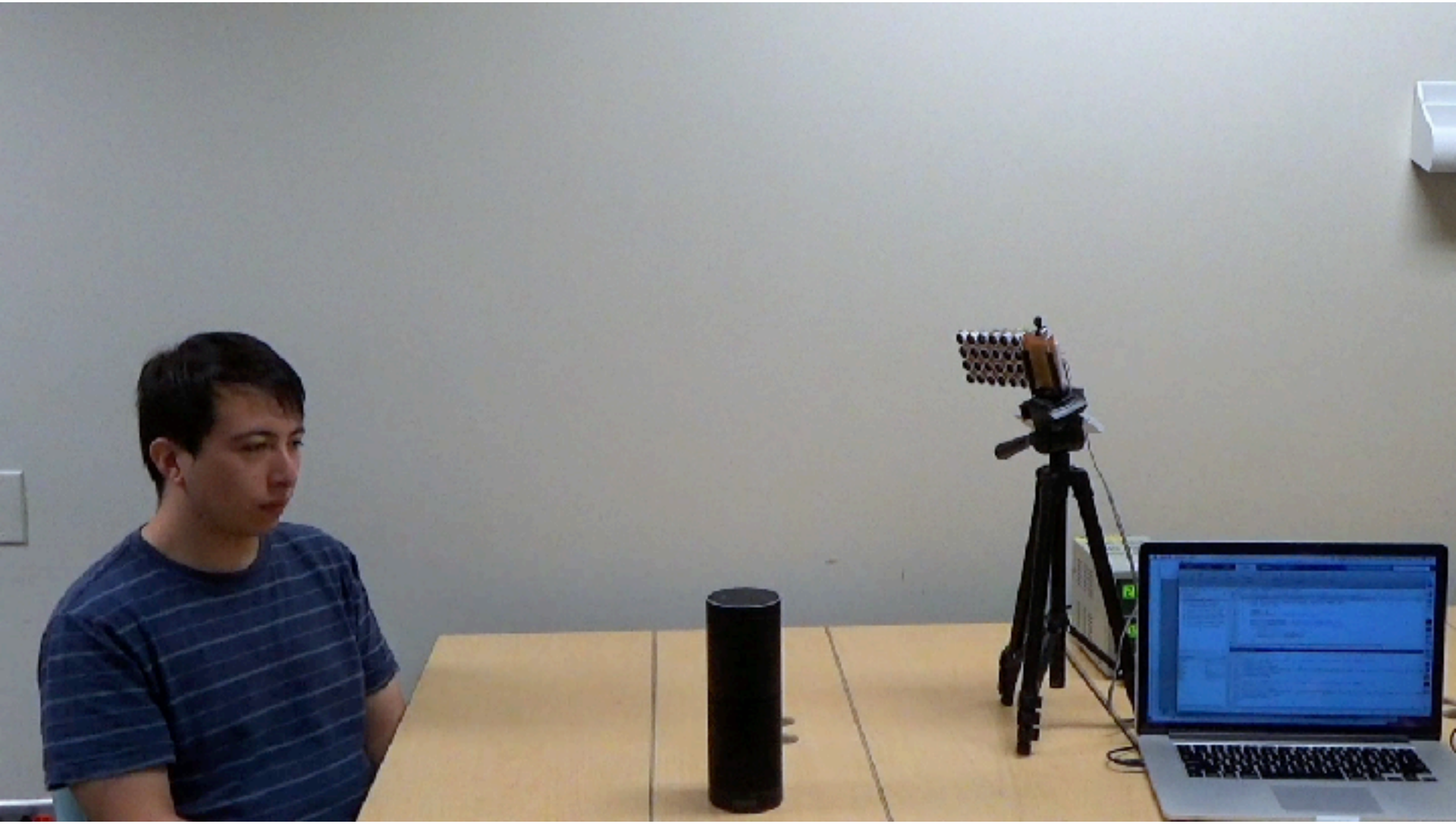
6.S062: Mobile and Sensor Computing

Lecture 14: IoT Security
Physical Security and Acoustic Attacks

Some material adapted from Nirupam Roy (UIUC)

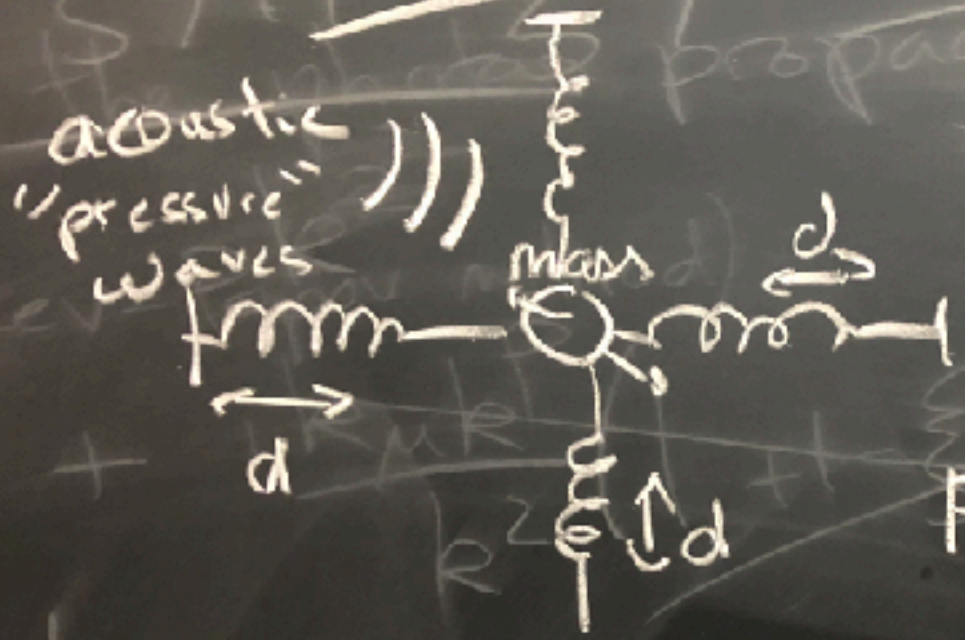
Mobile Security
Inaudible Voice Commands



Analog Sensor Security
Acoustic Attacks on MEMS Accelerometers


TITANIUM BULLET TWEETER
PYRAMID

Accelerometer

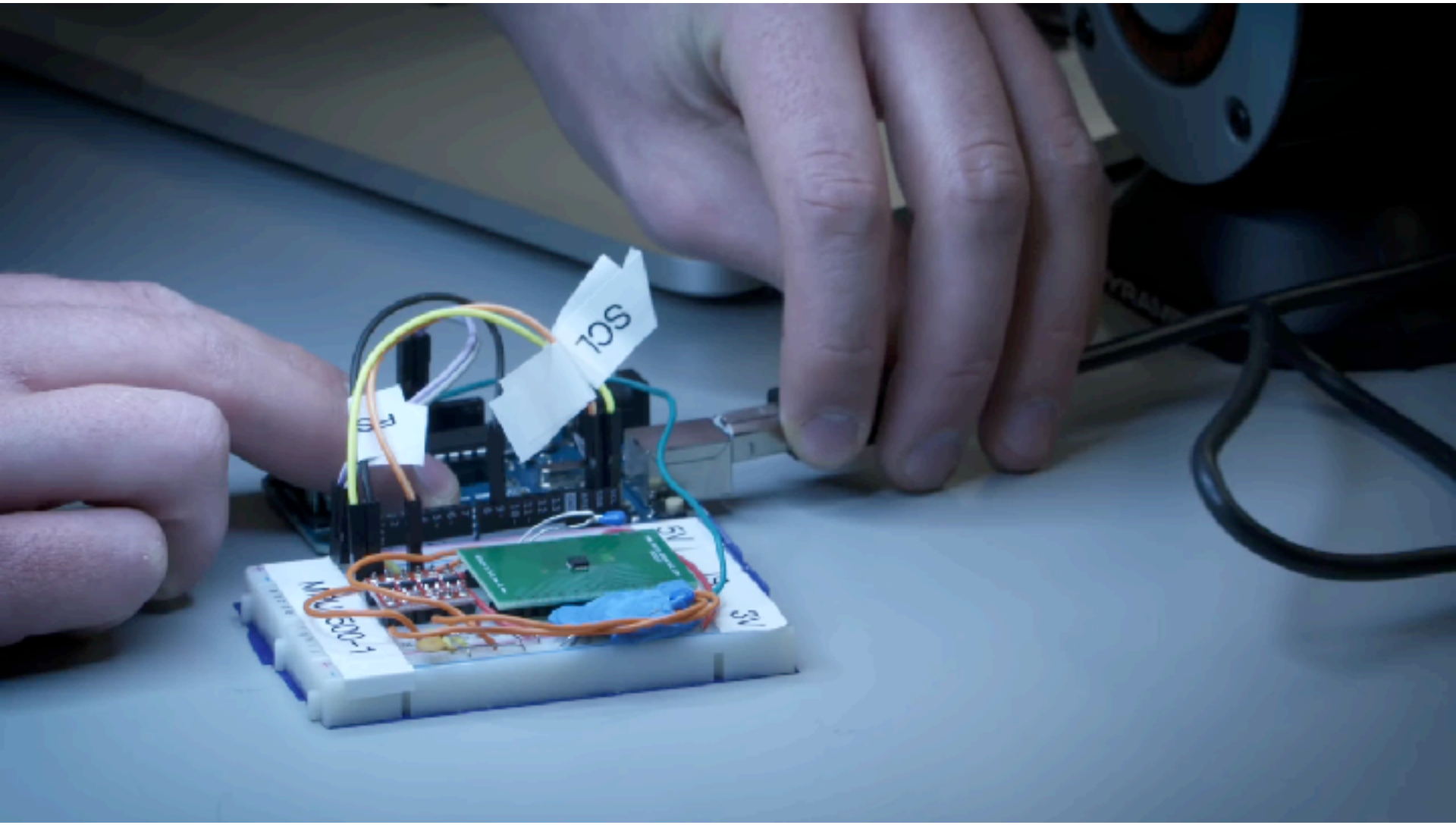


$$F = ma = kd$$

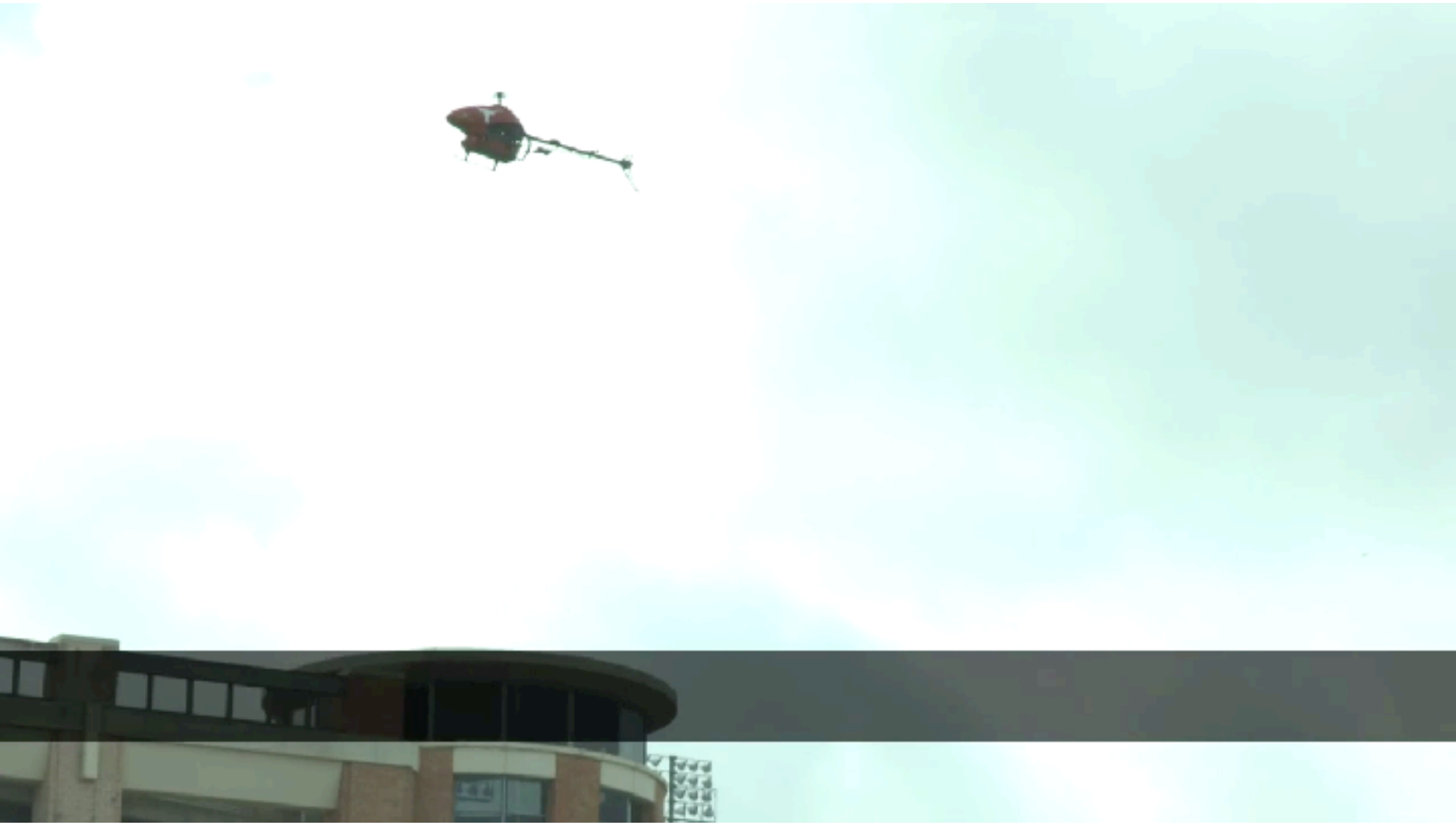
acceleration

measure displacem

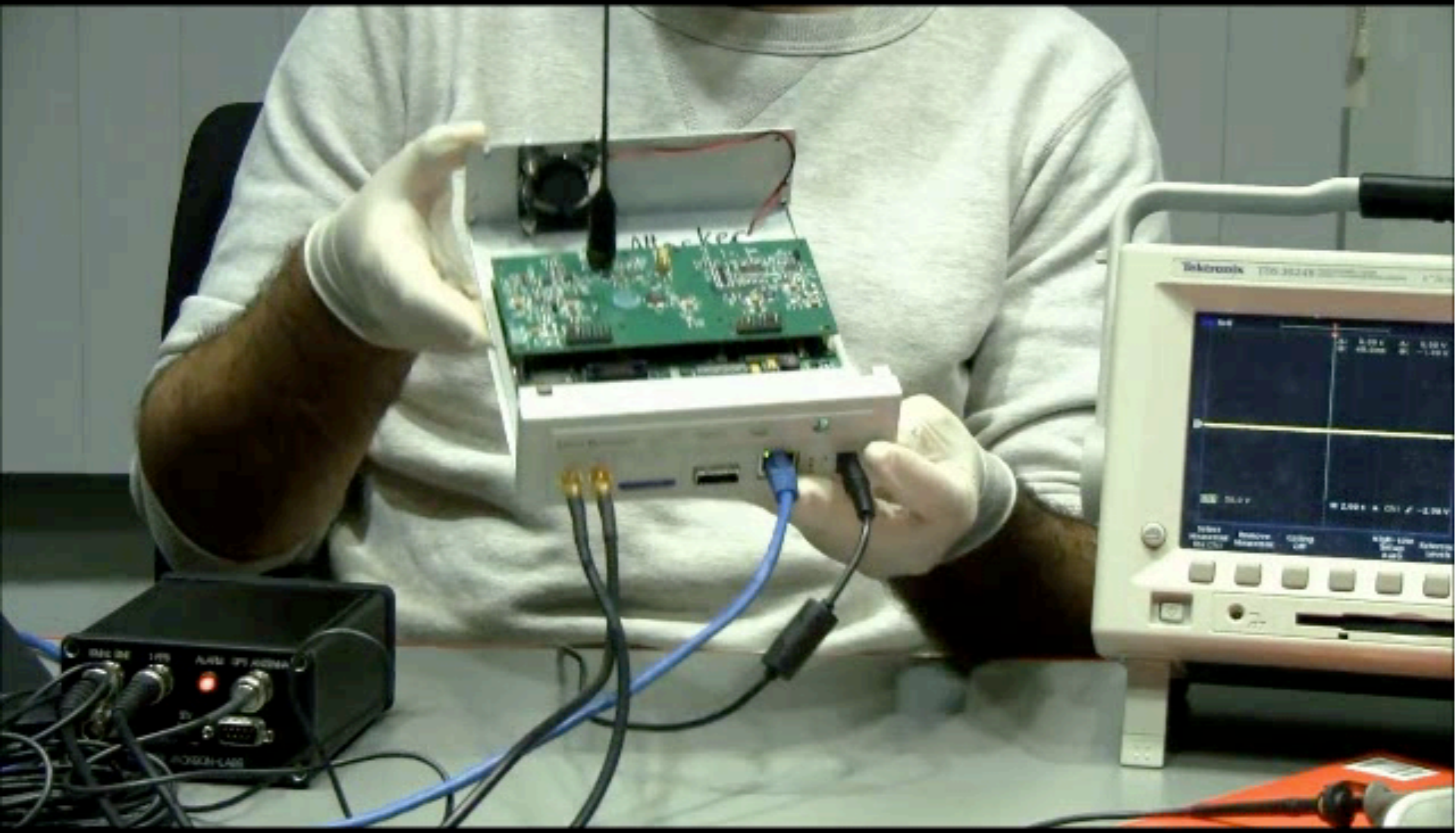
$$x = \iint a$$


SCL
5V
5V

Drone Security
Spoofing GPS Signals

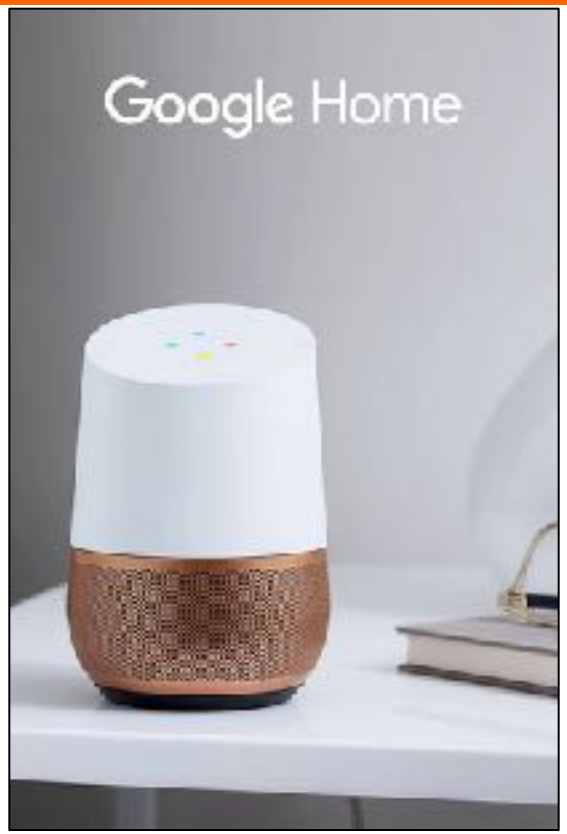


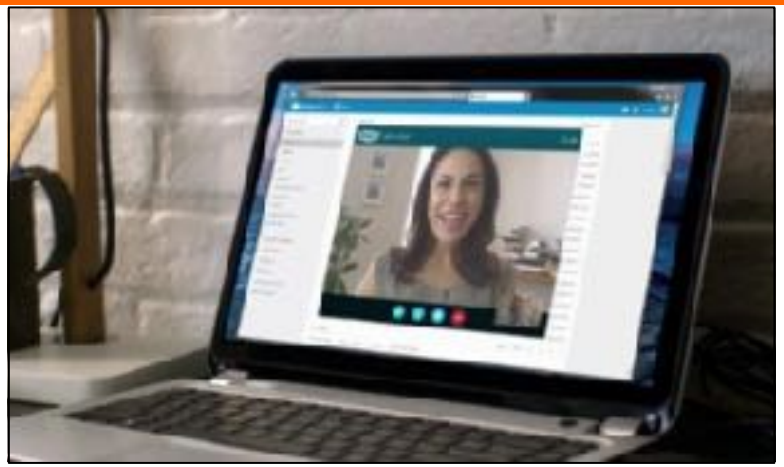
Pacemaker Security
Wireless Control of Pacemaker

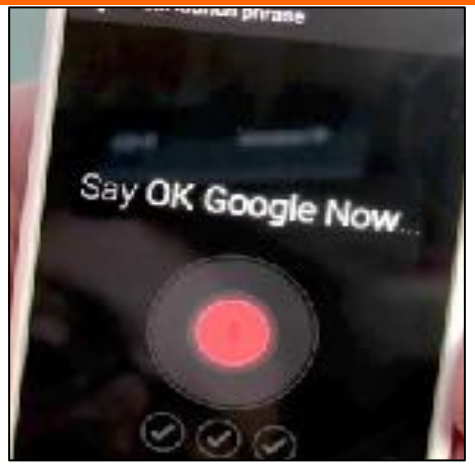

Tektronix

BackDoor: Making Microphones Hear Inaudible Sounds

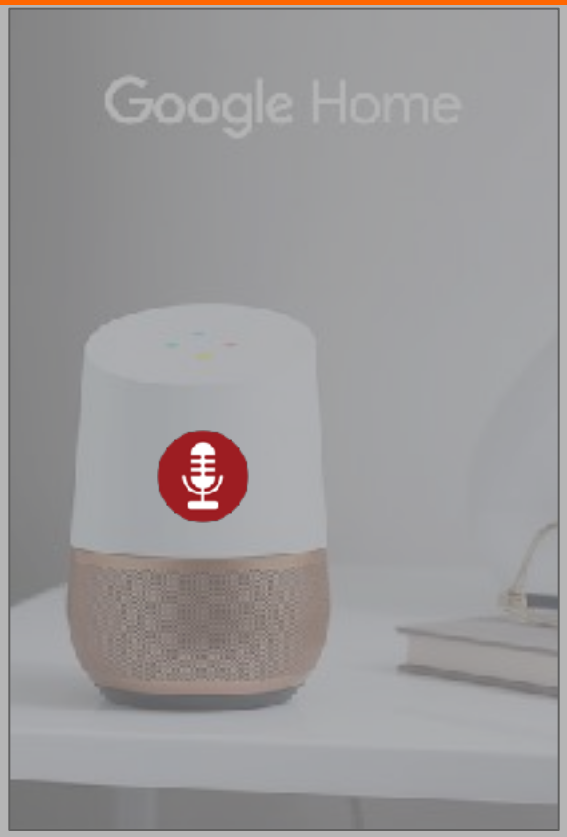
Microphones are everywhere

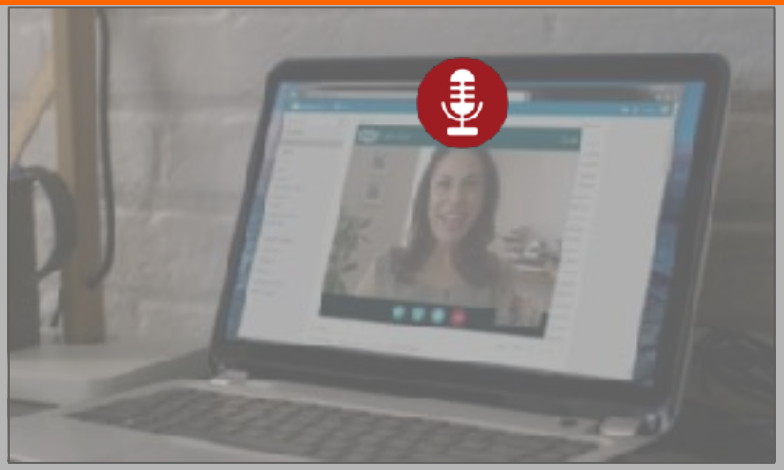


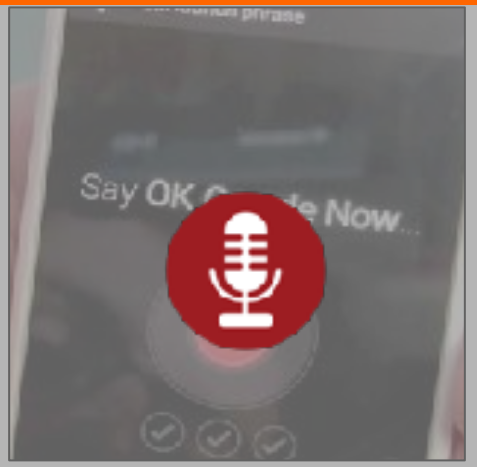


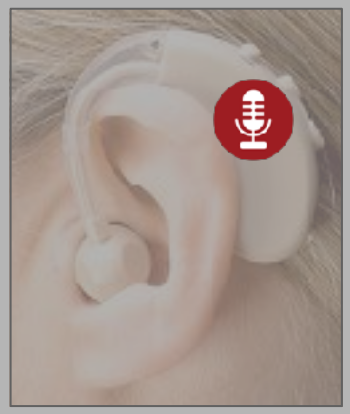


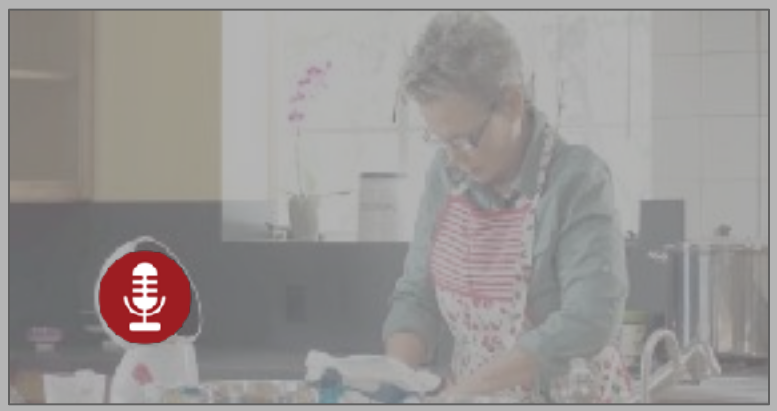
Microphones are everywhere

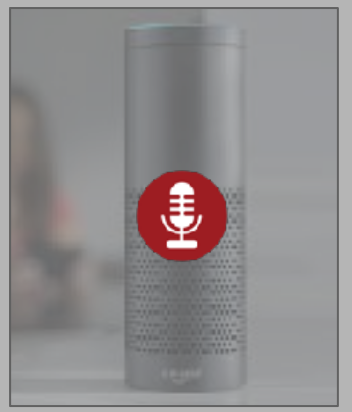




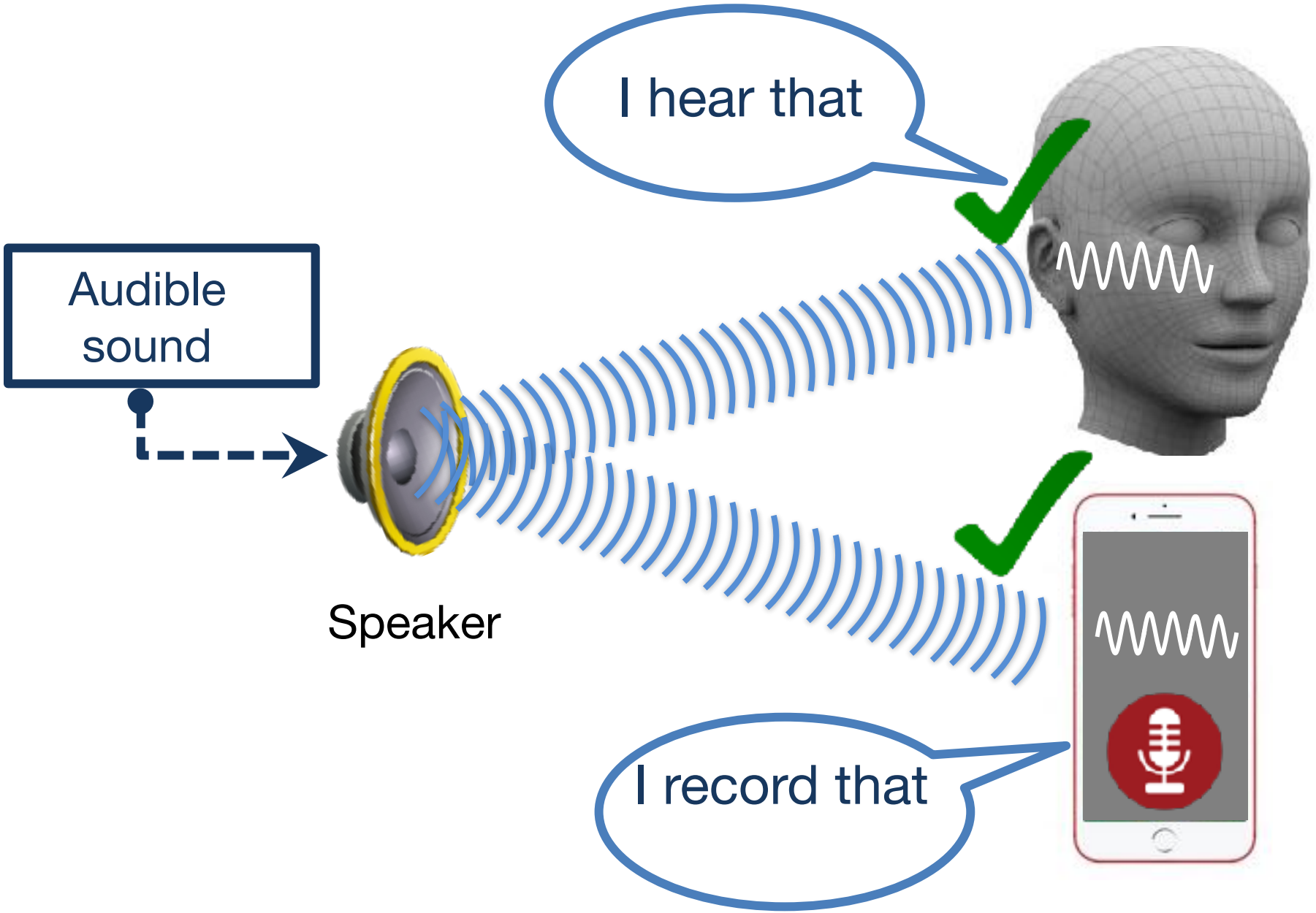




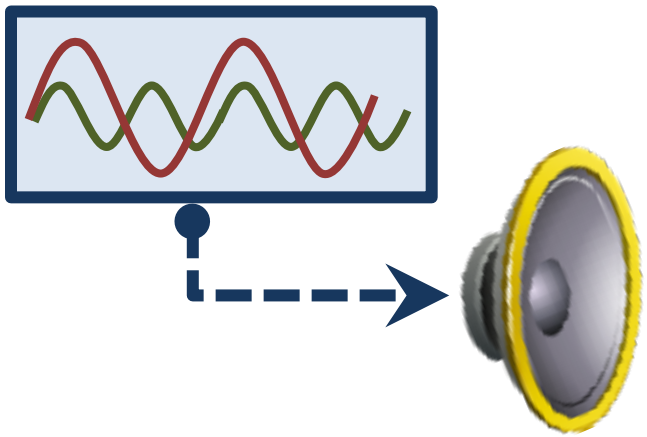




Microphones record audible sounds

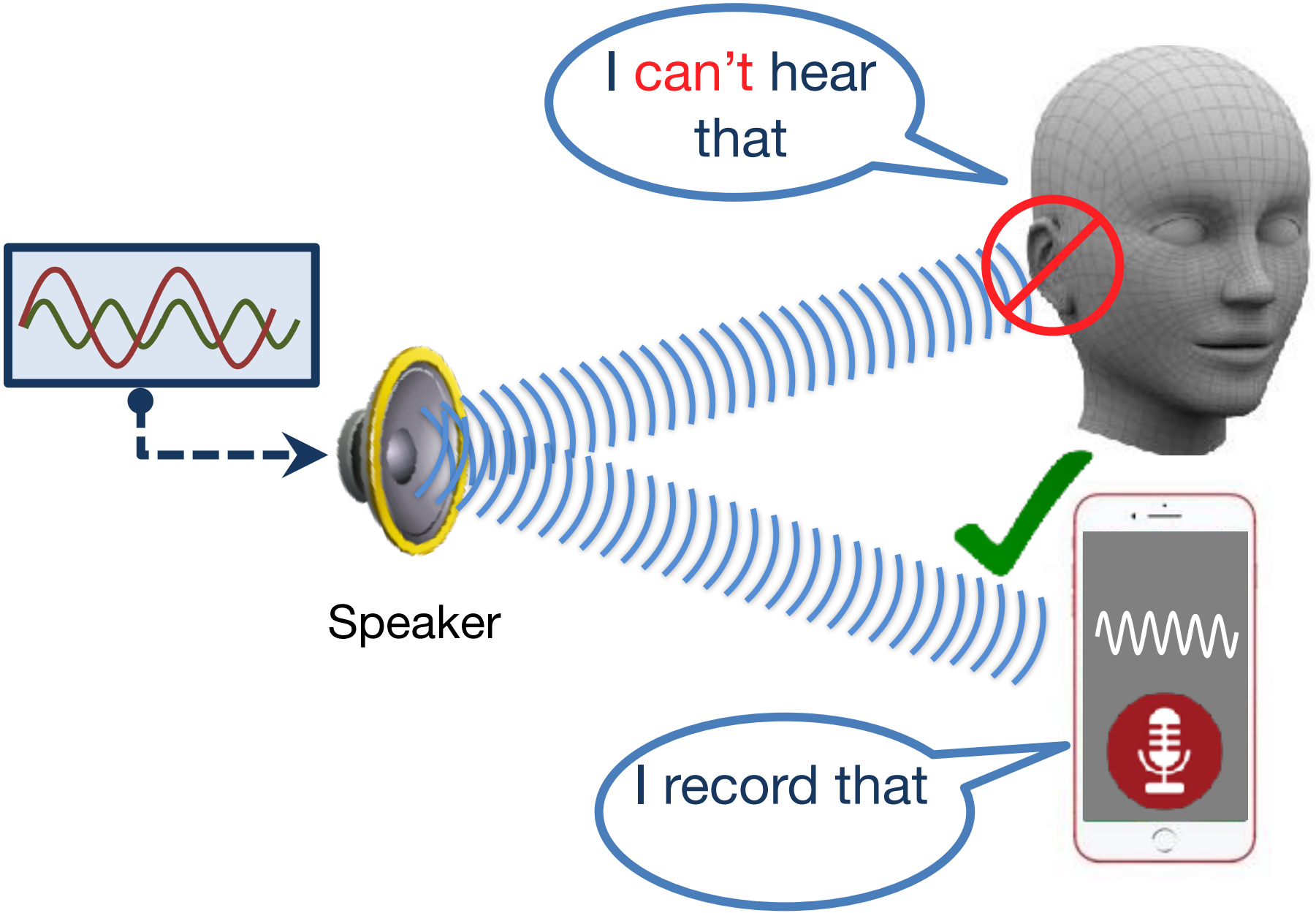


Inaudible, but recordable !



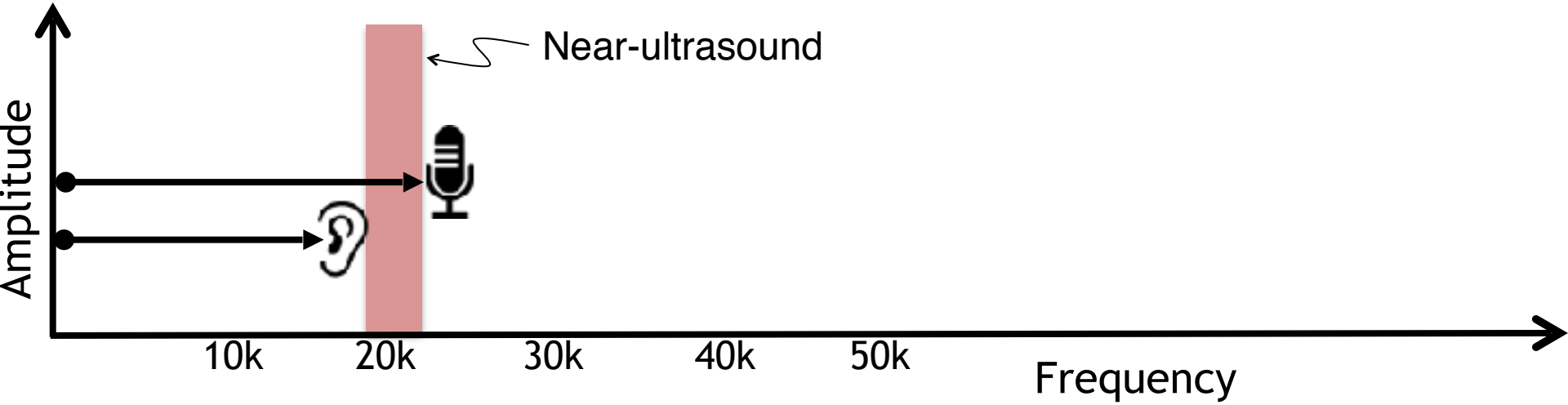
Speaker

Inaudible, but recordable !

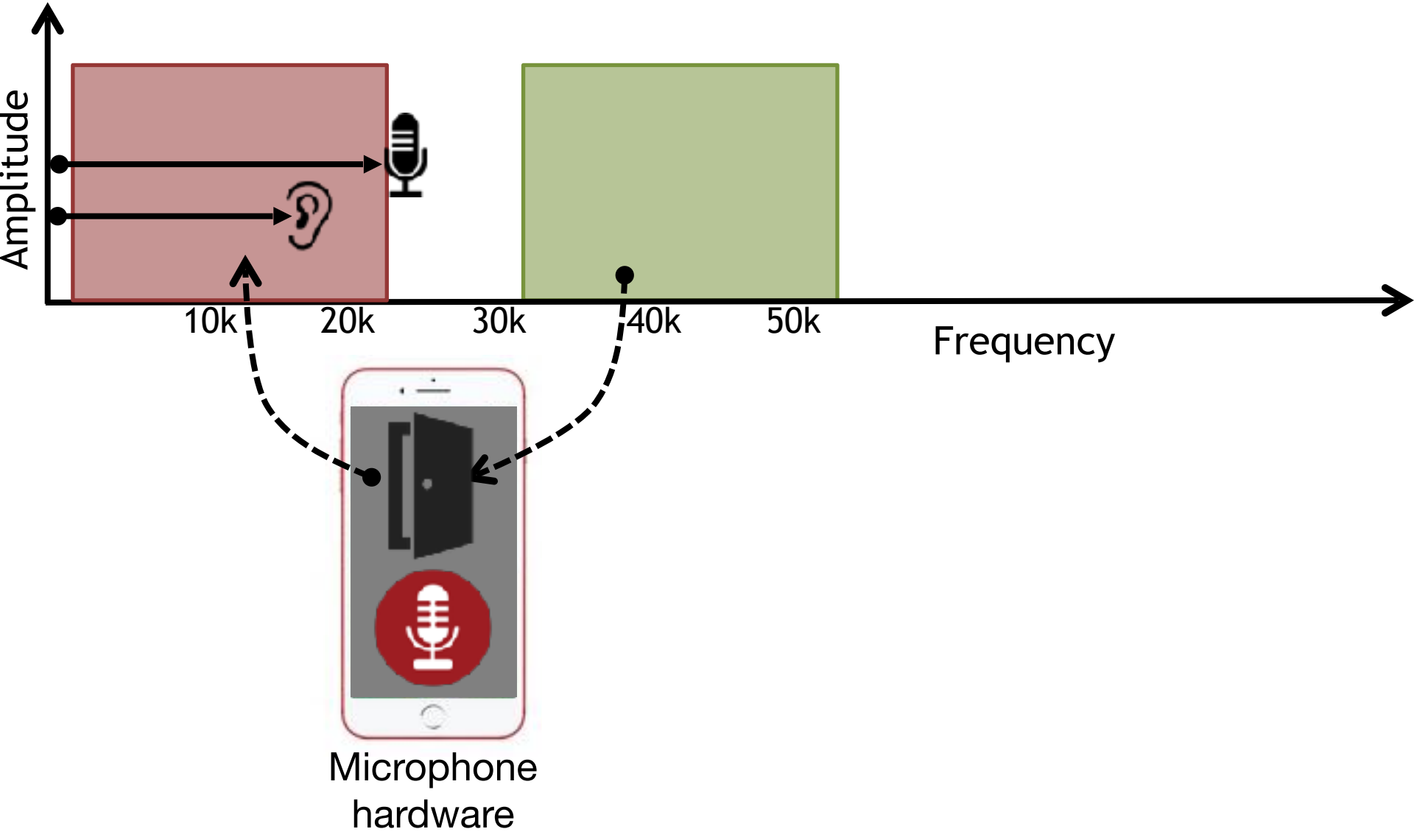


Works with unmodified devices

It's not "near-ultrasound"



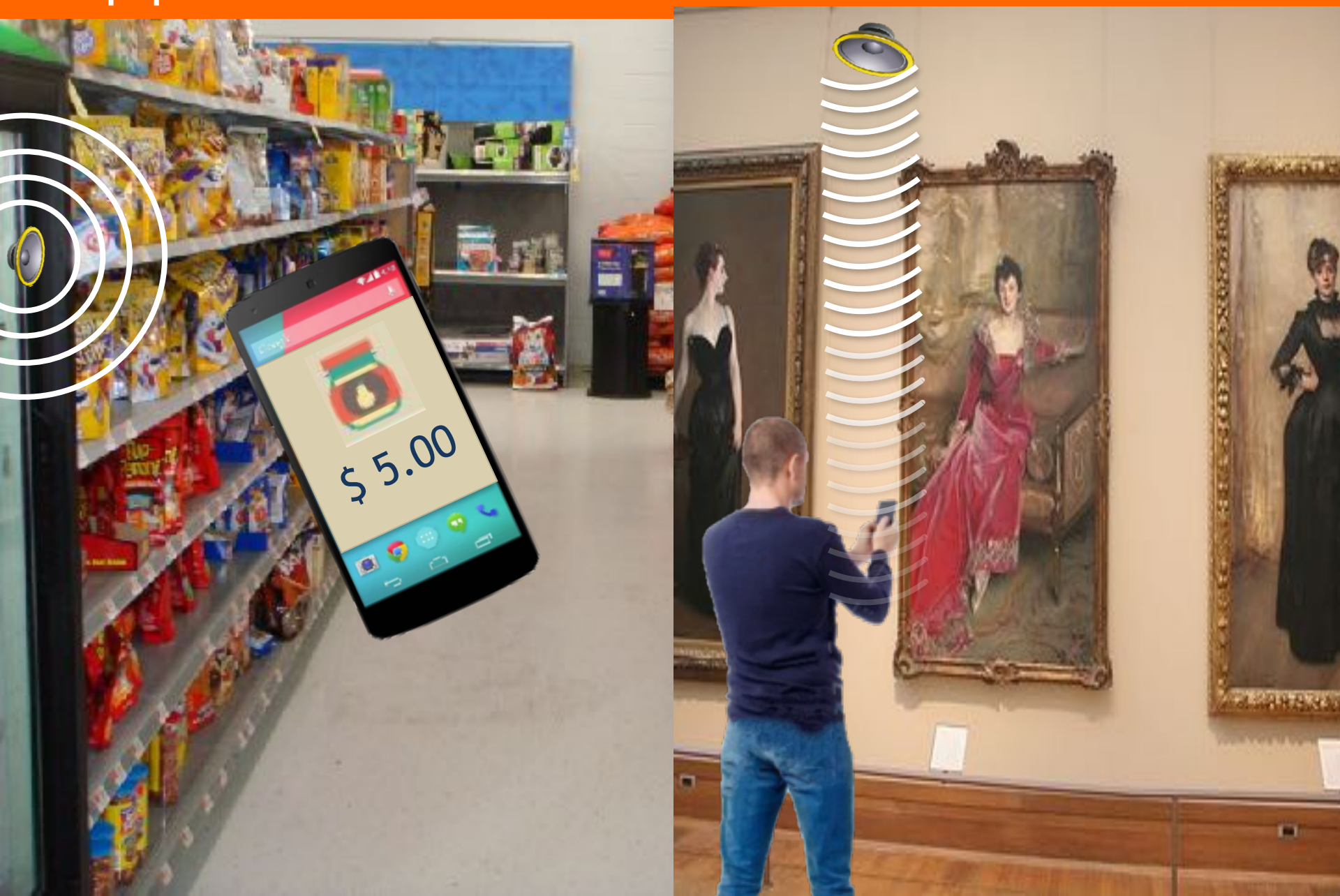
Exploiting fundamental nonlinearity



What can we do with it?

Application: Acoustic jammer

Application: Acoustic communication



Threat: Acoustic DOS attack

Threat: Acoustic DOS attack

Jamming
hearing aids

Threat: Acoustic DOS attack

Jamming
hearing aids

Blocking
911 calls

Talk outline

① Microphone Overview

② System Design

③ Challenges

④ Evaluation

Talk outline

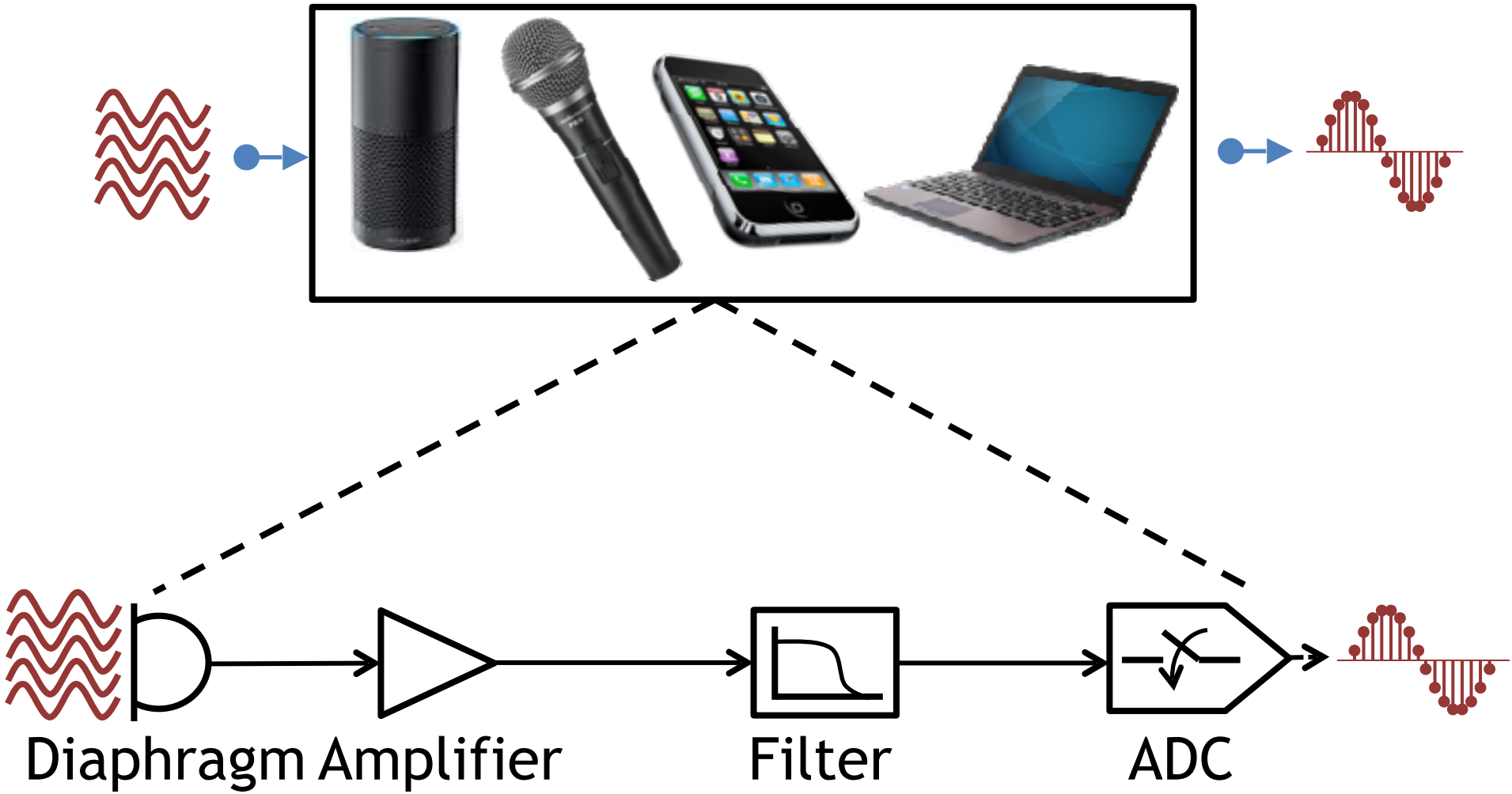
① Microphone Overview

② System Design

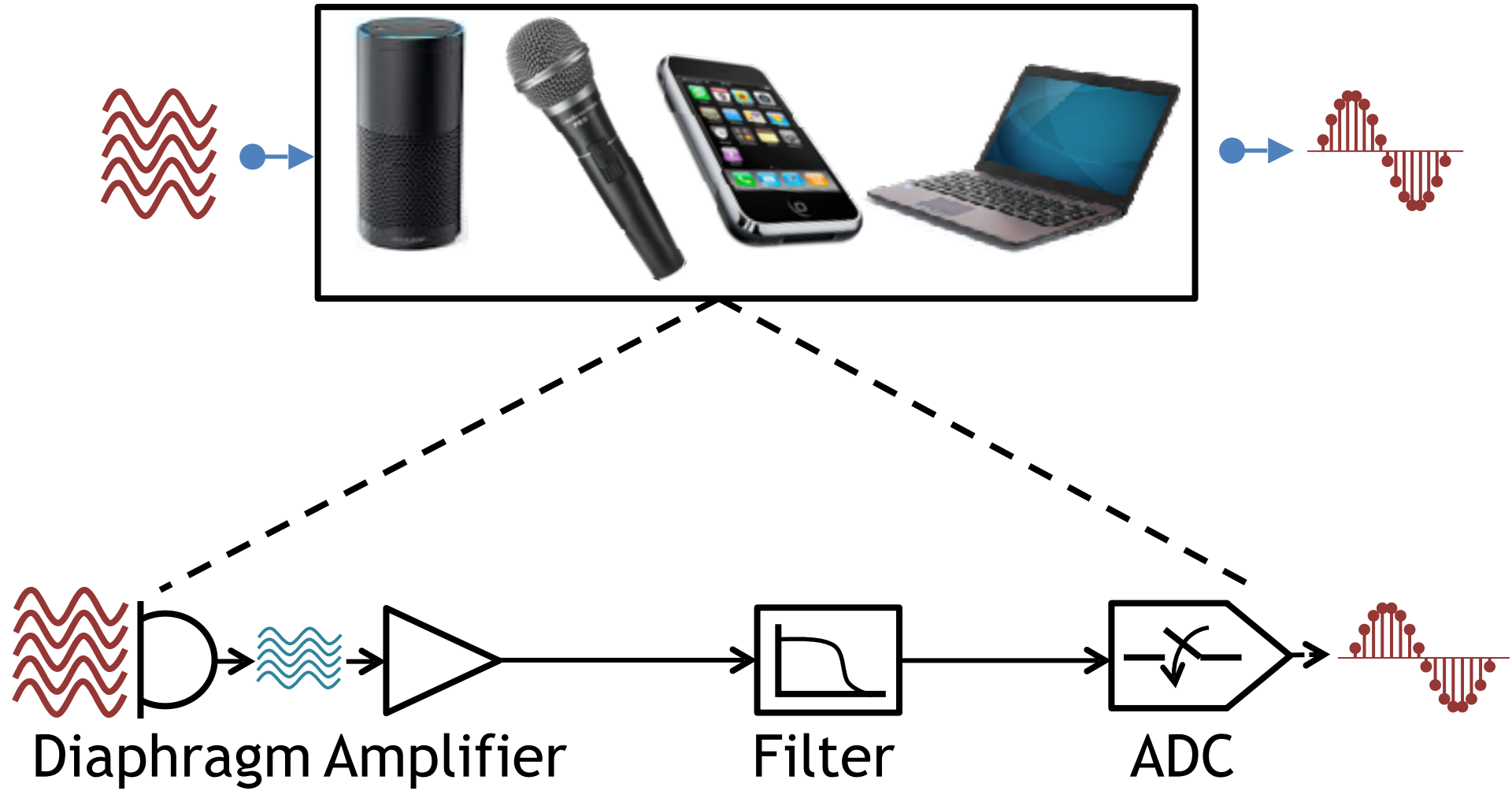
③ Challenges

④ Evaluation

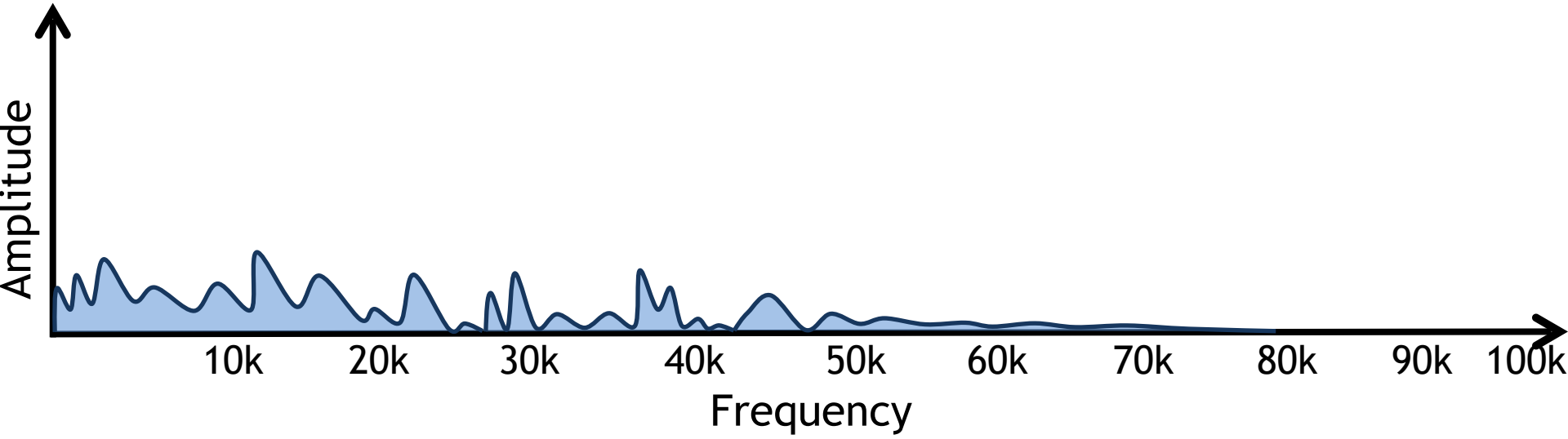
Microphone working principle

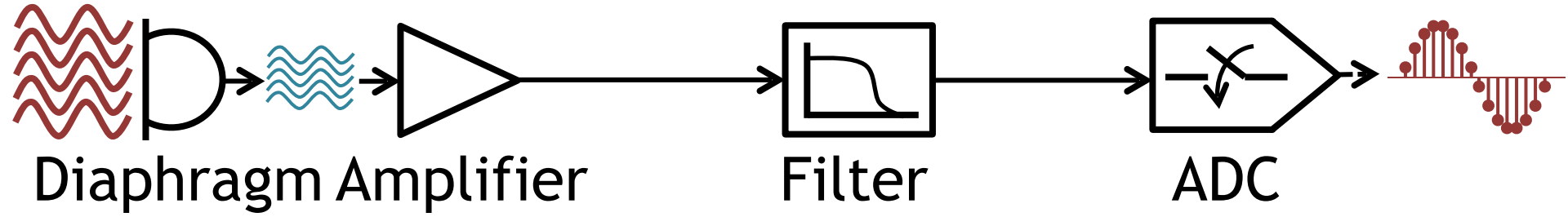


Microphone working principle

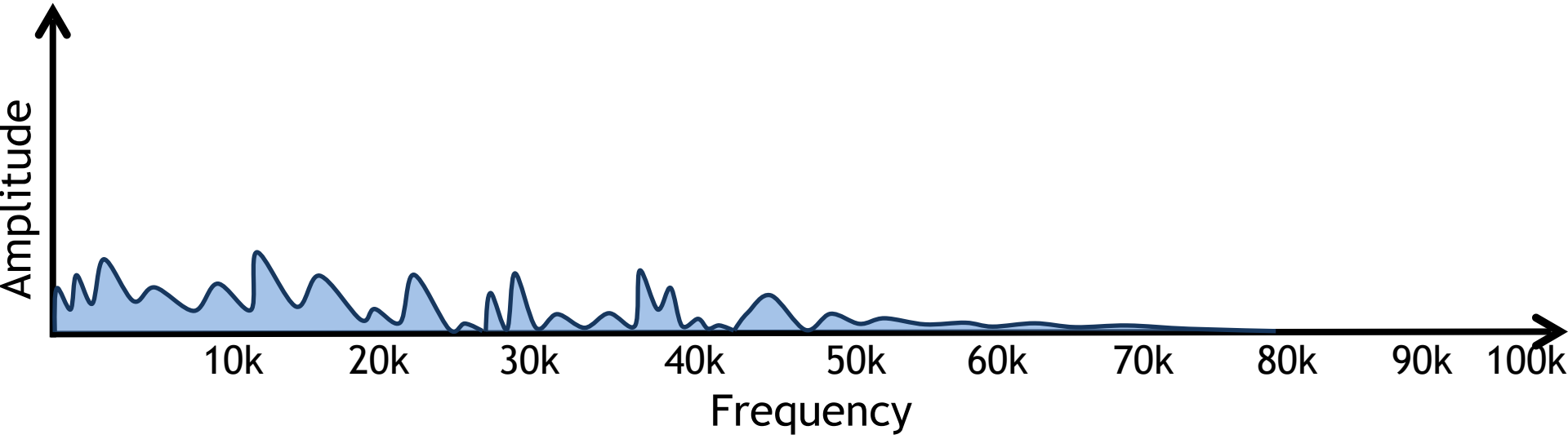


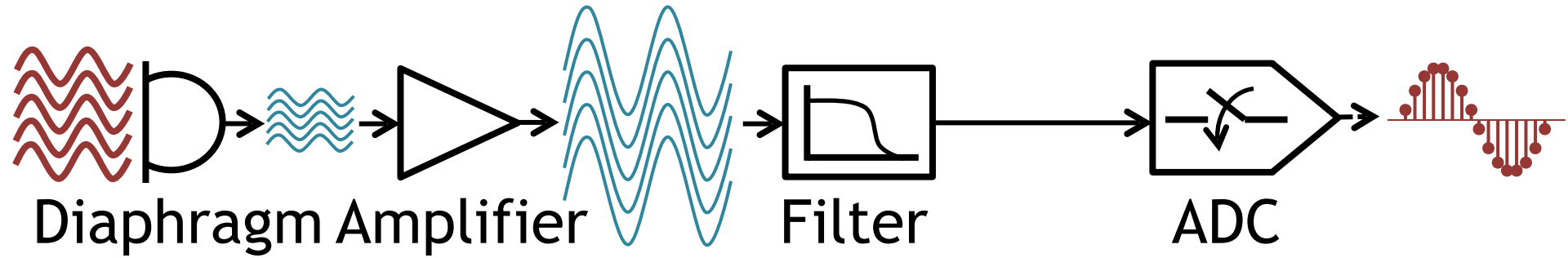
Microphone working principle



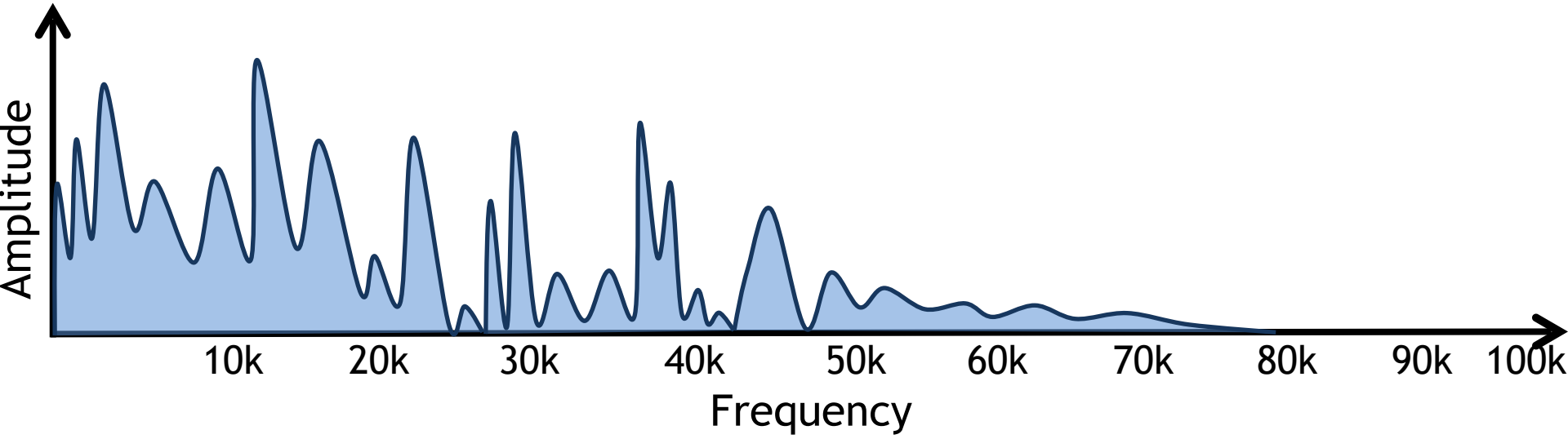


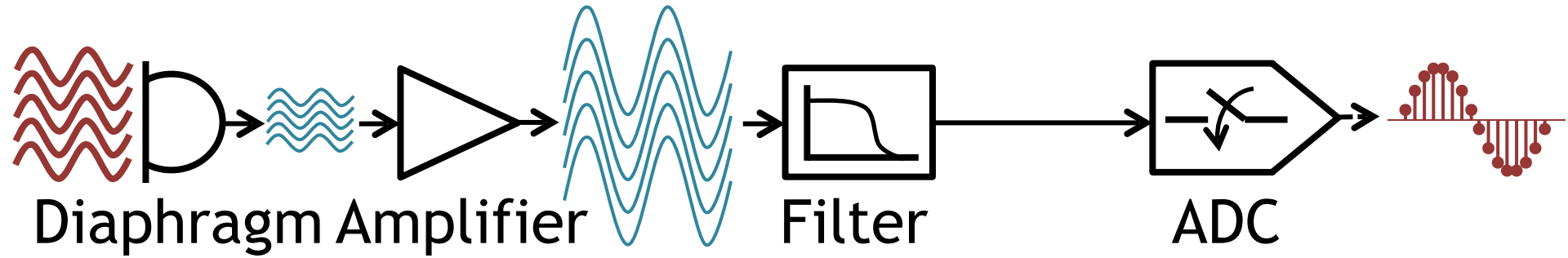
Microphone working principle



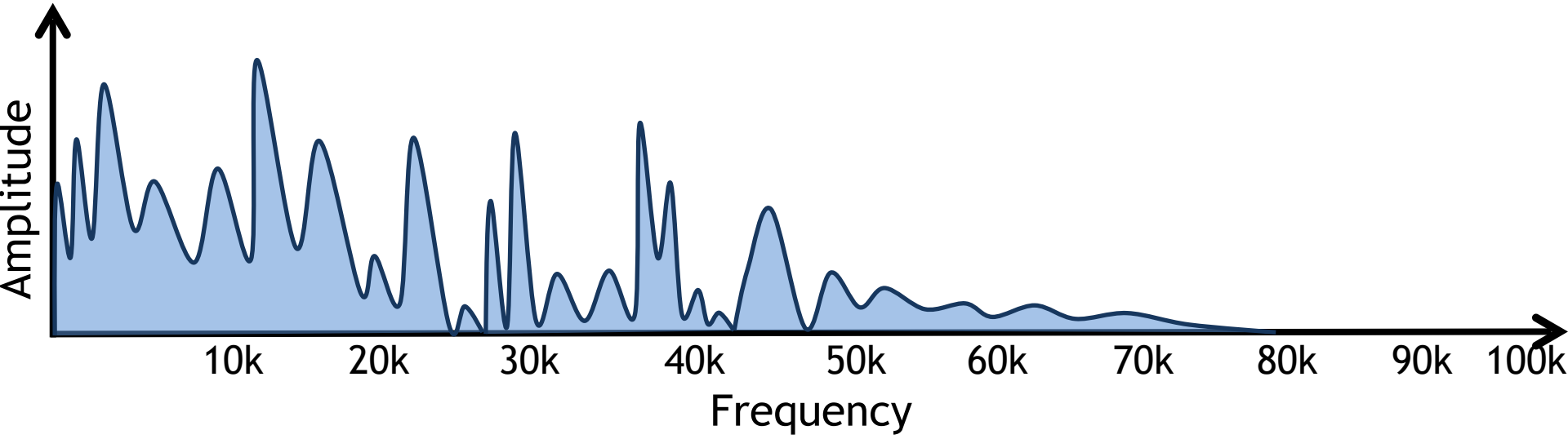


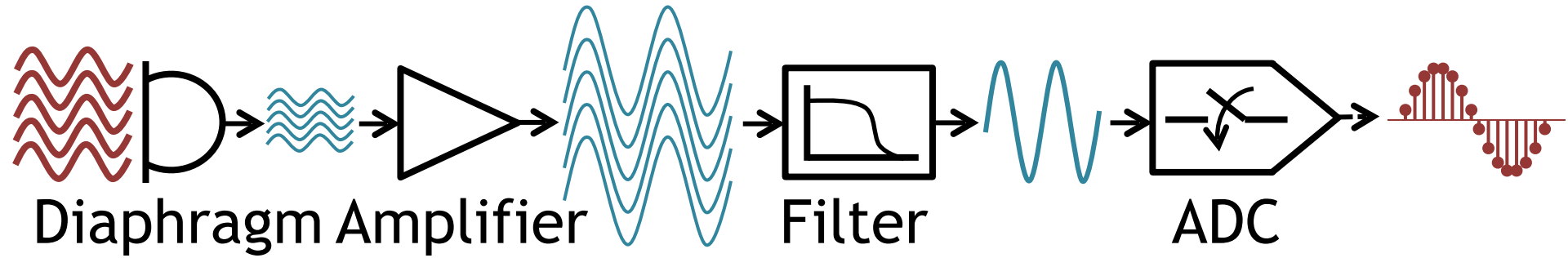
Microphone working principle



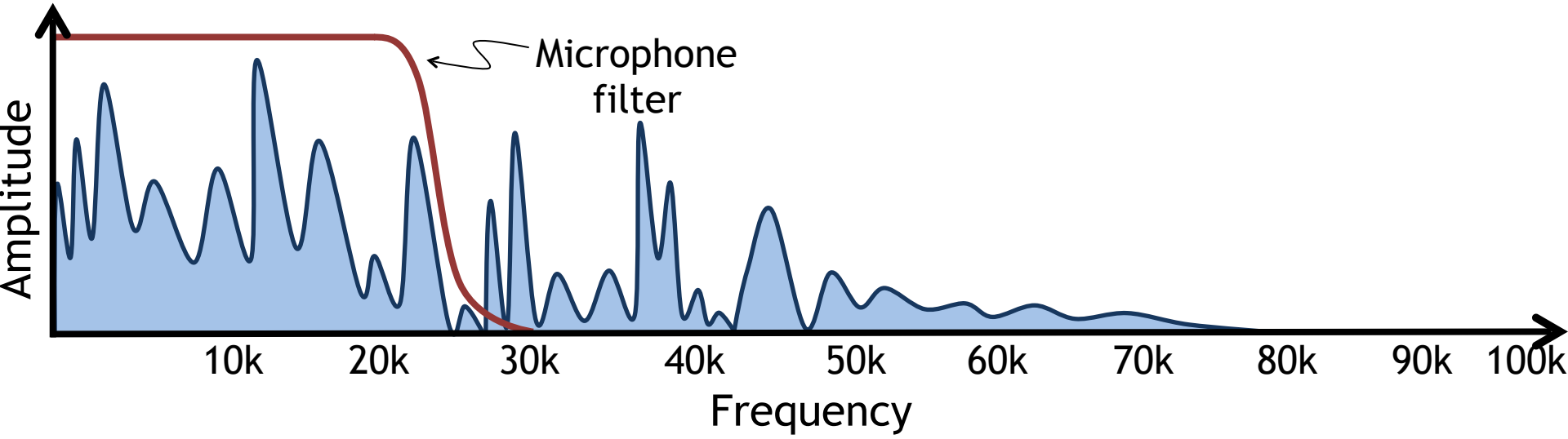


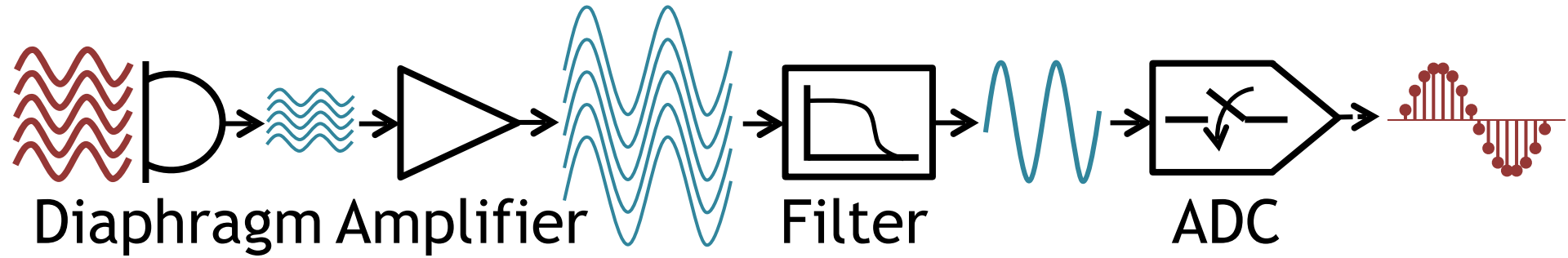
Microphone working principle



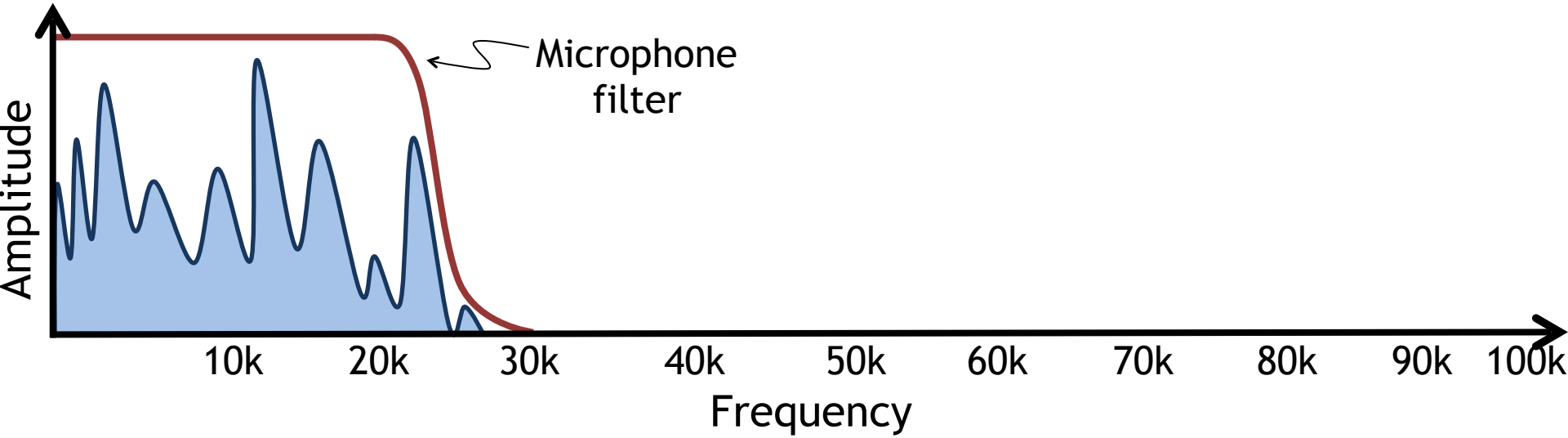


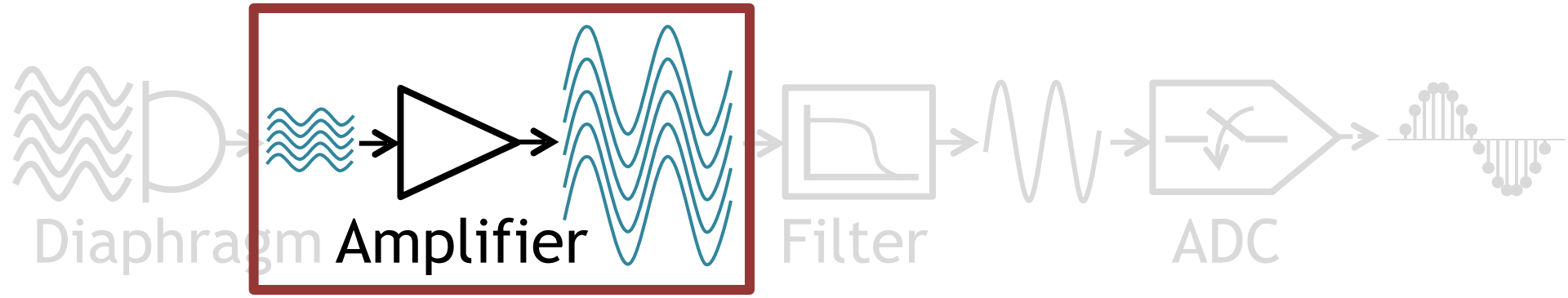
Microphone working principle



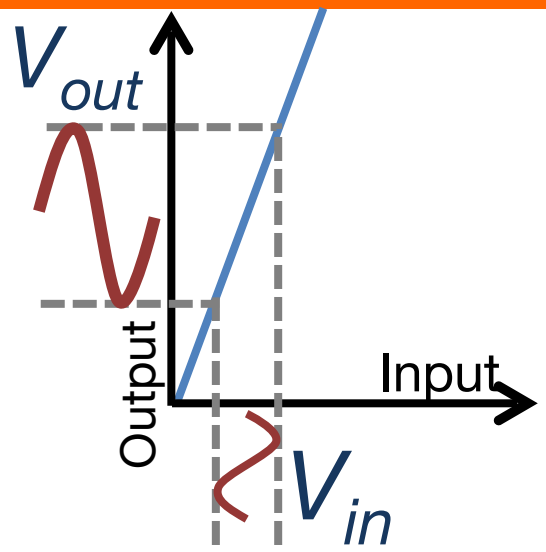


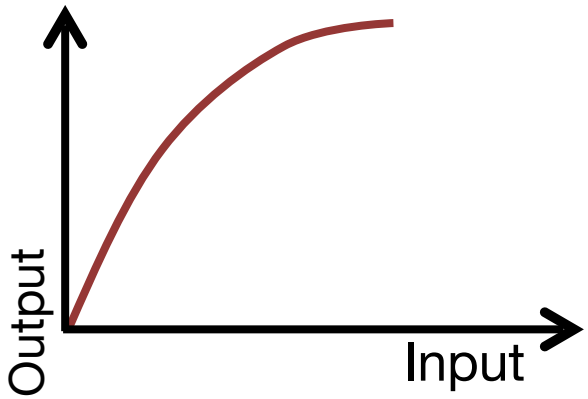
Microphone working principle





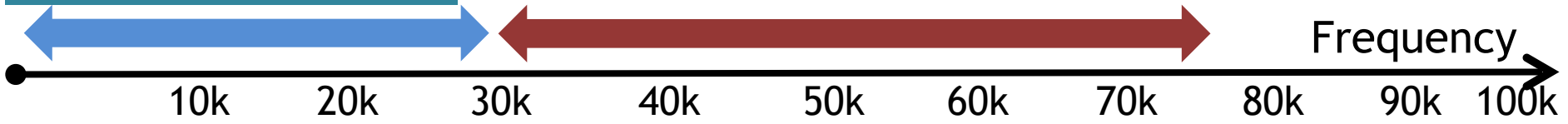
Microphone working principle

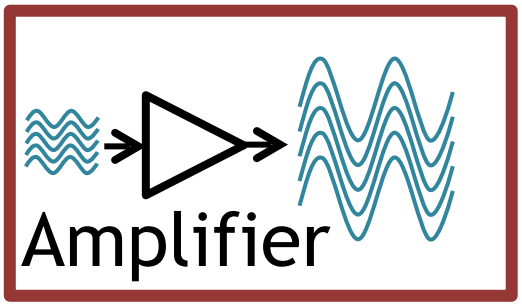




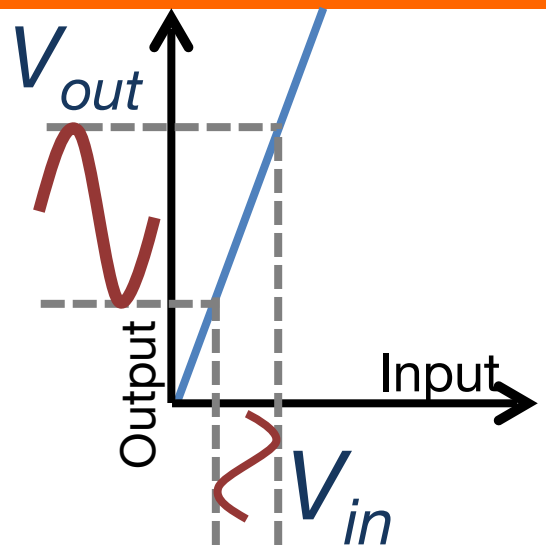
$V_{out} = a_1 V_{in}$

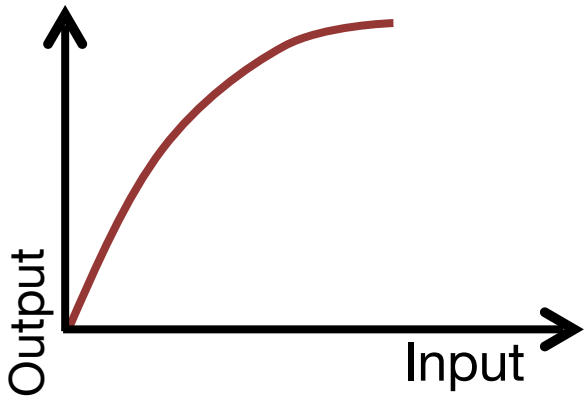
$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$





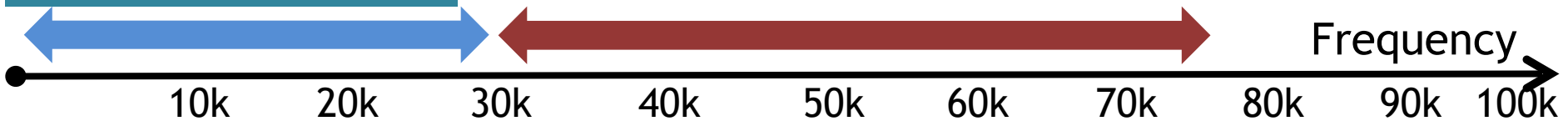
Microphone working principle

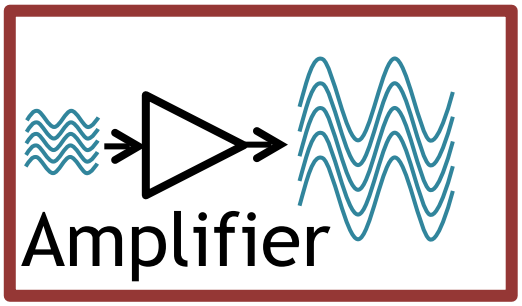




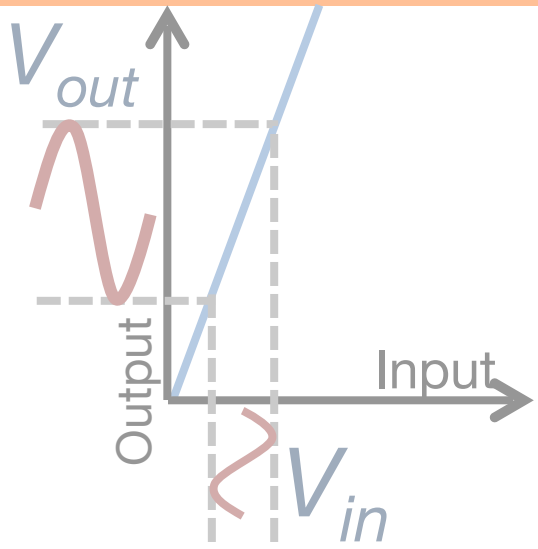
$V_{out} = a_1 V_{in}$

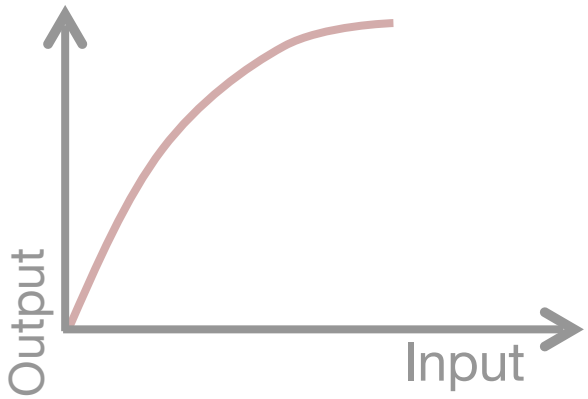
$V_{out} = a_1 V_{in} + a_2 V_{in}^2$





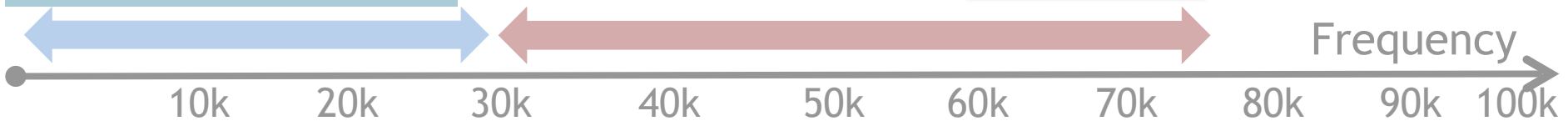
Microphone working principle

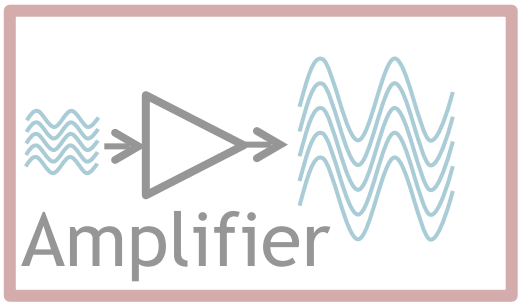




$V_{out} = a_1 V_{in}$

$V_{out} = a_1 V_{in} + a_2 V_{in}^2$





Talk outline

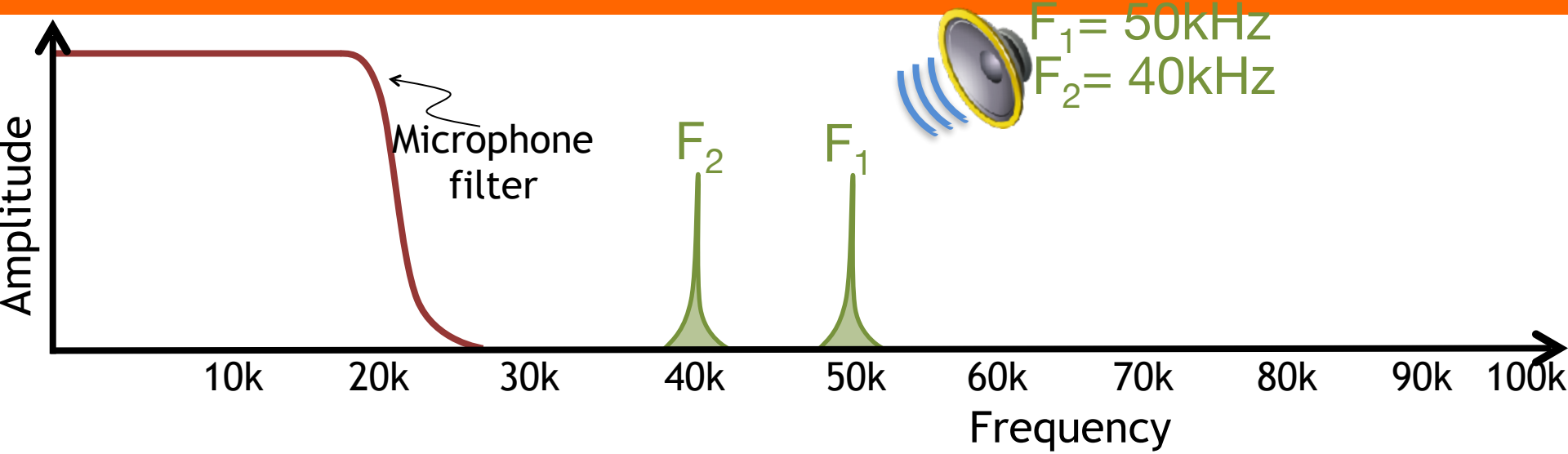
① Microphone Overview

② System Design

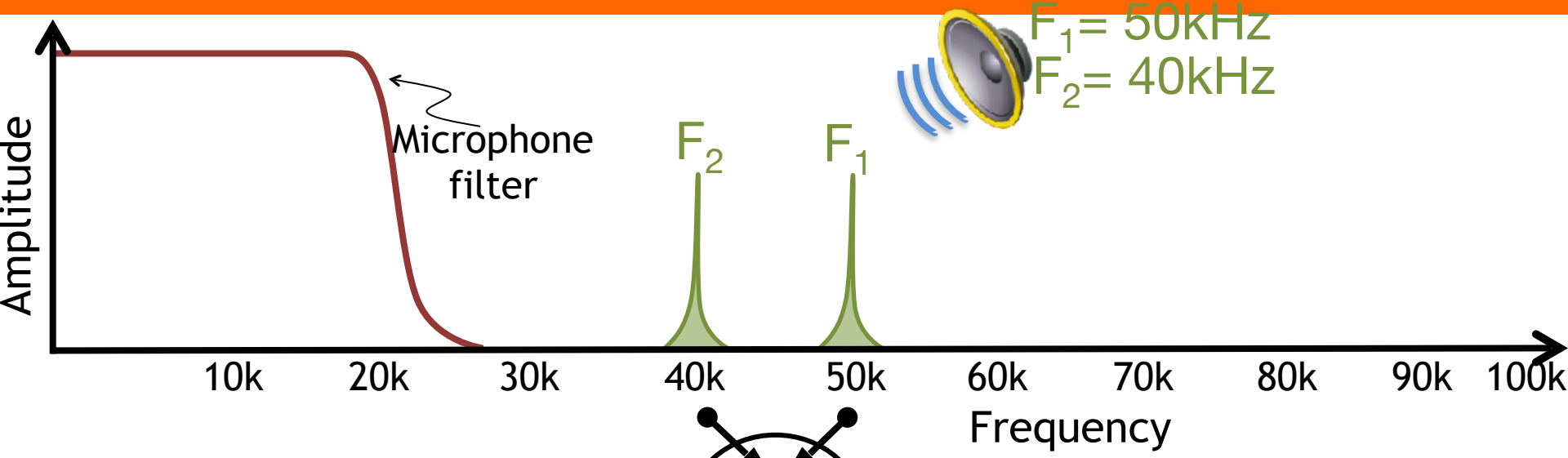
③ Challenges

④ Evaluation

Exploiting amplifier non-linearity



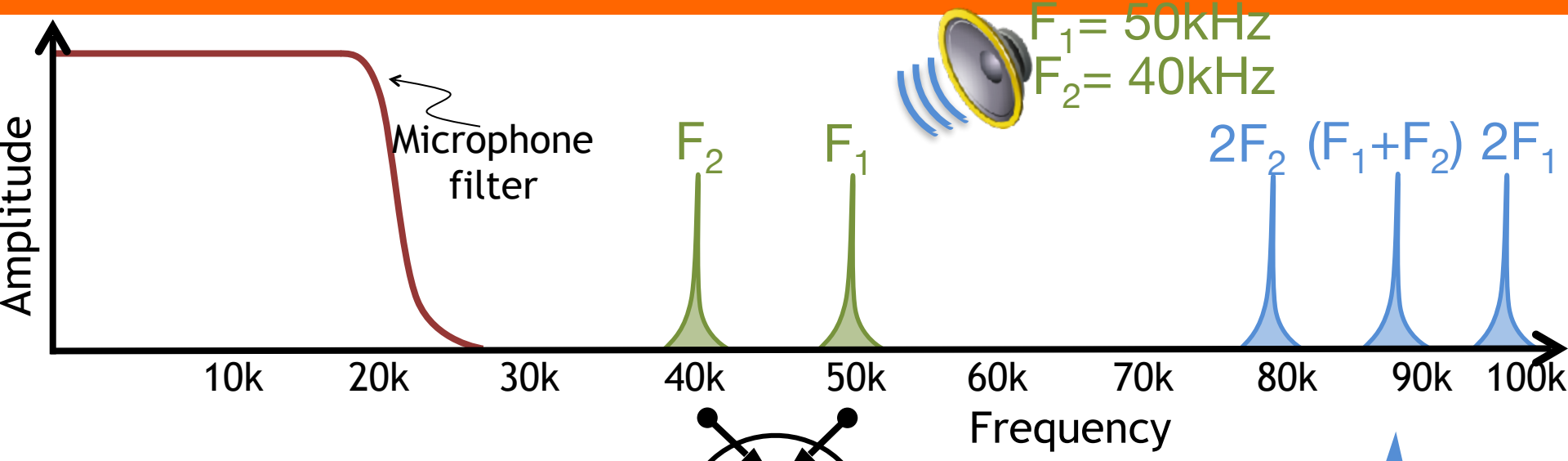
Exploiting amplifier non-linearity



$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 = \cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

Exploiting amplifier non-linearity

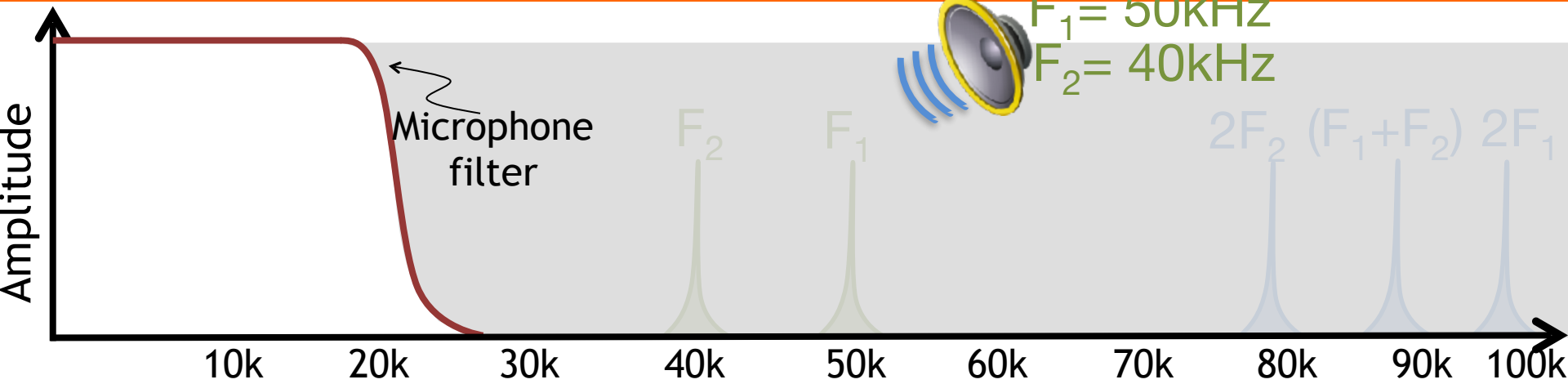


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

Exploiting amplifier non-linearity

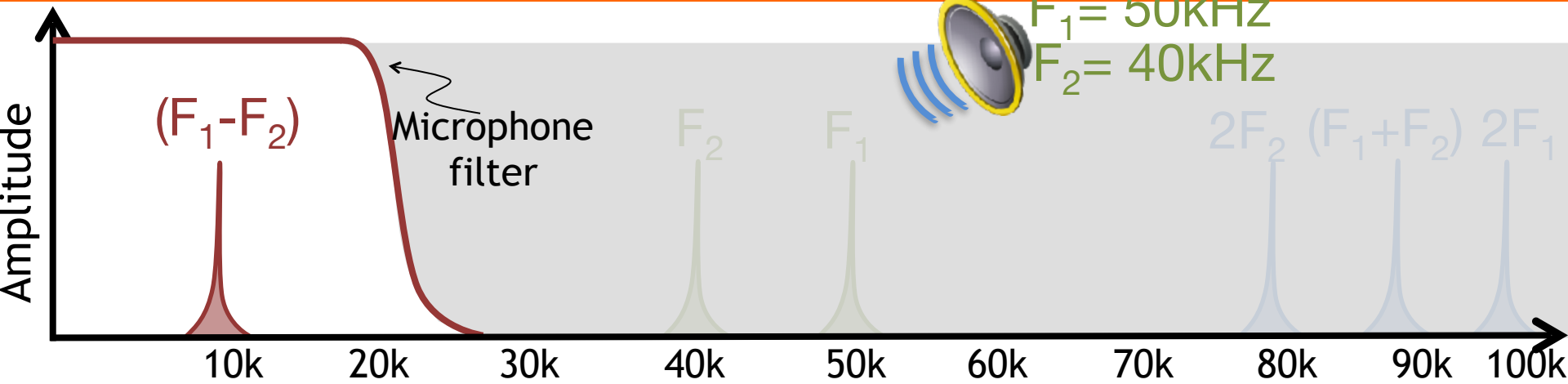


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

$$(\sin F_1 + \sin F_2)^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

Exploiting amplifier non-linearity

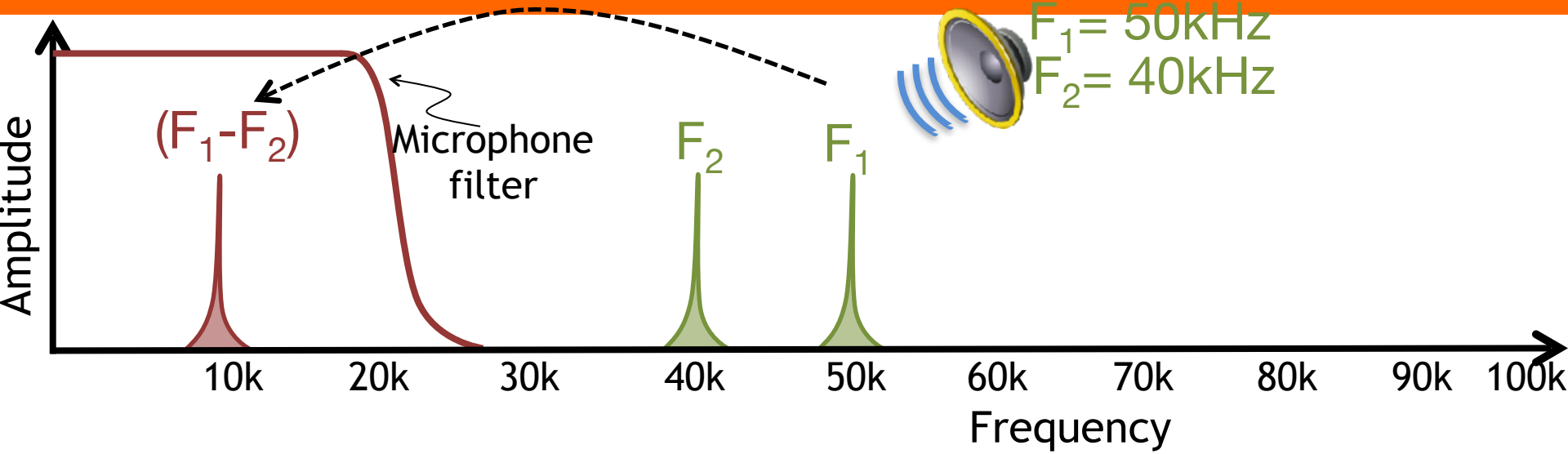


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

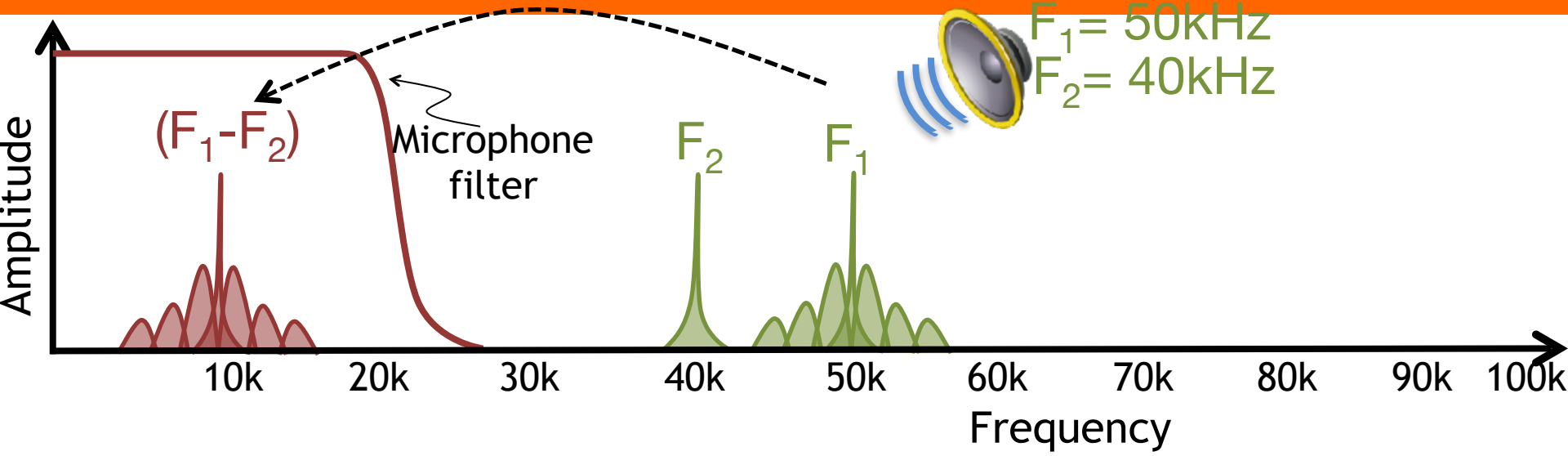
$$(\sin F_1 + \sin F_2)^2 =$$

$$\cos 2F_1 + \cos 2F_2 + \cos (F_1+F_2) + \cos (F_1 - F_2)$$

Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Talk outline

① Microphone Overview

② System Design

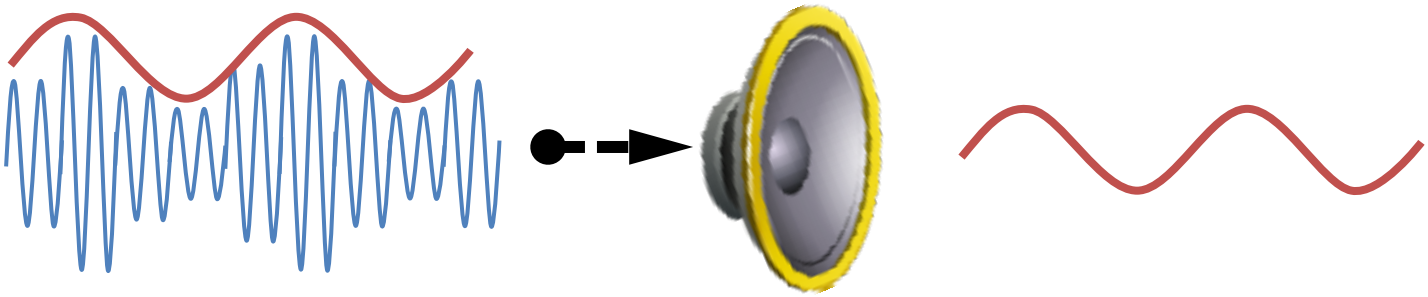
③ Challenges

④ Evaluation

Challenges

Amplitude modulation

$$S_{AM} = a \cdot \underbrace{\sin(\omega_m t)}_{\text{message}} \cdot \underbrace{\sin(\omega_c t)}_{\text{carrier}}$$



Ultrasonic speaker

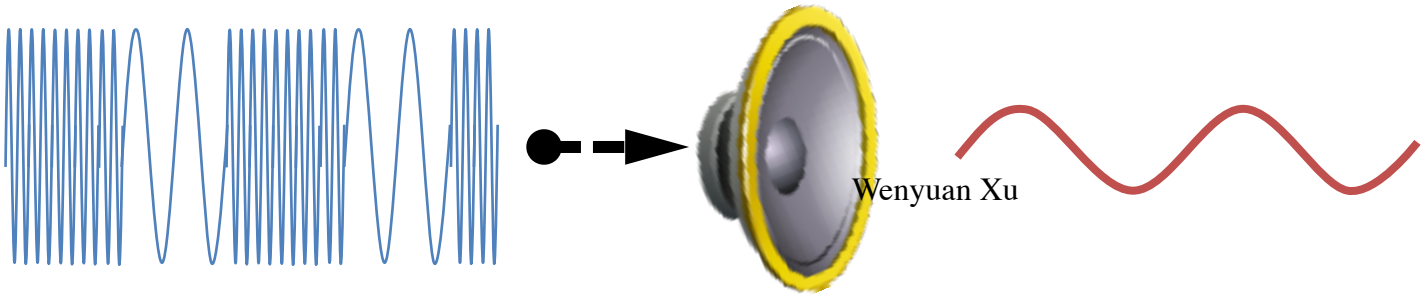
$$S_{AM}^2 = A_2\left(a\sin(\omega_m t)\cdot(\omega_c t)\right)^2$$
$$= -A_2\frac{a^2}{4}\cos(2\omega_m t) + \text{some higher frequency}$$

<u>Problem:</u> speaker has non-linearities => Audible sound

Challenges

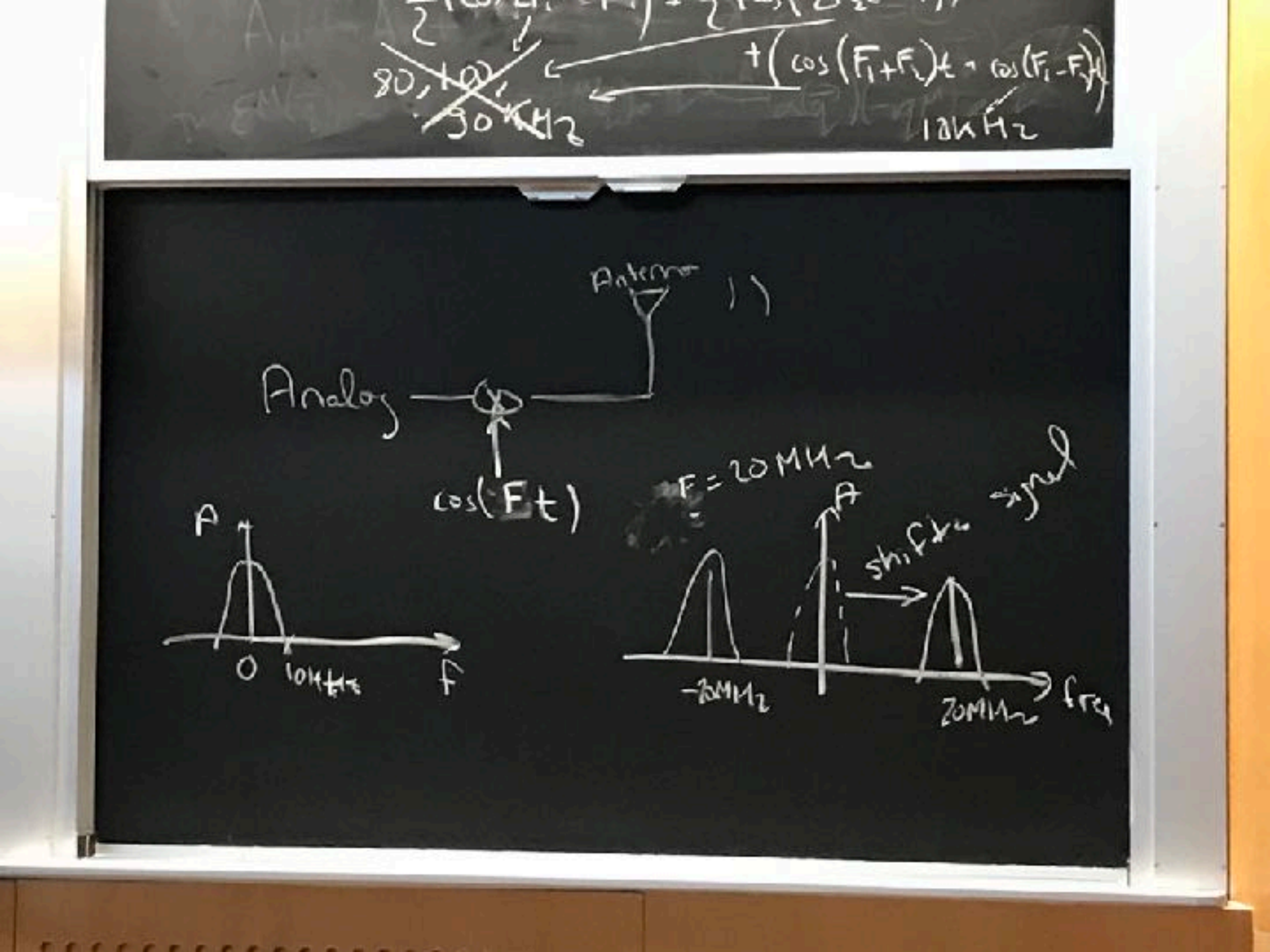
Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



Ultrasonic speaker

Primer on Modulation


Antenna
Analog
cos(Ft)
A
0
10MHz
F
F=20MHz
A
shifted signal
-20MHz
20MHz
freq

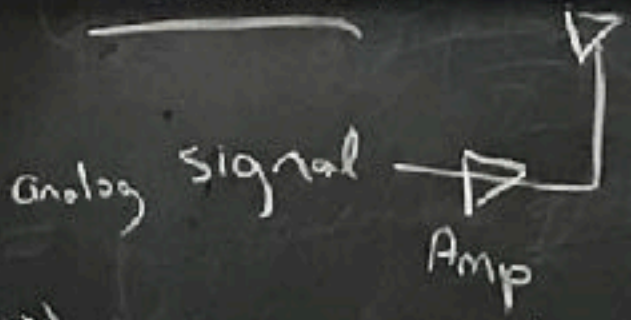
$+\left(\cos(F_1+F_2)t - \cos(F_1-F_2)t\right)$

80, 100, ~~90~~ KHz

10kHz

Modulation

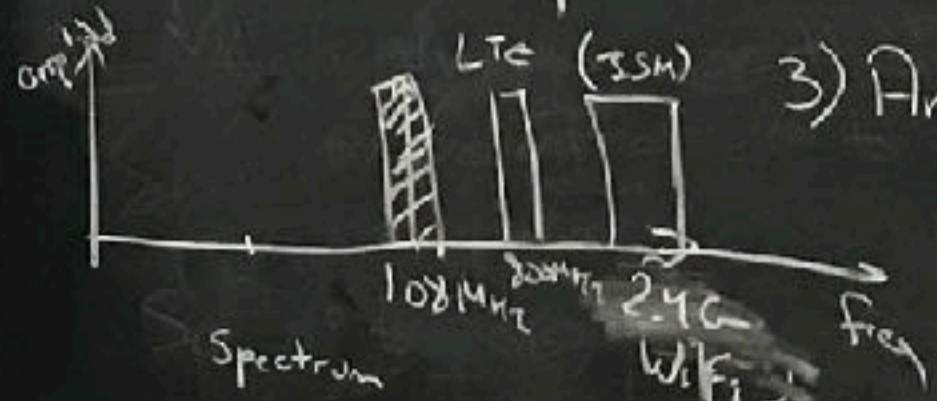
Why "modulation"?

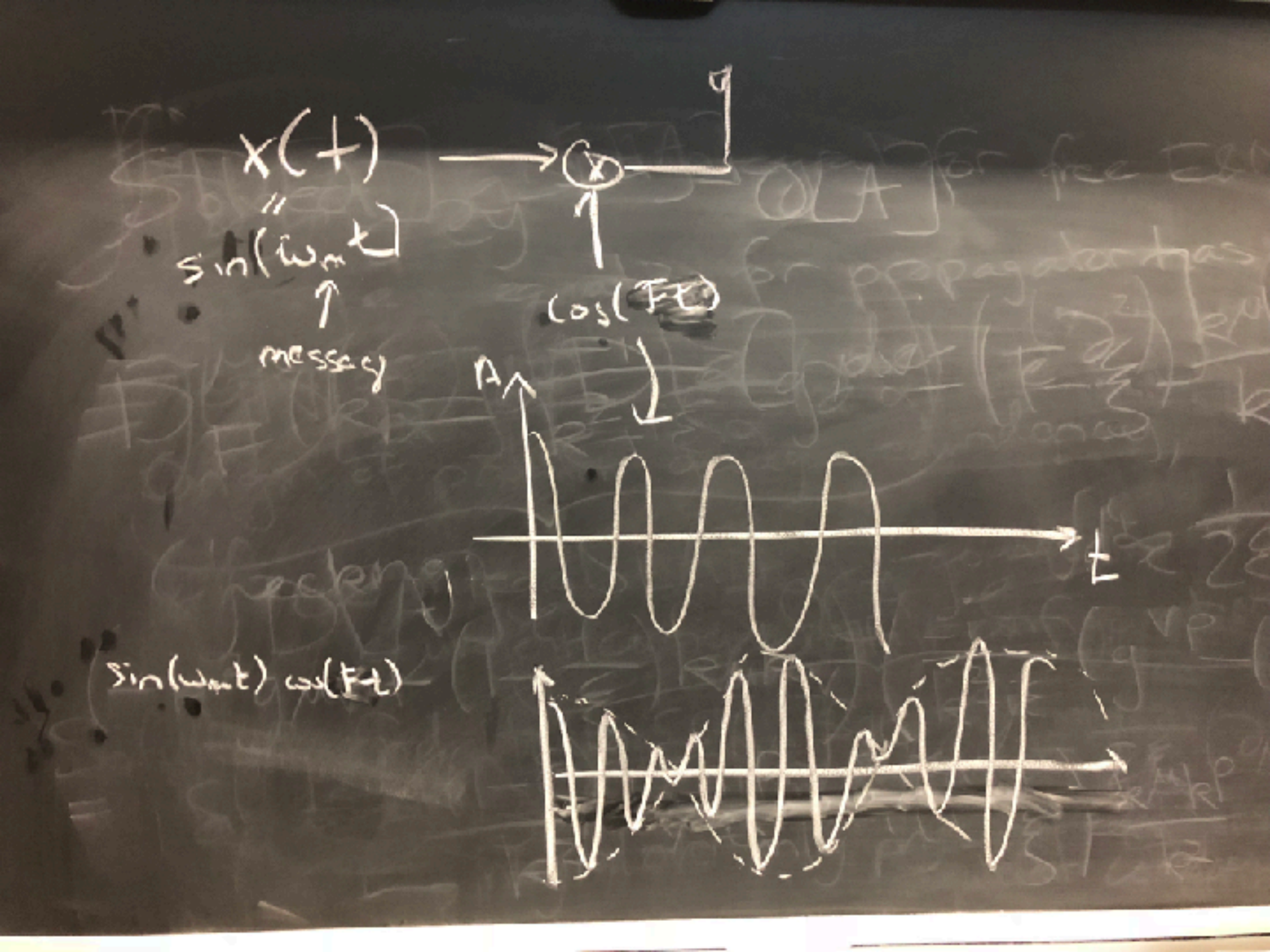


1) Interference

2) Spectrum Access (Legal usage)

3) Antenna size $\left(\sim \frac{\lambda}{4}\right)$




x(t)
sin(ωmt)
message
cos(Ft)
A
t
sin(ωmt) cos(Ft)

$$S^2 = \left(a \sin(\omega_m t) \sin(\omega_c t) \right)^2$$

$$= \frac{a^2}{4} \left[\left[\cos(\omega_m - \omega_c)t - \cos(\omega_m + \omega_c)t \right] \right]$$

$\omega_c >> 20\text{KHz}$ $\cos^2(\omega_m - \omega_c)t + \cos^2(\omega_m + \omega_c)t$ $\Rightarrow$ filte

$\omega_m << 20\text{KHz}$ $-2\cos(\omega_m - \omega_c)t \cos(\omega_m + \omega_c)t$ remove

Signal

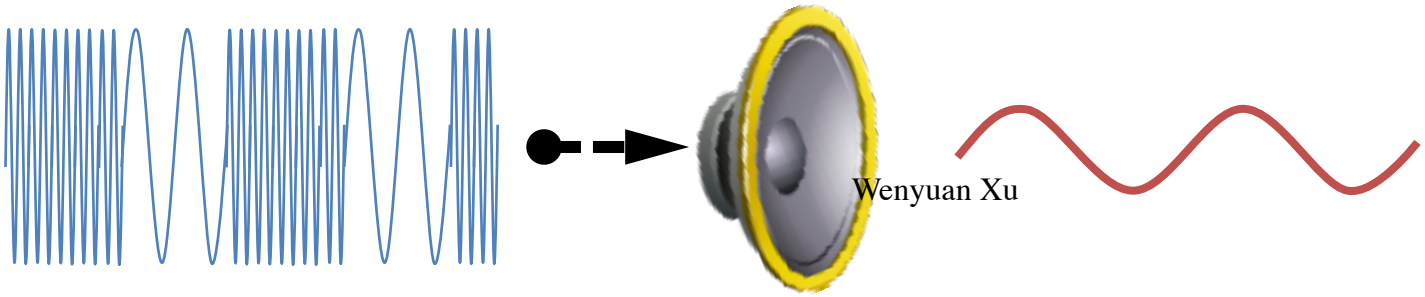
$$\frac{1}{2}\left(\cos(2\omega_m t) + \cos(2\omega_c t) \right)$$

will go through filter

Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



Ultrasonic speaker

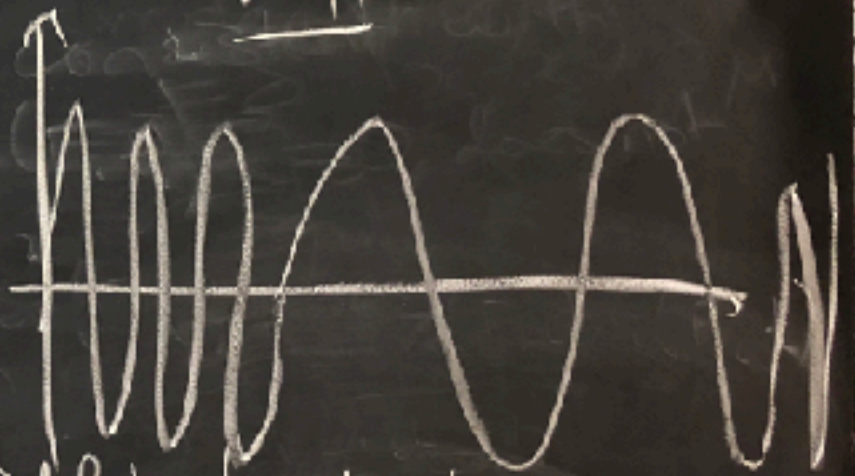
Message : $\sin(\omega_m t)$

Carrier : $\sin(\omega_c t)$

AM

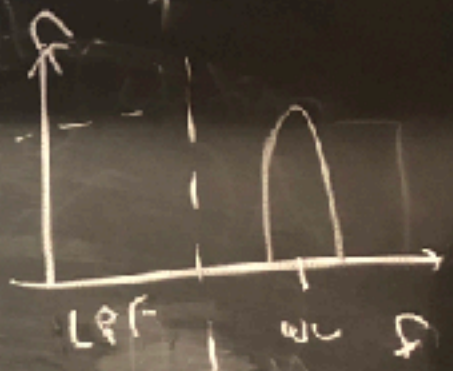
modulate amplitude to convey information

FM



modulate freq to transmit info.

$$S_{FM} = \sin(\omega_c t + \beta \sin(\omega_m t))$$



Amplifier =>

$$S_{FM}^2 = \sin^2(\omega_c t + \beta \sin(\omega_m t))$$

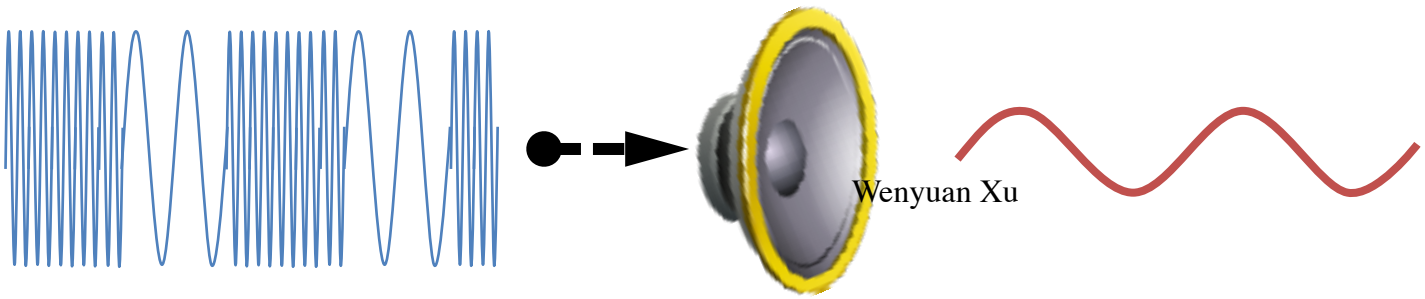
$$= \frac{1}{2}\left(1 - \cos\left(2(\omega_c t + \beta \sin(\omega_m t))\right)\right)$$

=> ever mic can't record sound

Challenges

Frequency modulation

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



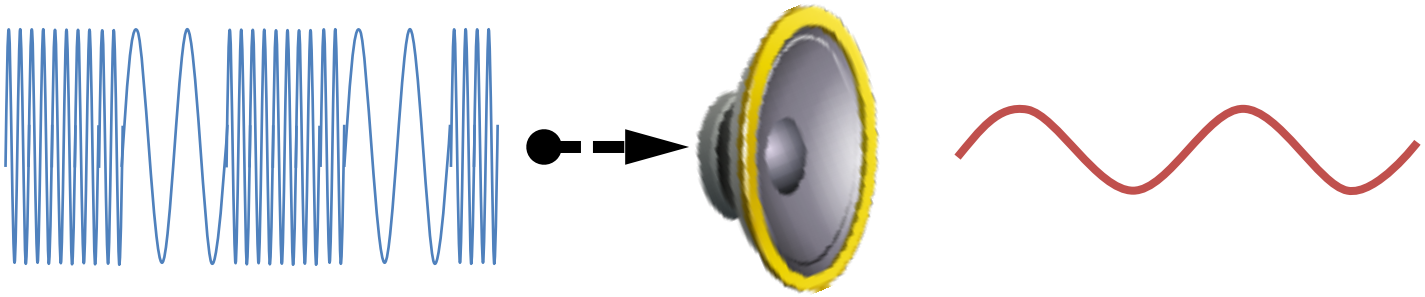
Ultrasonic speaker

$$S_{FM}^2 \sim 1 + \cos(2\omega_c t + \text{ other terms })$$

<u>Problem:</u> microphone can't measure inaudible sound

Solution?

$$S_{FM} = sin\Big(\omega_c t + \beta \sin(\omega_m t)\Big)$$



Ultrasonic speaker

Add another speaker

How do we structure its signal?

$$S_{Rx} = \sin(\omega_c t + \beta \sin(\omega_m t))$$

$$+ \sin(\omega_c t)$$

$$S_{Rx}^2 = \text{"higher freq terms"} + \sin(\beta \sin \omega_m t)$$

$\Rightarrow$ inaudible voice command

Talk outline

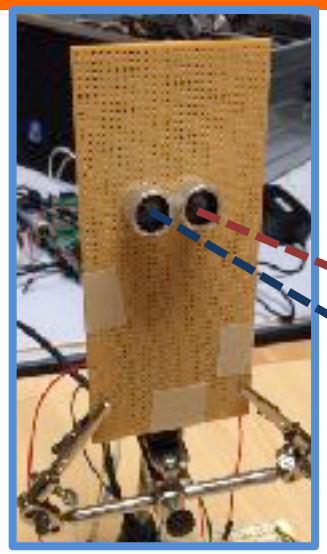
① Microphone Overview

② System Design

③ Challenges

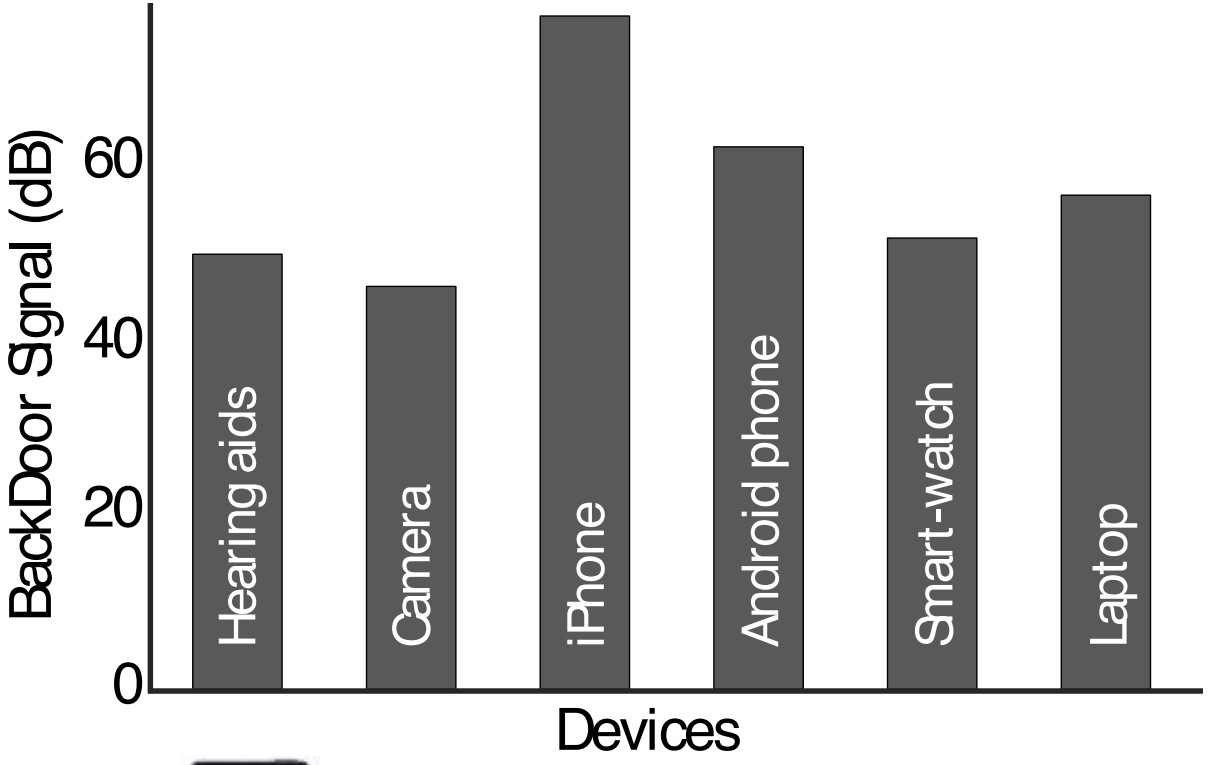
④ Evaluation

Hardware generalizability



40 kHz

50 kHz



Hearing Aid

Camera

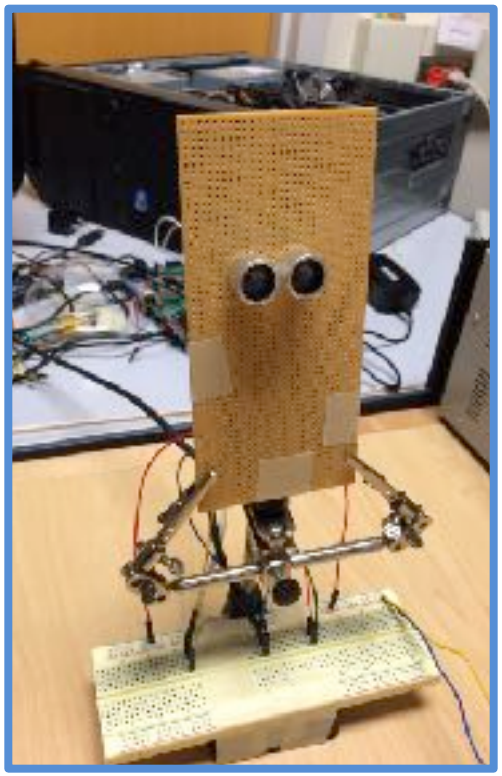
iPhone

Android phone

Smartwatch

Laptop

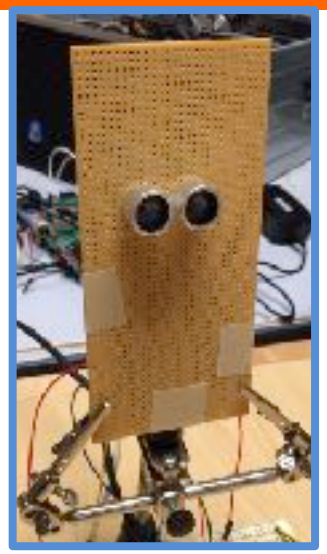
Implementation



Communication prototype

Jammer prototype

Communication performance

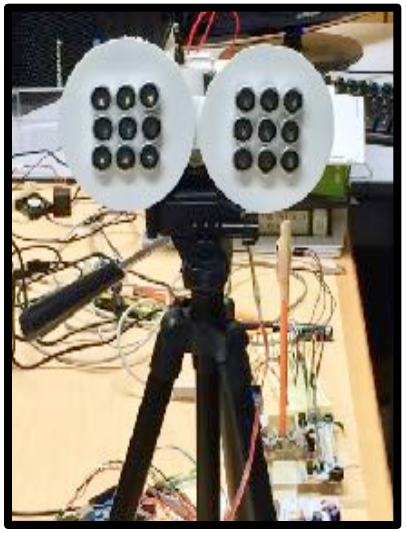


FM data packets

4kbps
up to 1 meter

More power can increase the distance

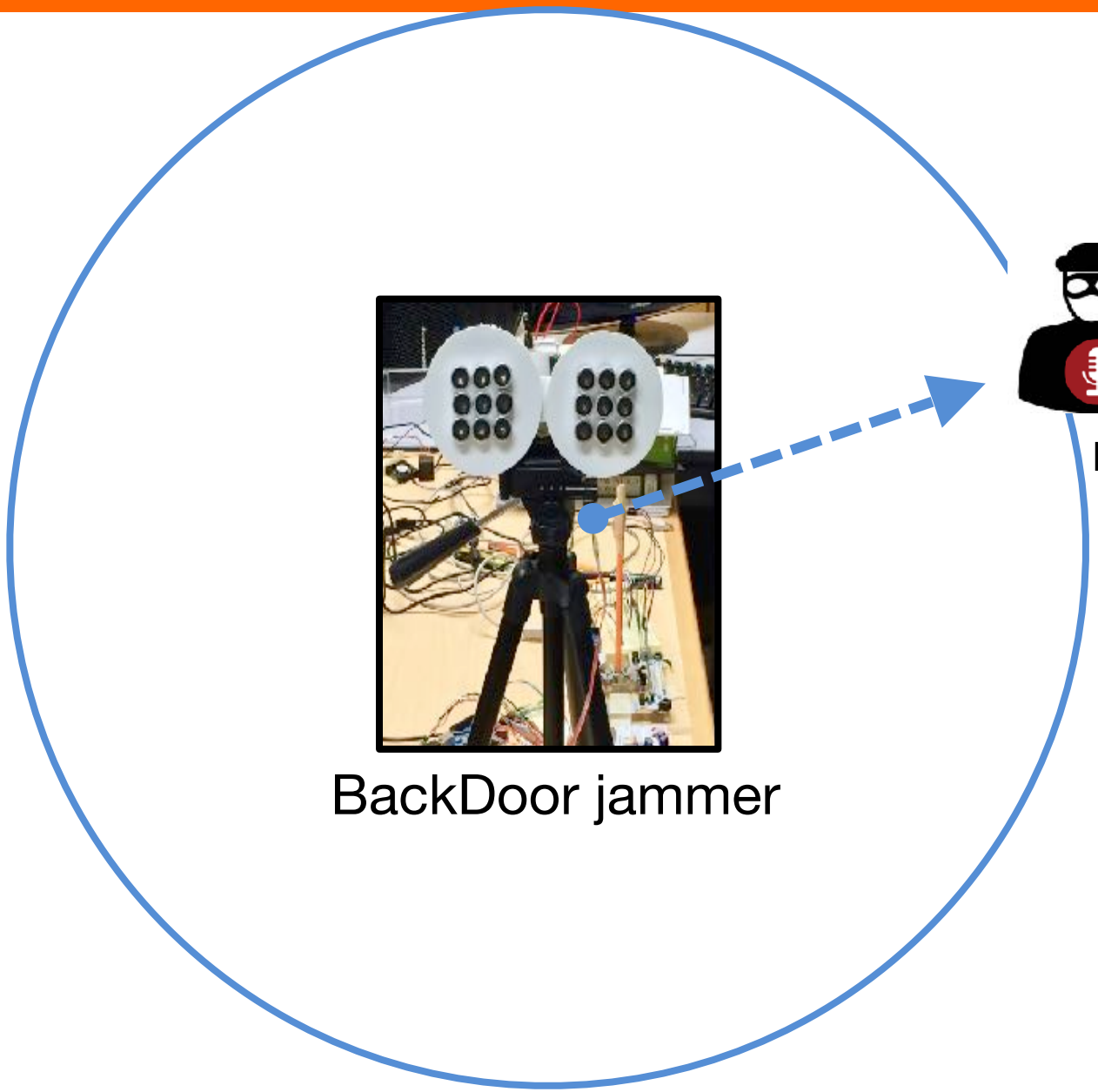
Jamming performance



BackDoor jammer

Spy microphone

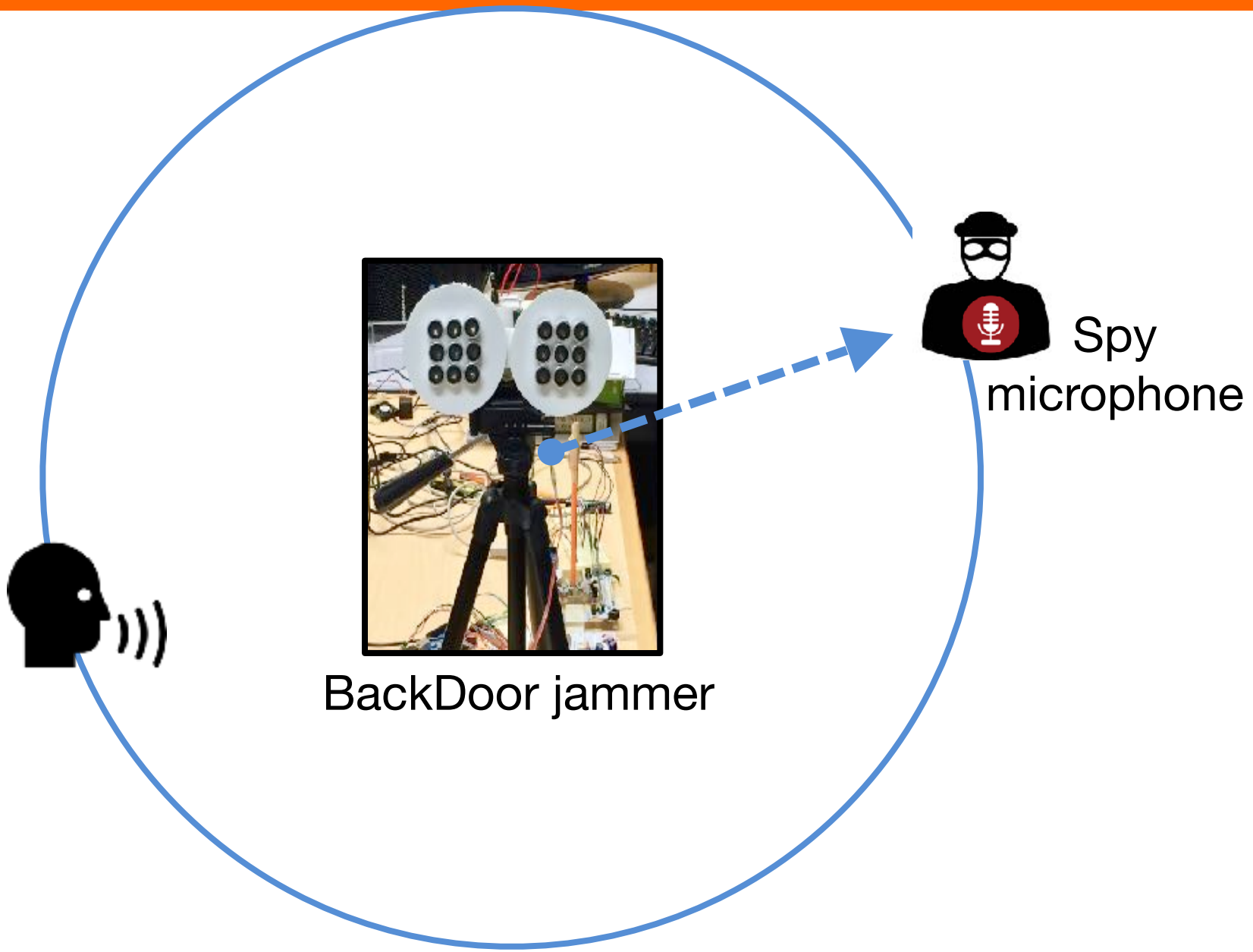
Jamming performance



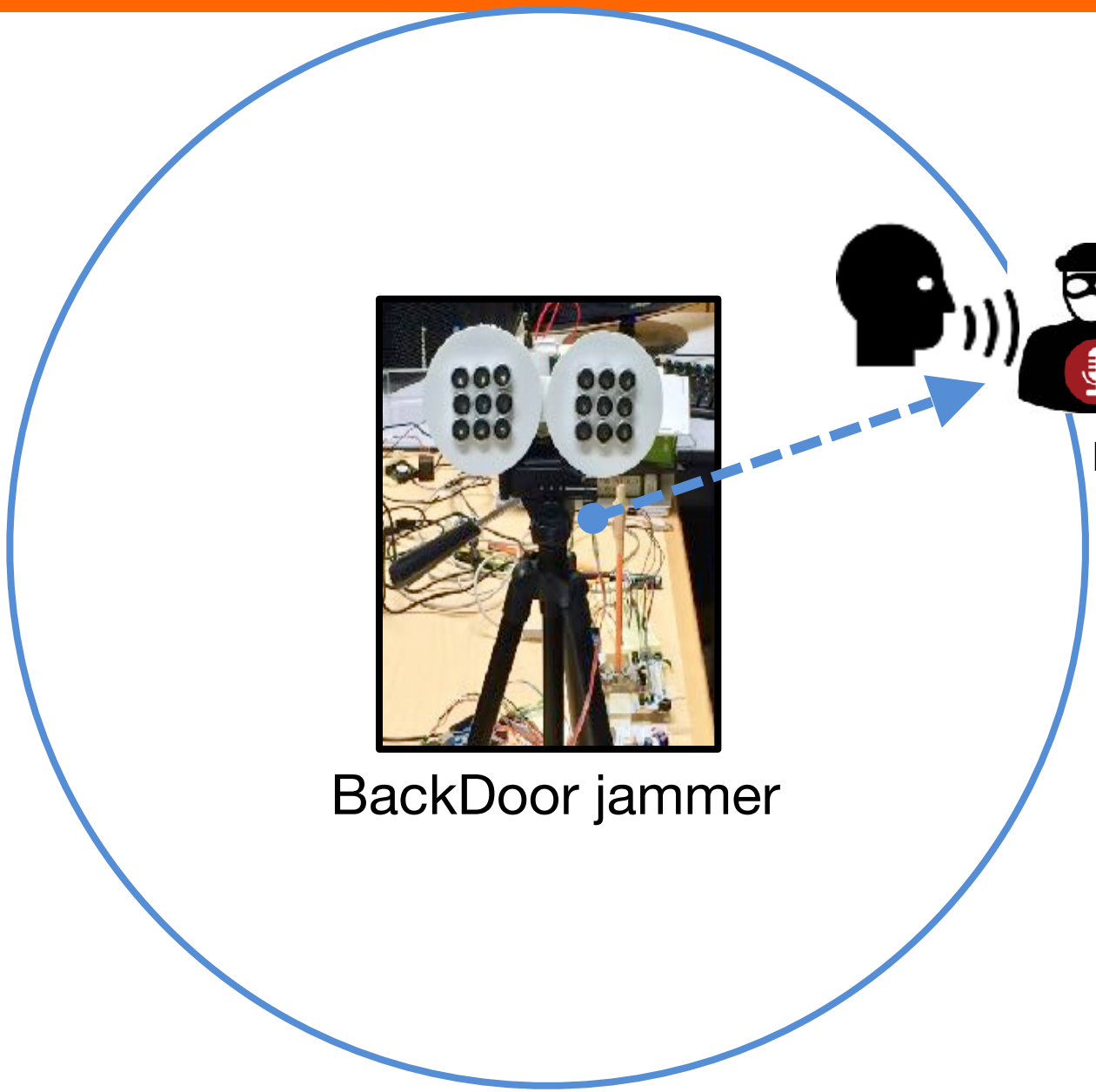
BackDoor jammer

Spy
microphone

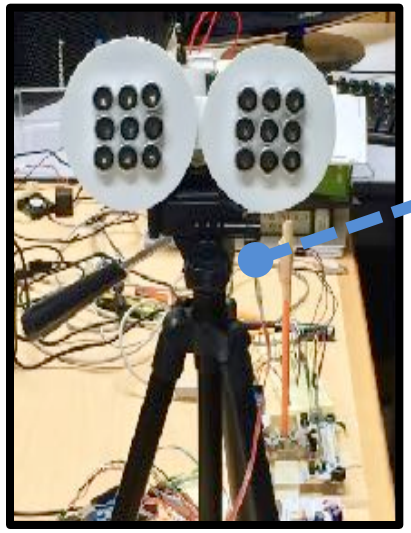
Jamming performance



Jamming performance



Jamming performance

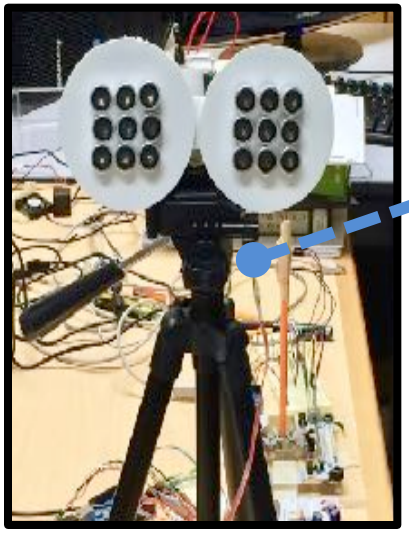


BackDoor jammer

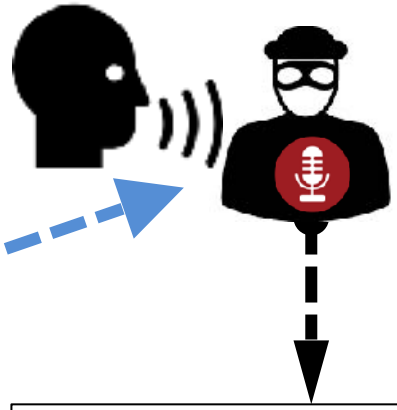
Spy microphone

Jamming performance

2000 spoken words

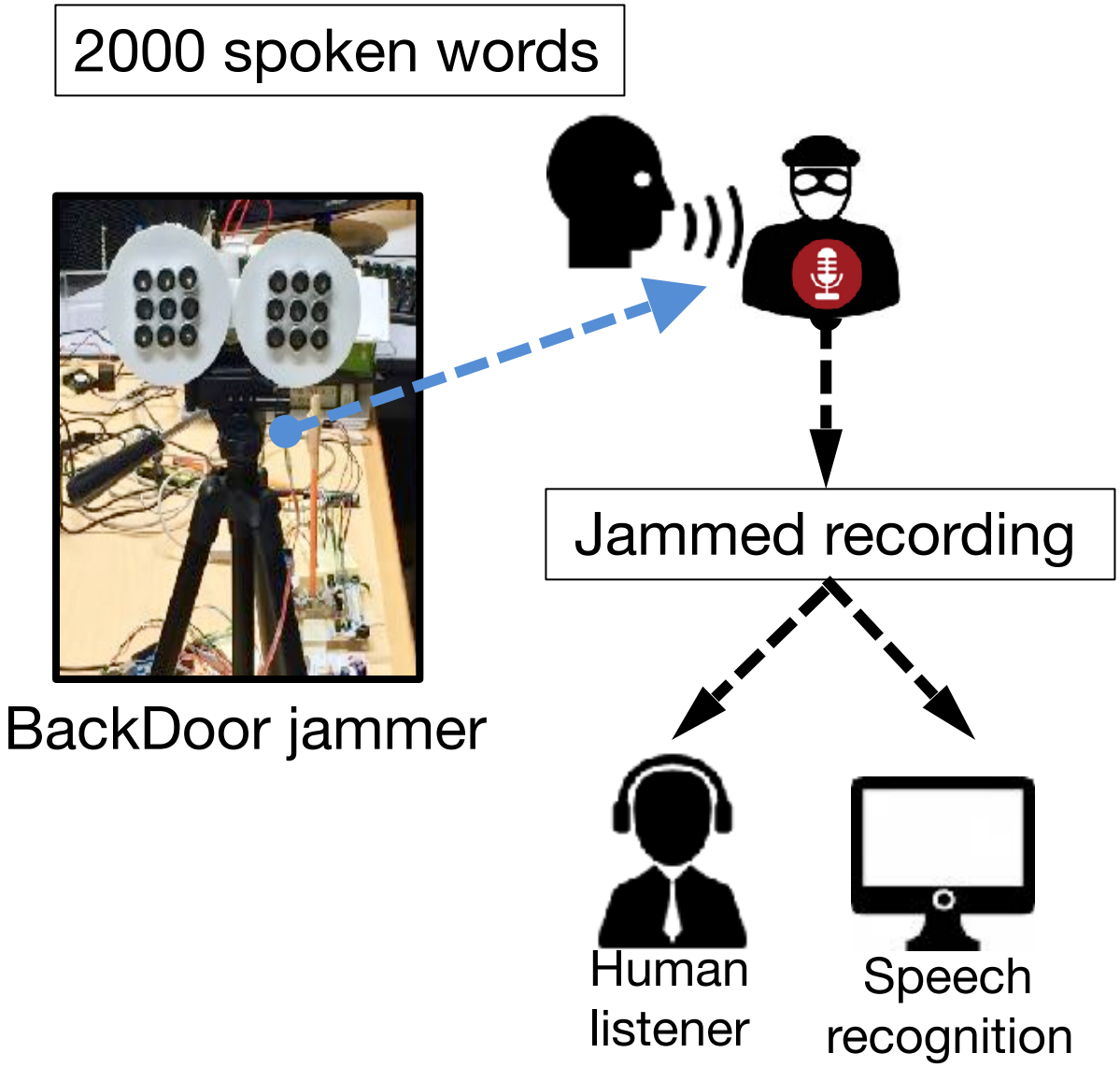


BackDoor jammer

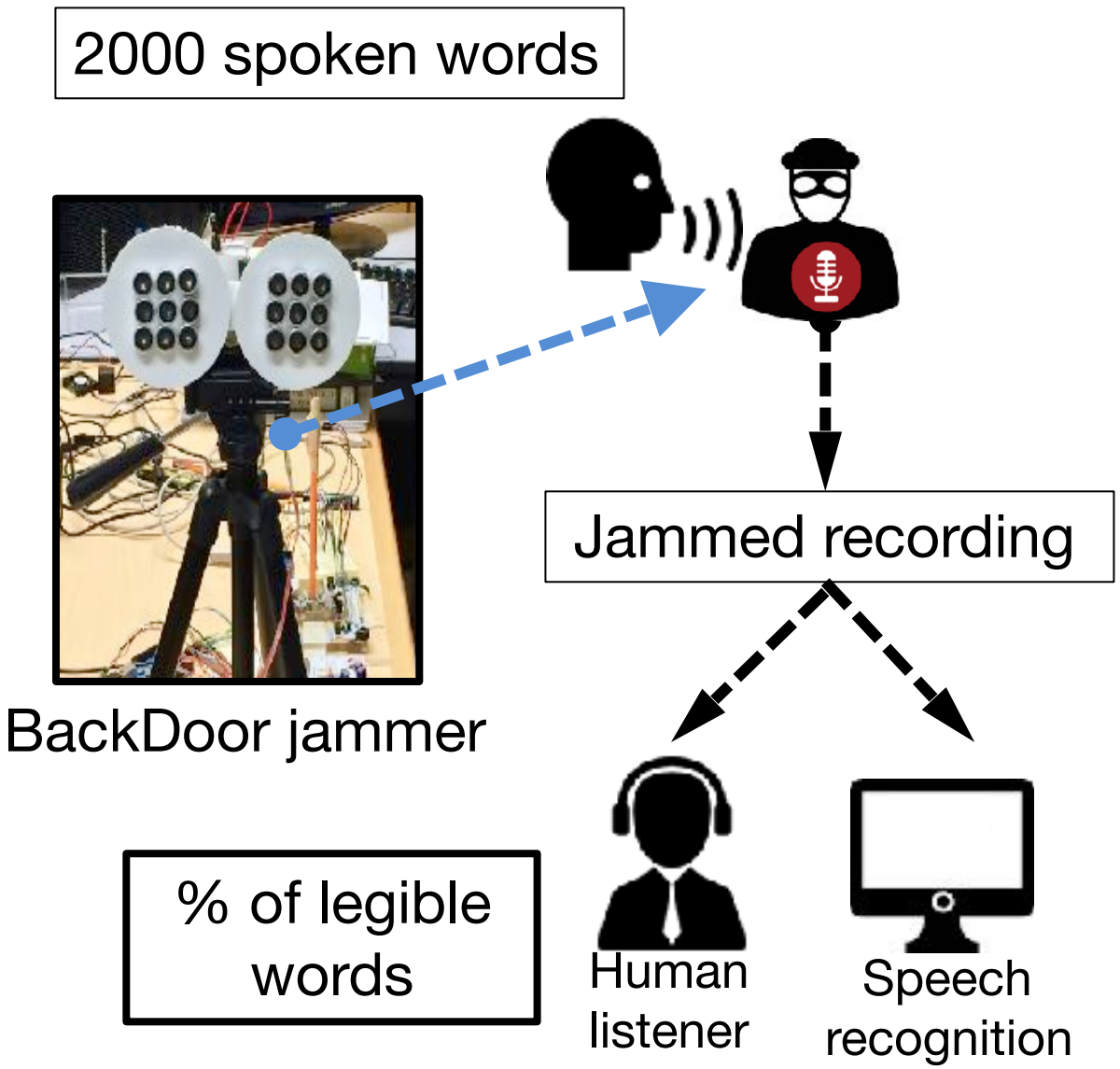


Jammed recording

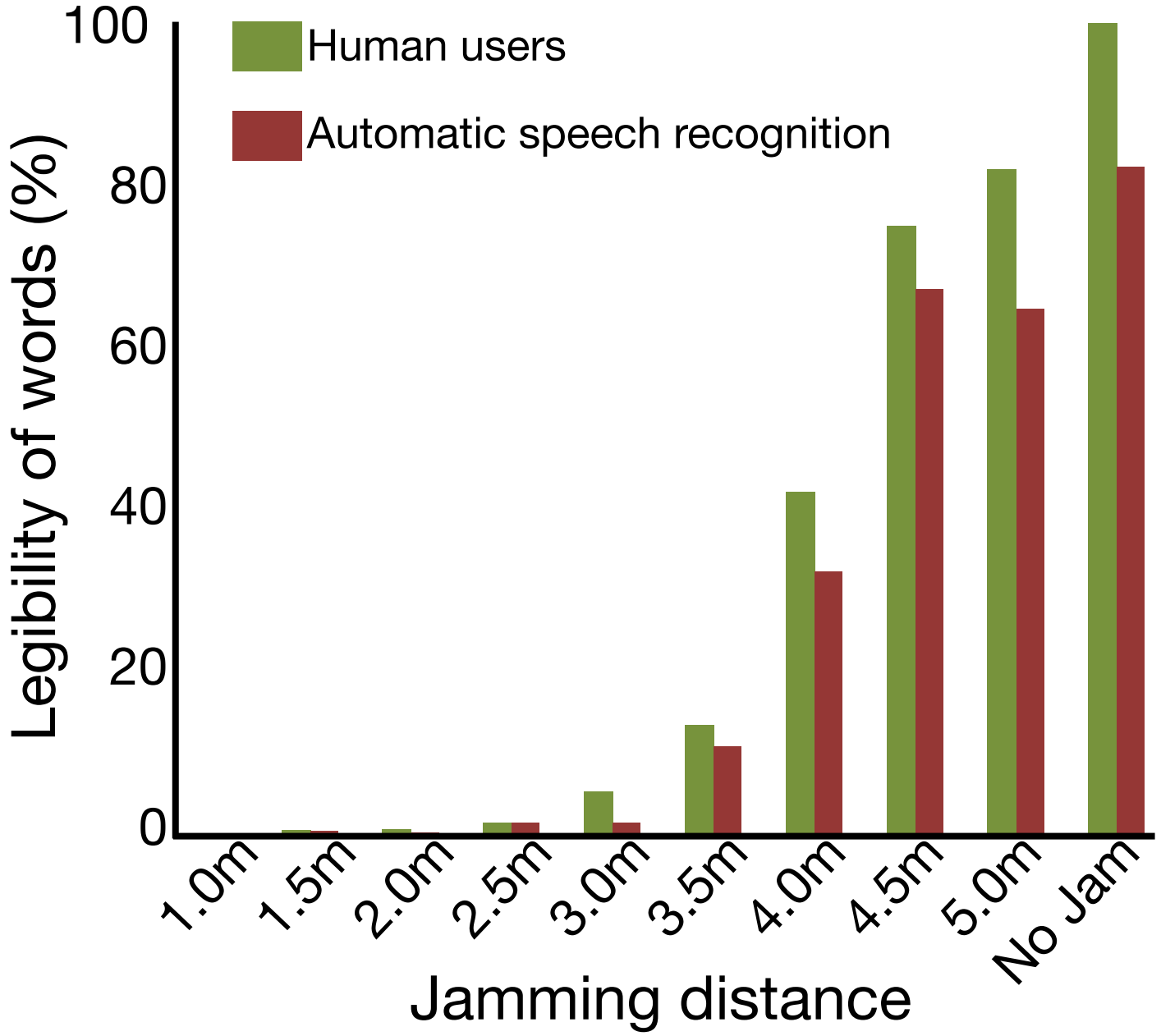
Jamming performance



Jamming performance



Jamming performance



How would you design a system to secure against this attack?

Summary

- IoT Security: both digital and analog
- "Sensor" security & attacks:
  - Mobile acoustic attacks (inaudible voice commands)
  - Analog Sensor attacks (on MEMS accelerometers)
  - Drone Security (Spoofing GPS)
  - Medical Security (Hacking Pacemakers)
- Modulation schemes
  - AM
  - FM
  - Inter-modulation
- Fundamentals have implications beyond IoT (e.g., Cuban "acoustic attack")