $c(t)$ used at the Tx to spread the signal
  - **synchronize** the codes of the received signal and the locally generated code.
- The process of detection (despreading) is **identical** to the process 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).

Spread spectrum modem



[Viterbi, 1995, Fig. 1.2]

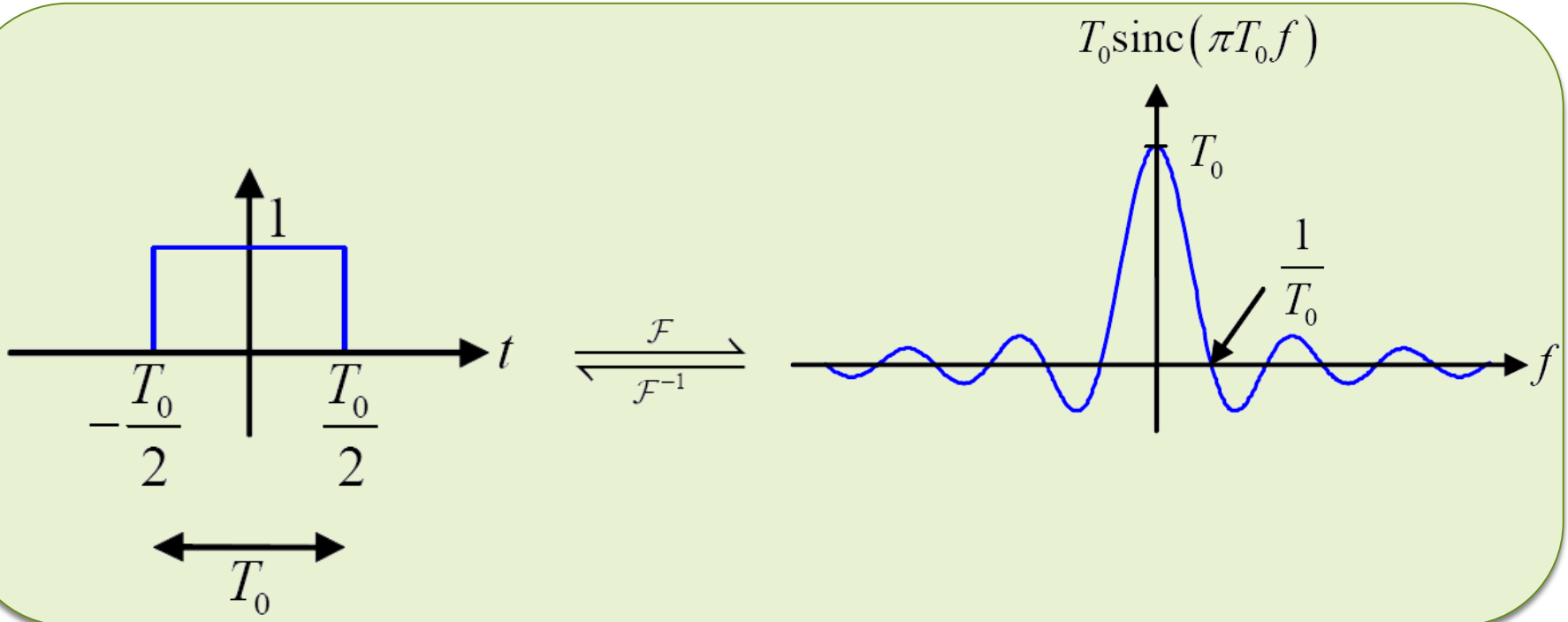
DS/SS: Spectral Spreading Signal $c(t)$



- A **pseudorandom** signal
  - **Appear** to be **unpredictable**
  - Can be generated by **deterministic** means (hence, pseudorandom)
- The bit rate is chosen to be much higher then the bit rate of $m(t)$.
- The basic pulse in $c(t)$ is called the **chip**.
- The bit rate of $c(t)$ is known as the **chip rate**.
- The autocorrelation function of $c(t)$ should be very narrow.
  - Small similarity with its delayed version
- Remark: In multiuser (CDMA) setting, the cross-correlation between any two codes $c_1(t)$ and $c_2(t)$ should also be very small
  - Negligible interference between various multiplexed signals.

TBD

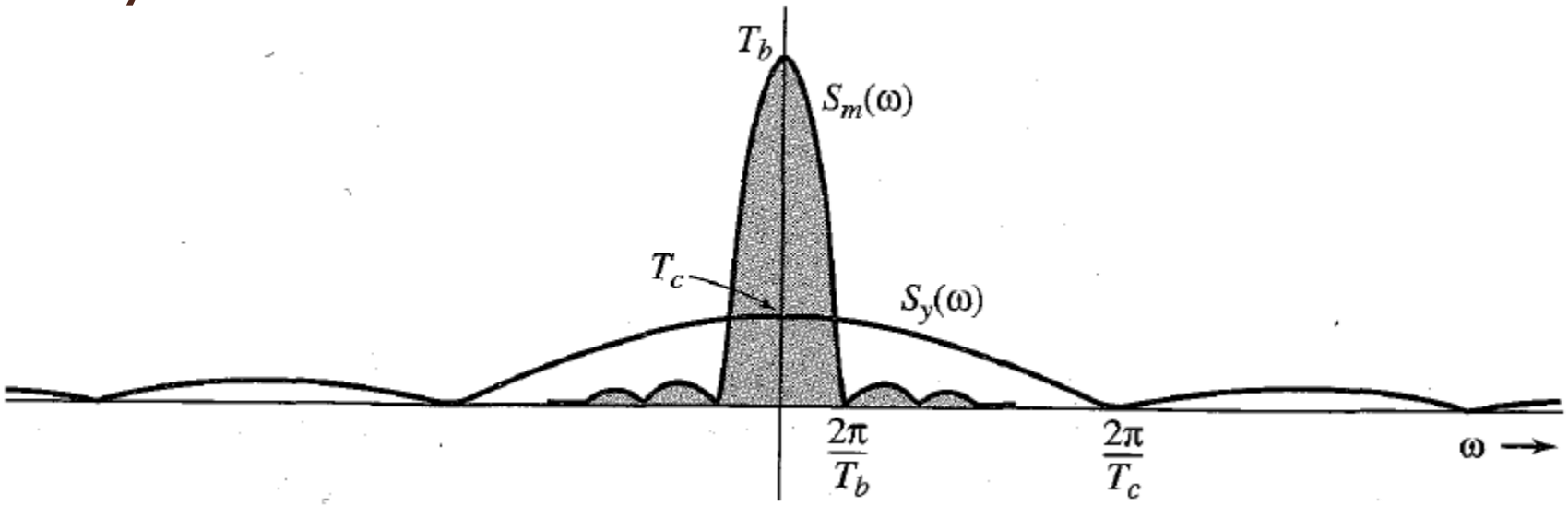
Frequency-Domain Analysis



Shifting Properties: $g(t-t_0) \overset{\mathcal{F}}{\rightleftharpoons} e^{-j2\pi f t_0} G(f)$ $\quad e^{j2\pi f_0 t} g(t) \overset{\mathcal{F}}{\rightleftharpoons} G(f-f_0)$

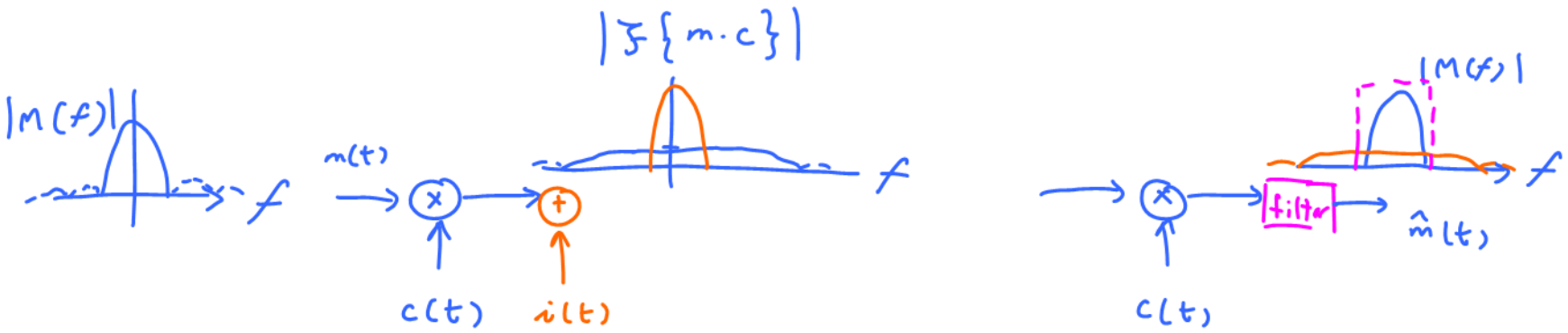
Modulation: $m(t)\cos(2\pi f_c t) \overset{\mathcal{F}}{\rightleftharpoons} \frac{1}{2}M(f-f_c)+\frac{1}{2}M(f+f_c)$

DS/SS: Secure Communication



- 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 **PSD is very small**, which makes it easier to hide the signal within the noise floor

DS/SS: Jamming Resistance



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

- 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, can recover $m(t)$ with only a small fraction of the power from $i(t)$.
- Caution: Channel noise will not spread.

DS/SS: Multipath Fading Immunity

- The signal received from any undesired path is a delayed version of the DS/SS signal.
- DS/SS signal has a property of low autocorrelation (small similarity) with its delayed version, especially if the delay is of more than one chip duration.
- The delayed signal, looking more like an interfering signal, will not be despread by $c(t)$ effectively minimizes the effect of the multipath signals.
- What is more interesting is that DS/SS cannot only mitigate but may also exploit the multipath propagation effect.
  - This is accomplished by a **rake receiver**.
  - This receive designed as to coherently combine the energy from several multipath components, which increases the received signal power and thus provides a form of diversity reception.
  - The rake receiver consists of a bank of correlation receivers, with each individual receiver correlating with a different arriving multipath component.
  - By adjusting the delays, the individual multipath components can be made to add coherently rather than destructively.