http://www.mit.edu/~fadel/courses/MAS.s60/index.html

MAS.S60

# How to Wirelessly Sense Almost Anything

## Lecture 6: Hacking Sensors

Lecturers
Fadel Adib (fadel@mit.edu)
Aline Eid (alineeid@mit.edu)
TA
Tara Boroushaki (tarab@mit.edu)

# This Week in Wireless Sensing

**MIT Technology Review**
22 hrs ·

NEW: Elon Musk said no thanks to using his mega-constellation for navigation. Researchers went ahead anyway.

TECHNOLOGYREVIEW.COM

**Starlink signals can be reverse-engineered to work like GPS—whether SpaceX likes it or not**

# How to Wirelessly Sense Almost Anything

sensing the physical world & transmitting data wirelessly

sensing via the wireless signals themselves

combine principles from both to hack physical sensors

# Objectives of Today's Lecture

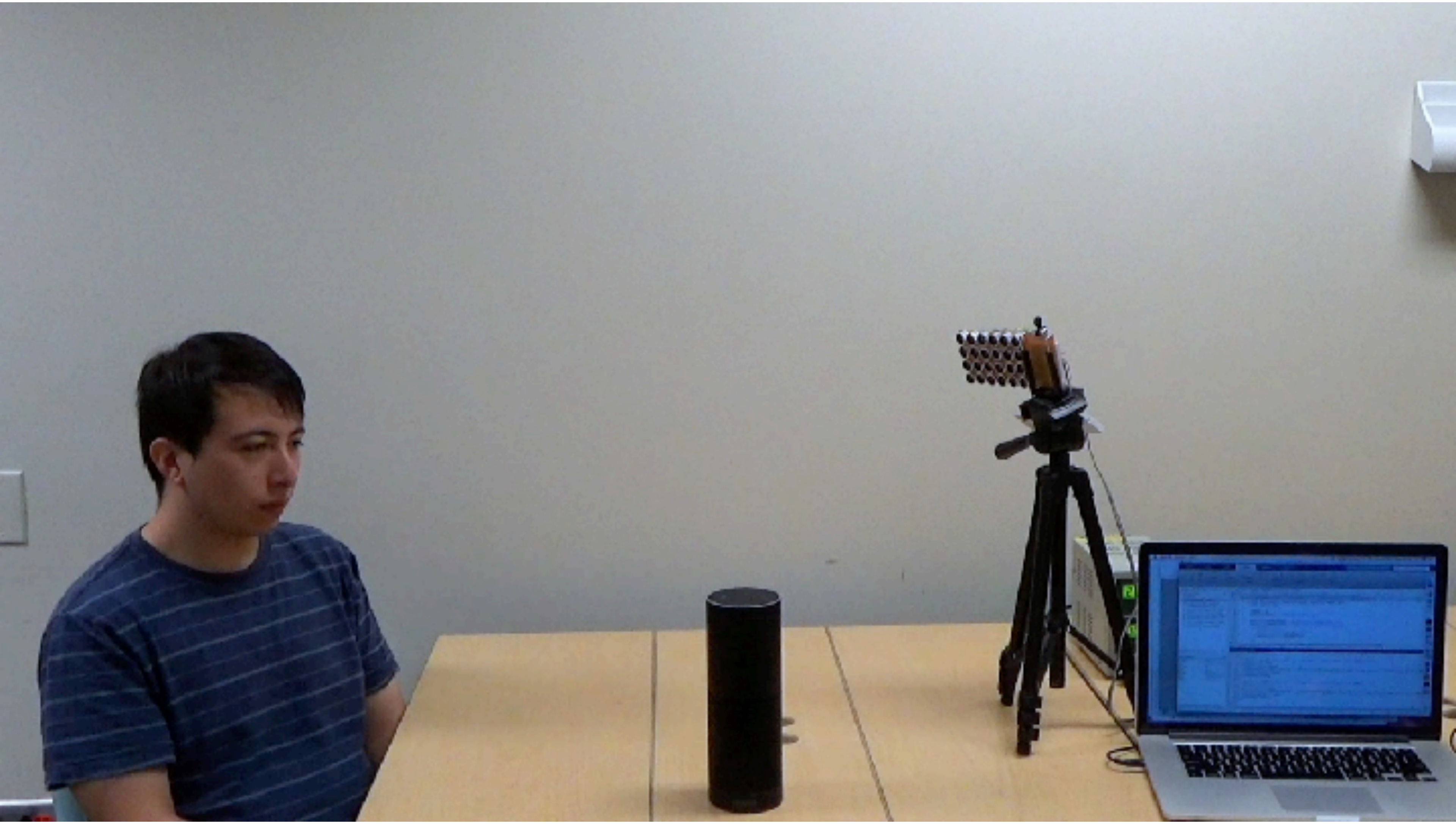
Learn the fundamentals, applications, and implications of **hacking physical sensors**

1. What are the general principles of injection attacks into physical sensors?
2. What are some examples of injection attacks: GPS, pacemakers, Alexa/Google Home/Fitbit?
3. How do acoustic attacks work on Alexa/Google Home/etc?
4. How can we protect against physical sensor attacks?

**Discuss projects end to lecture**

# Mobile Security

Inaudible Voice Commands



# Light Commands

## Hacking using Laser

UEC TOKYO

CSE COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF MICHIGAN

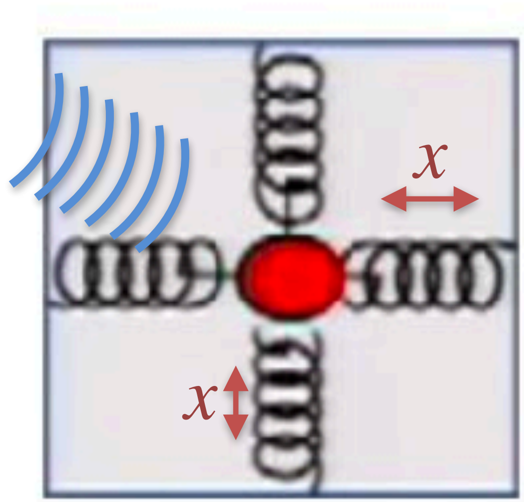
LIGHT
COMMANDS

# Analog Sensor Security

Acoustic Attacks on MEMS Accelerometers


TITANIUM BULLET TWEETER
PYRAMID

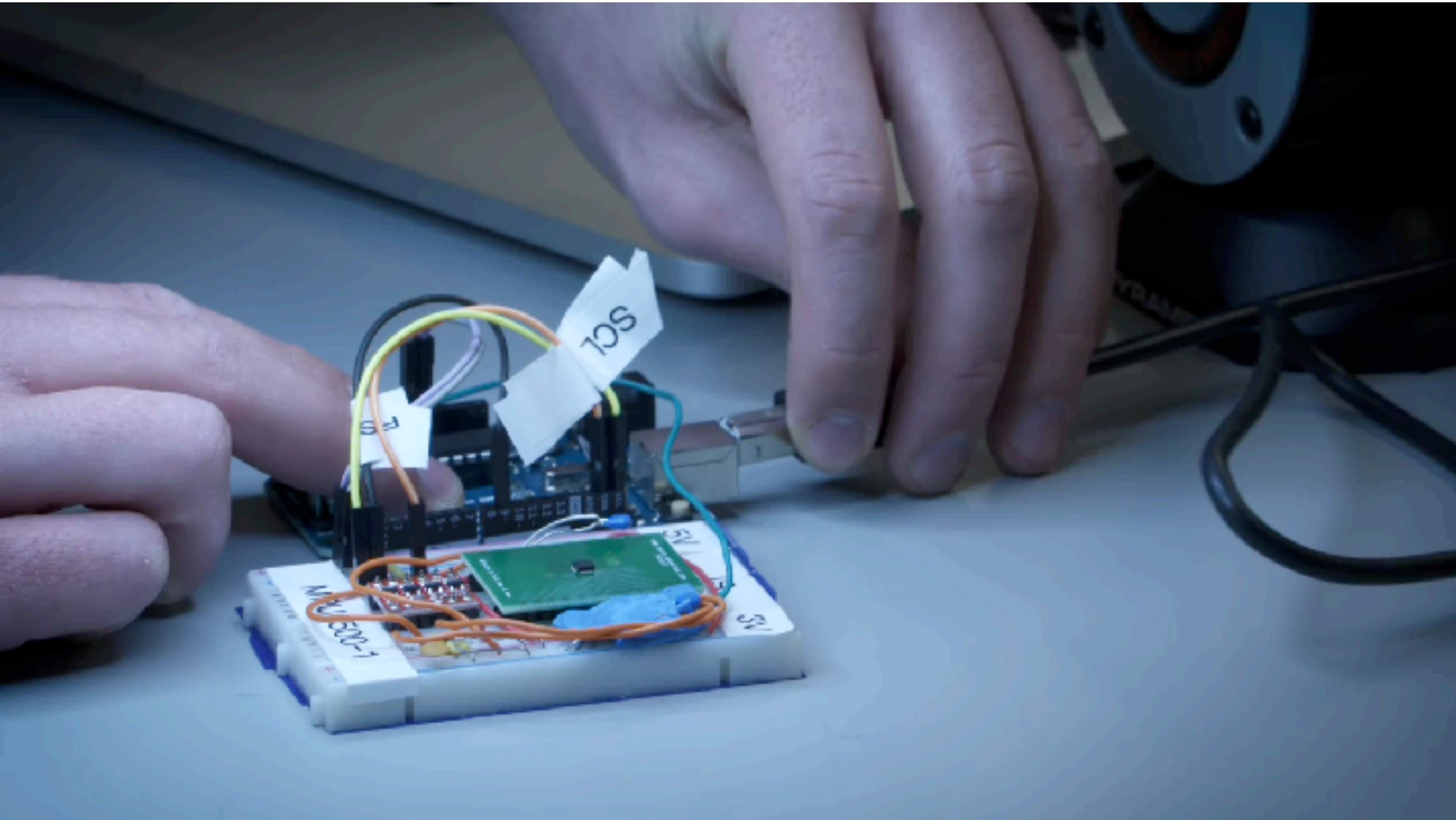
Acoustic
“pressure” waves




$$F = ma = kx$$

acceleration

measure
displacement

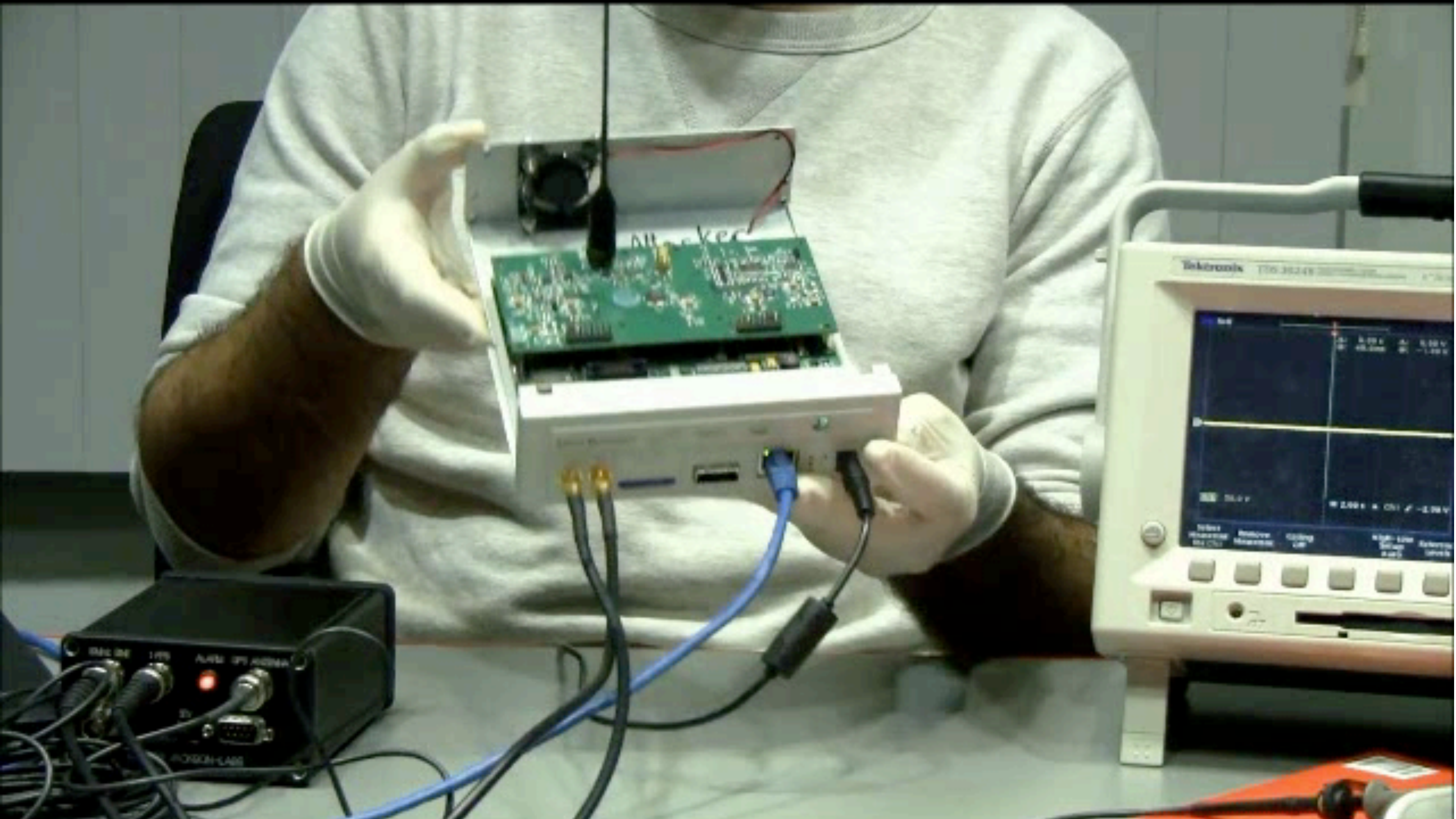

SCL
5V
3V

# Drone Security

Spoofing GPS Signals

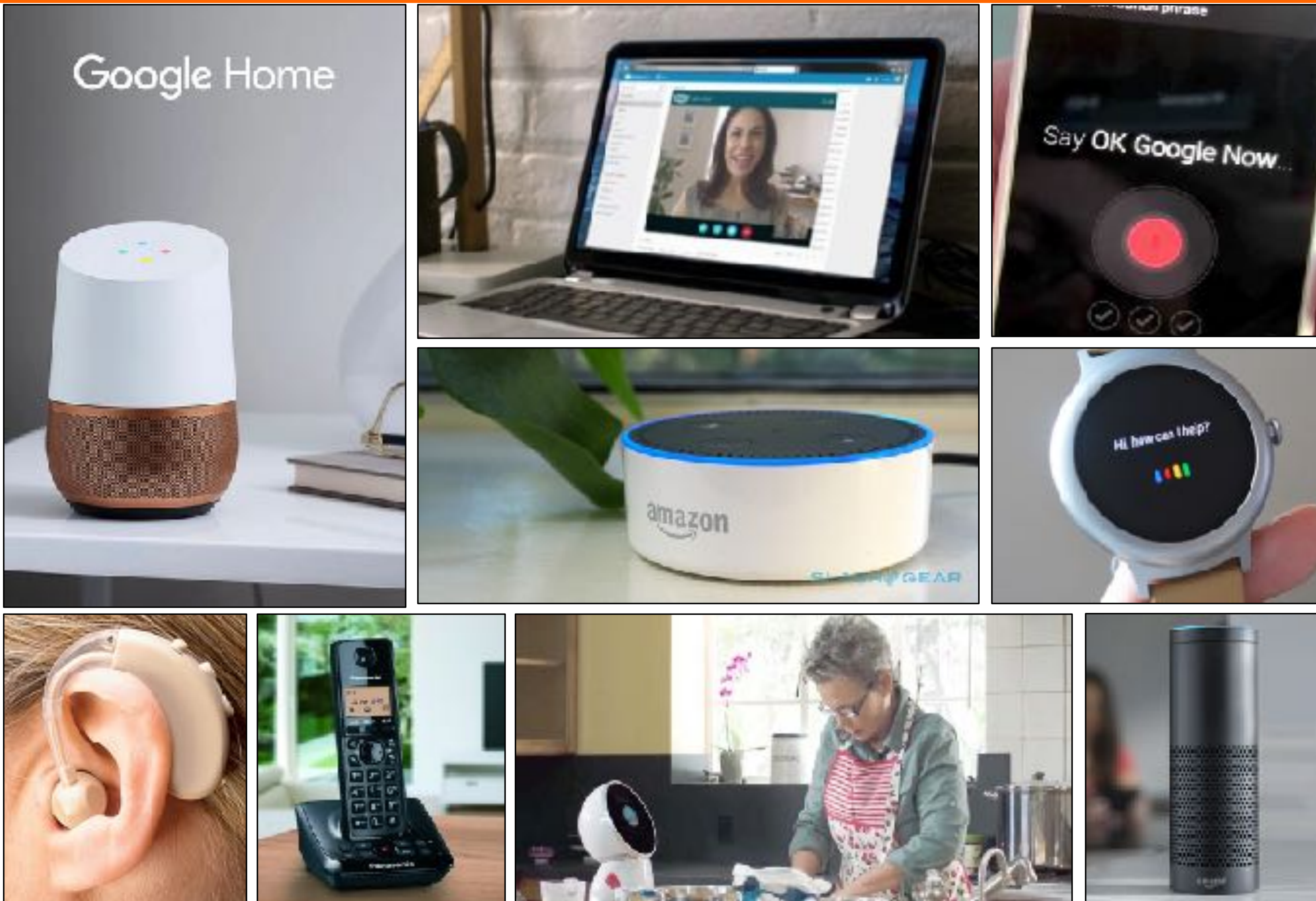
# Pacemaker Security

Wireless Control of Pacemaker

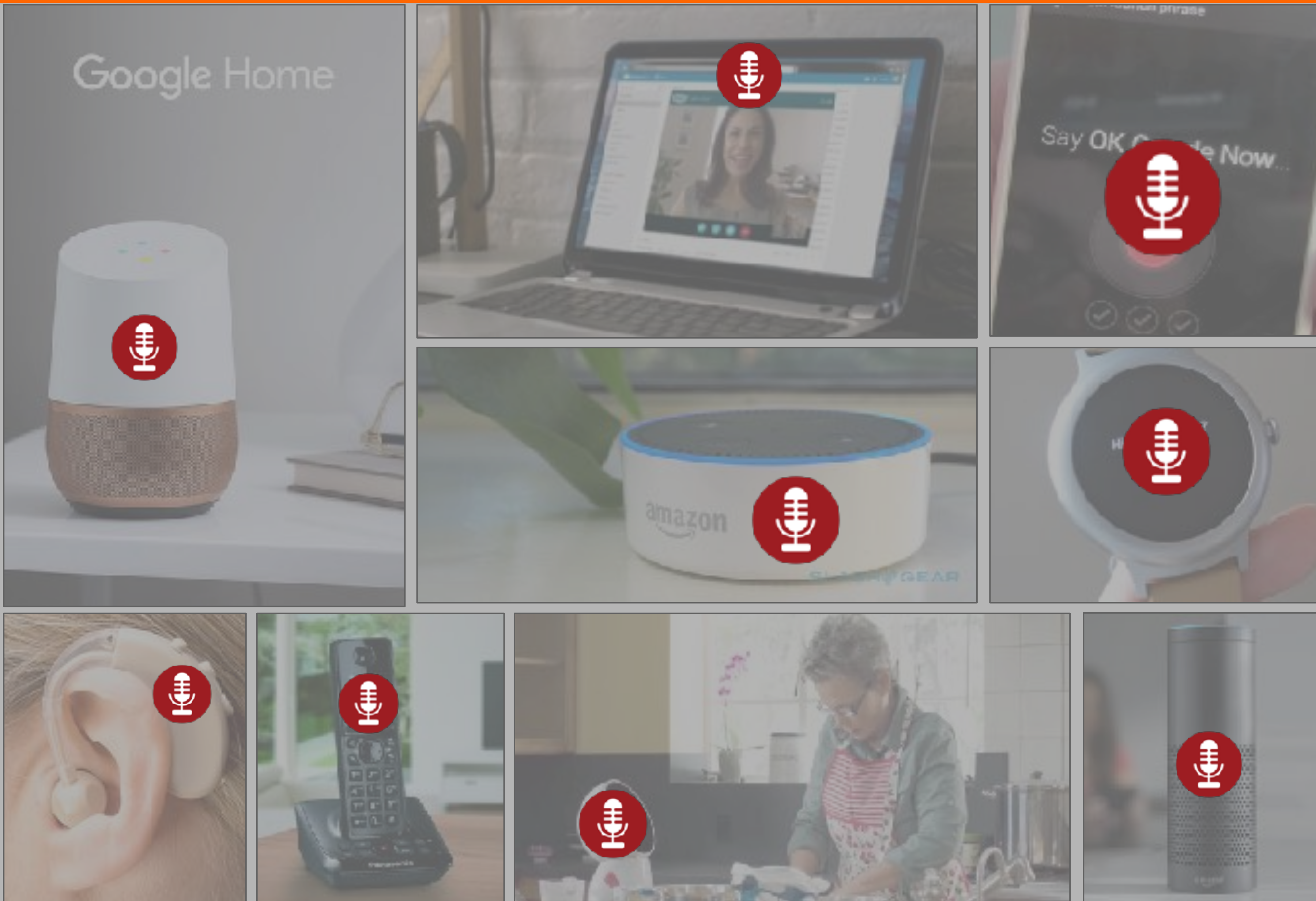

Tektronix
GPS ANTENNA

# BackDoor: Making Microphones Hear Inaudible Sounds

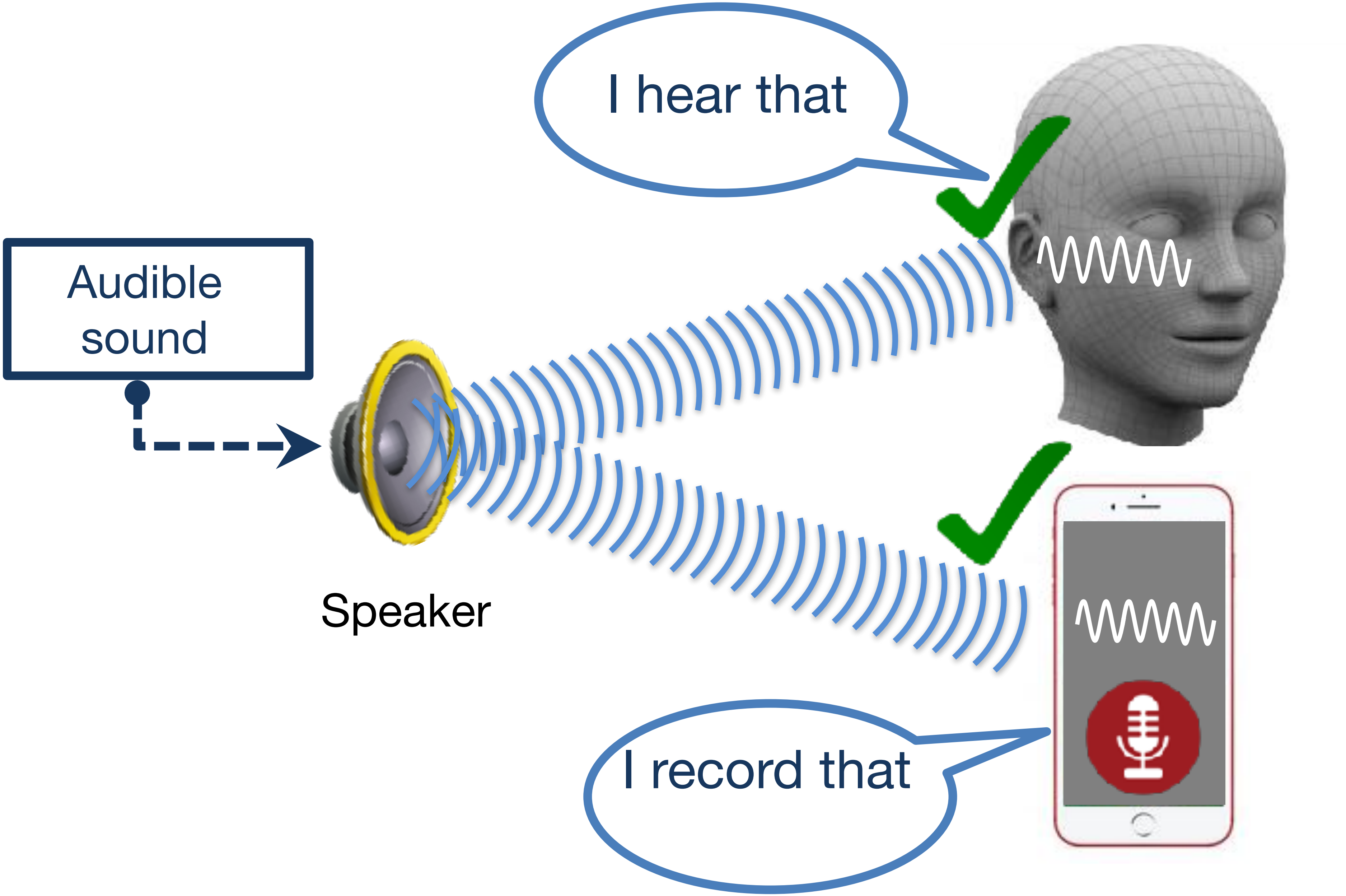
# Microphones are everywhere



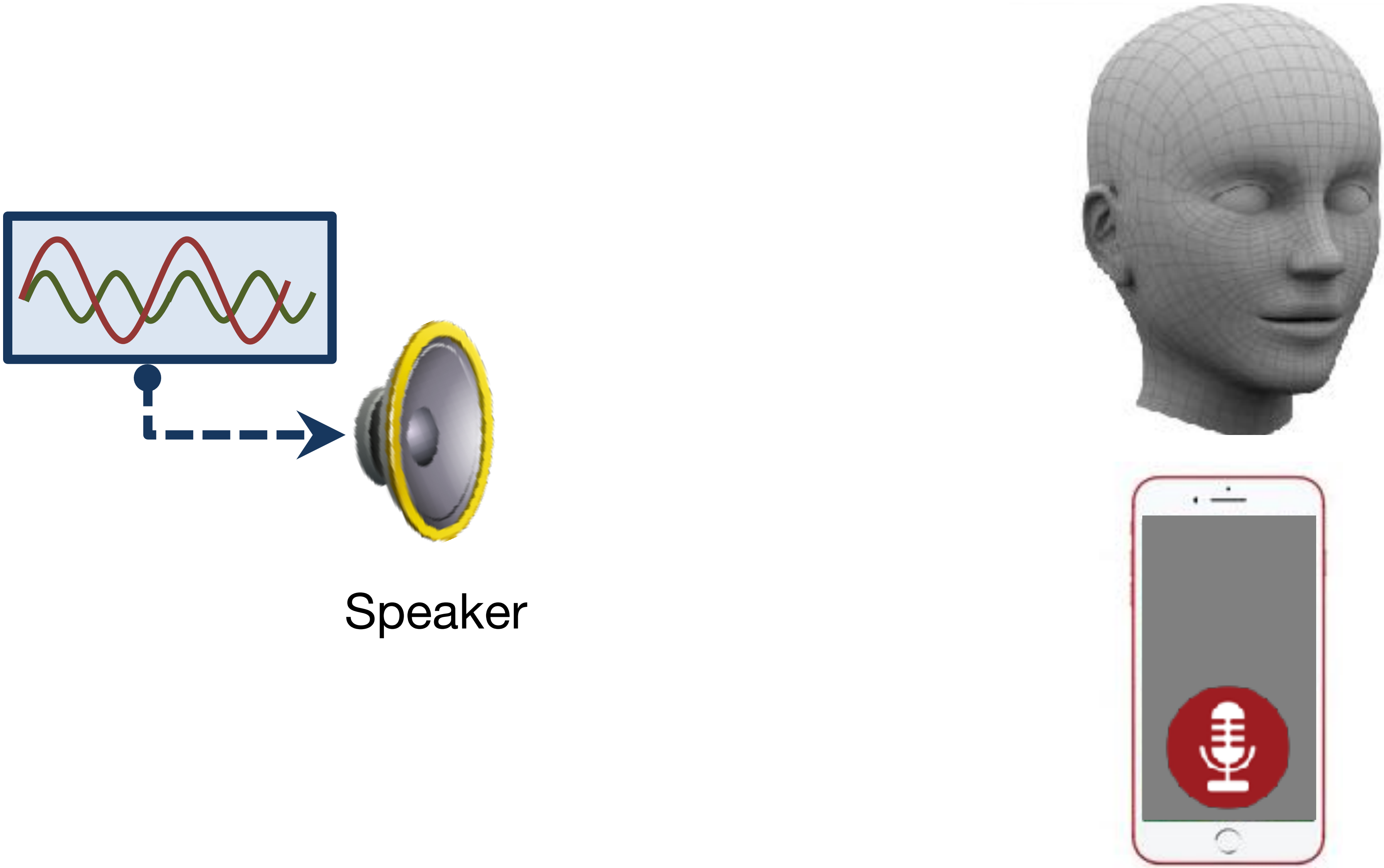
# Microphones are everywhere



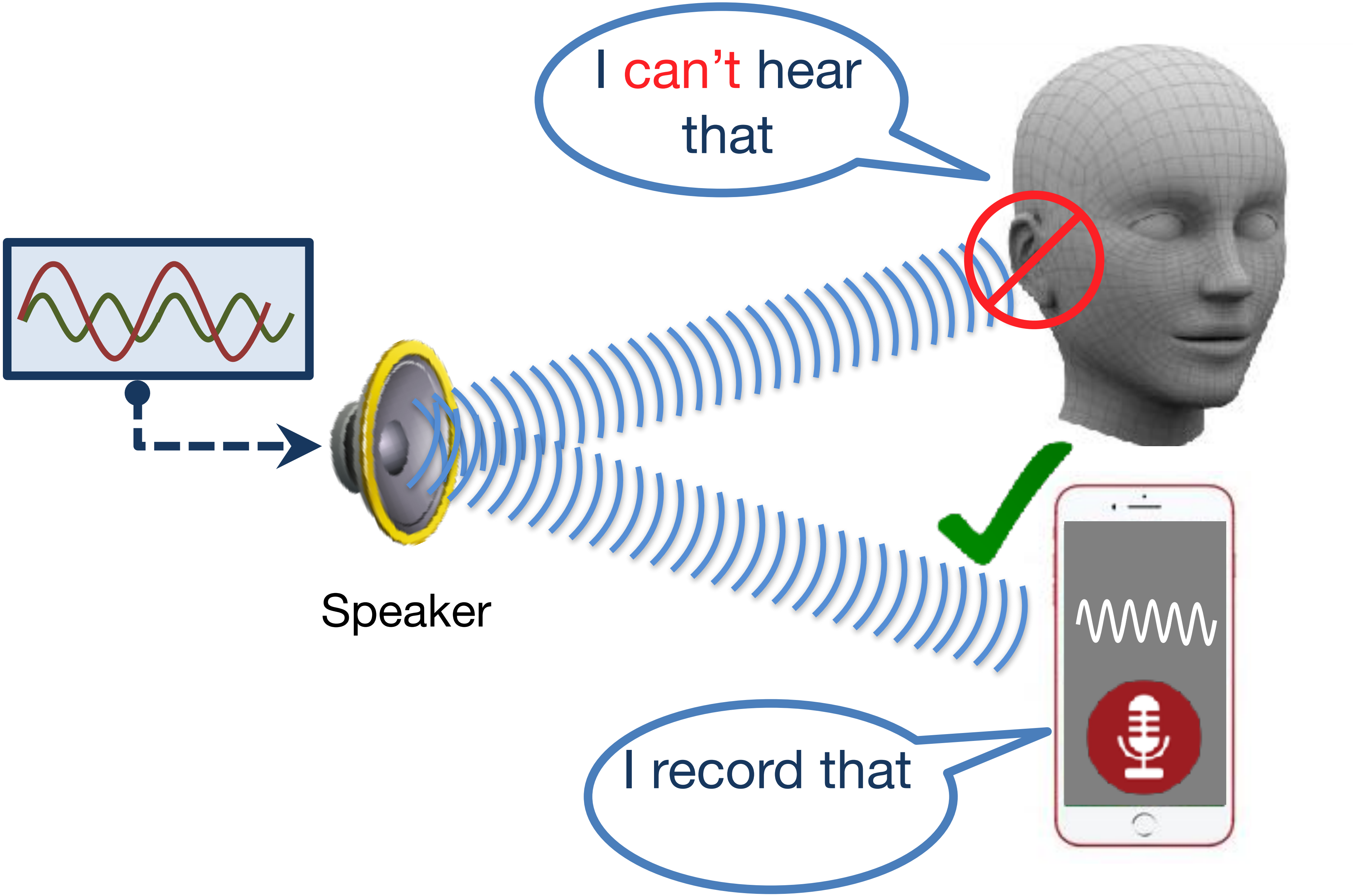
# Microphones record audible sounds



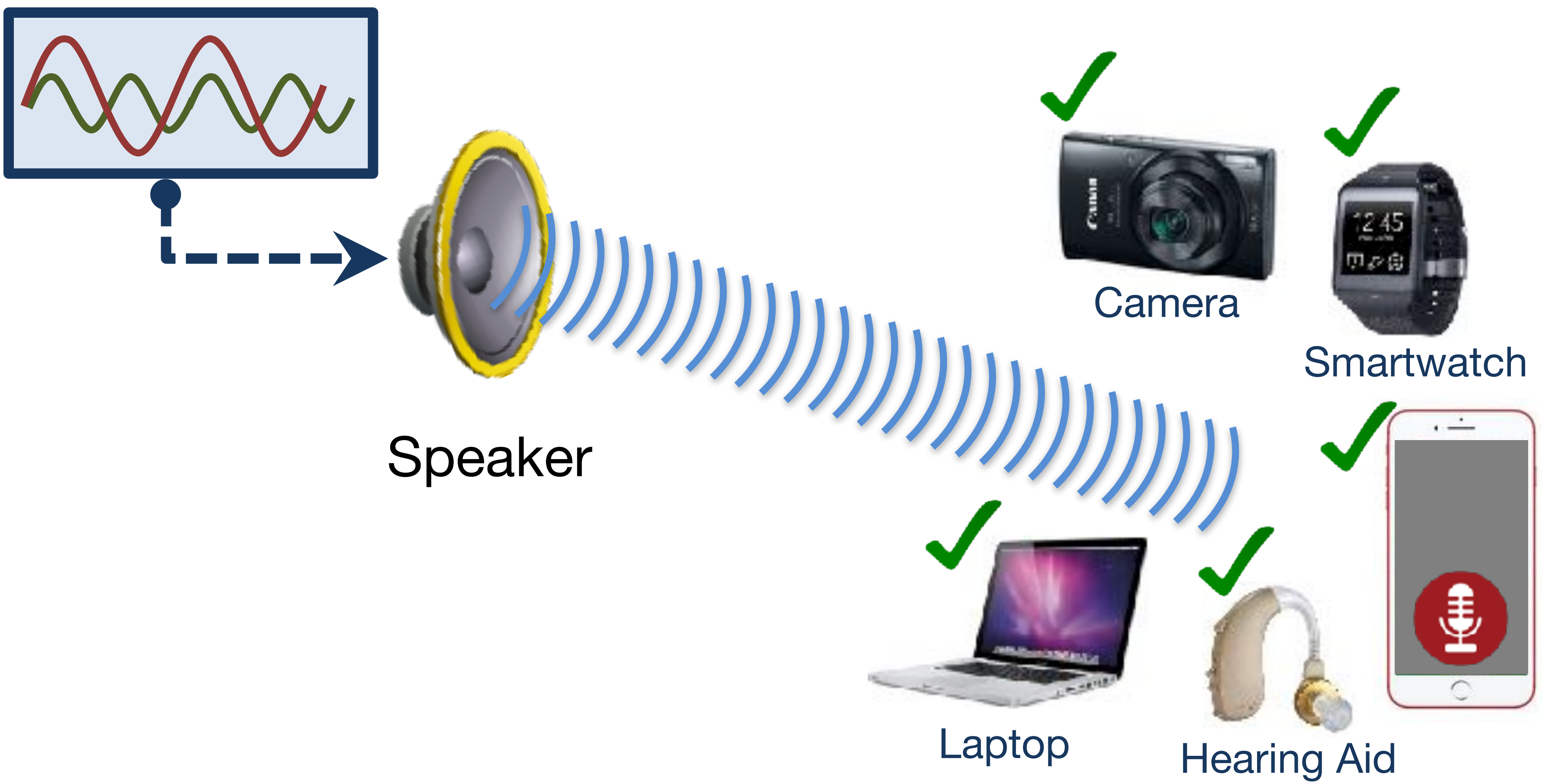
# Inaudible, but recordable !



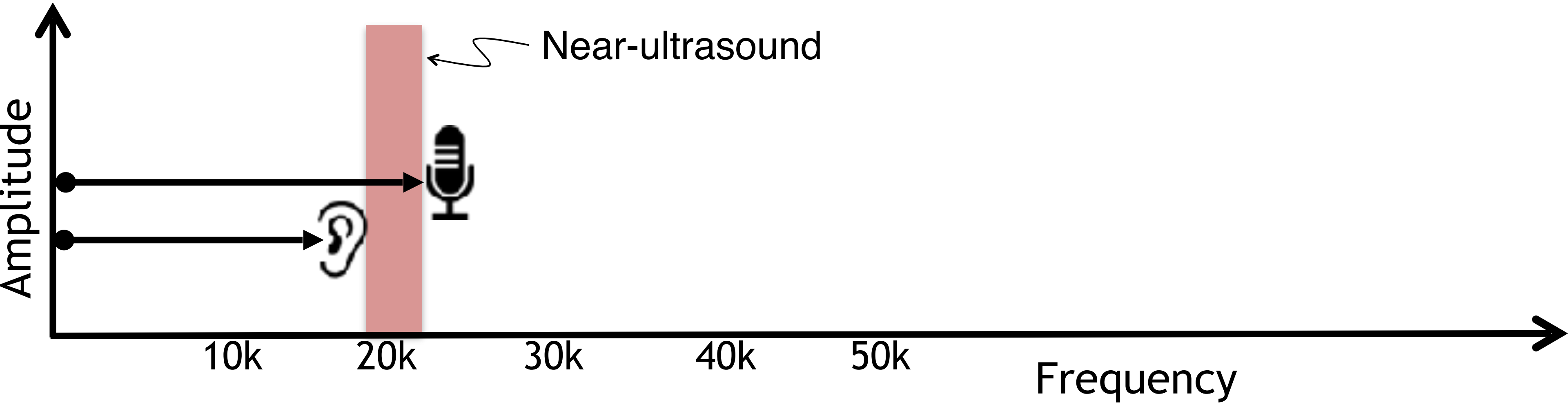
# Inaudible, but recordable !



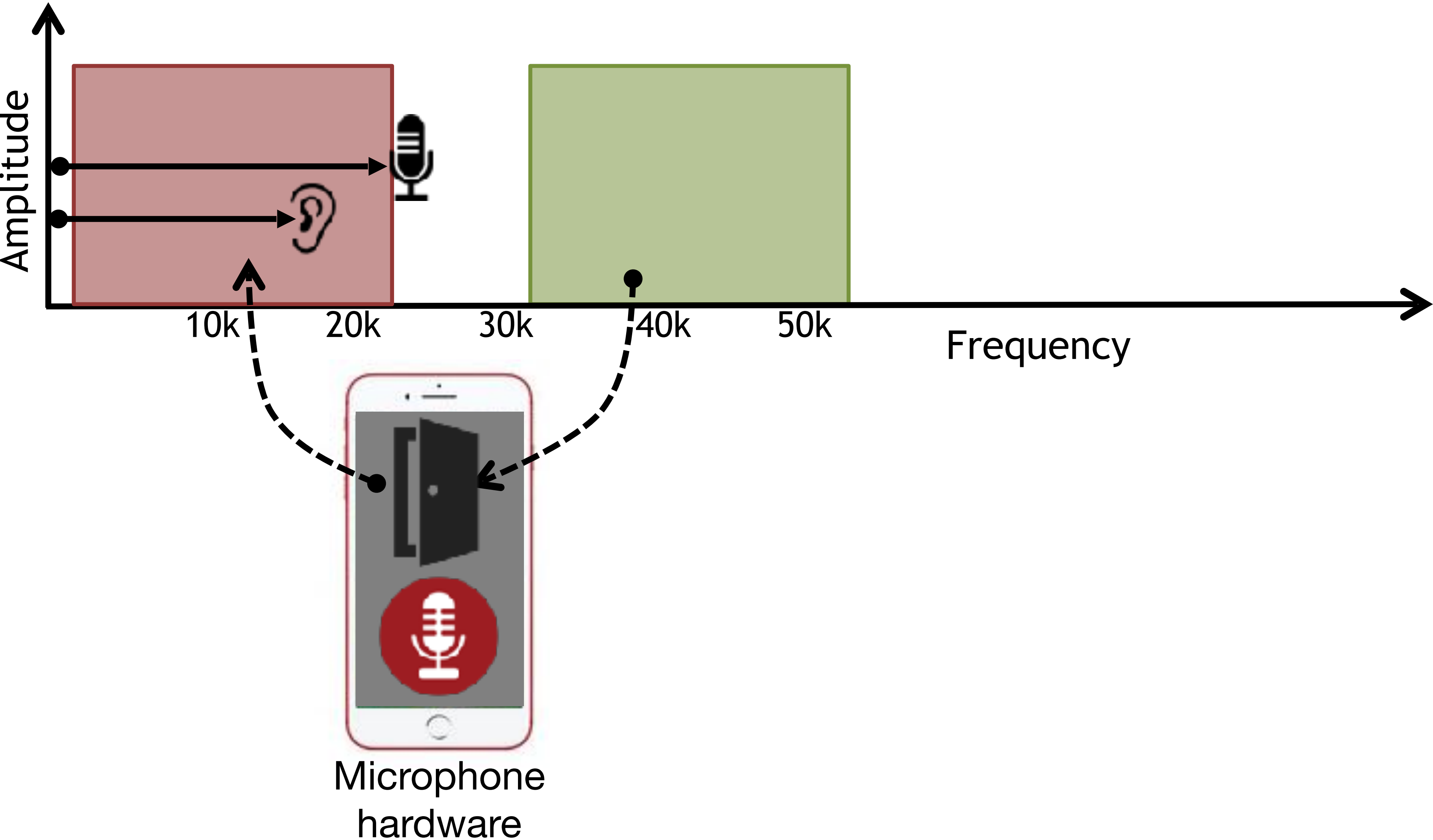
# Works with unmodified devices



# It's not "near-ultrasound"



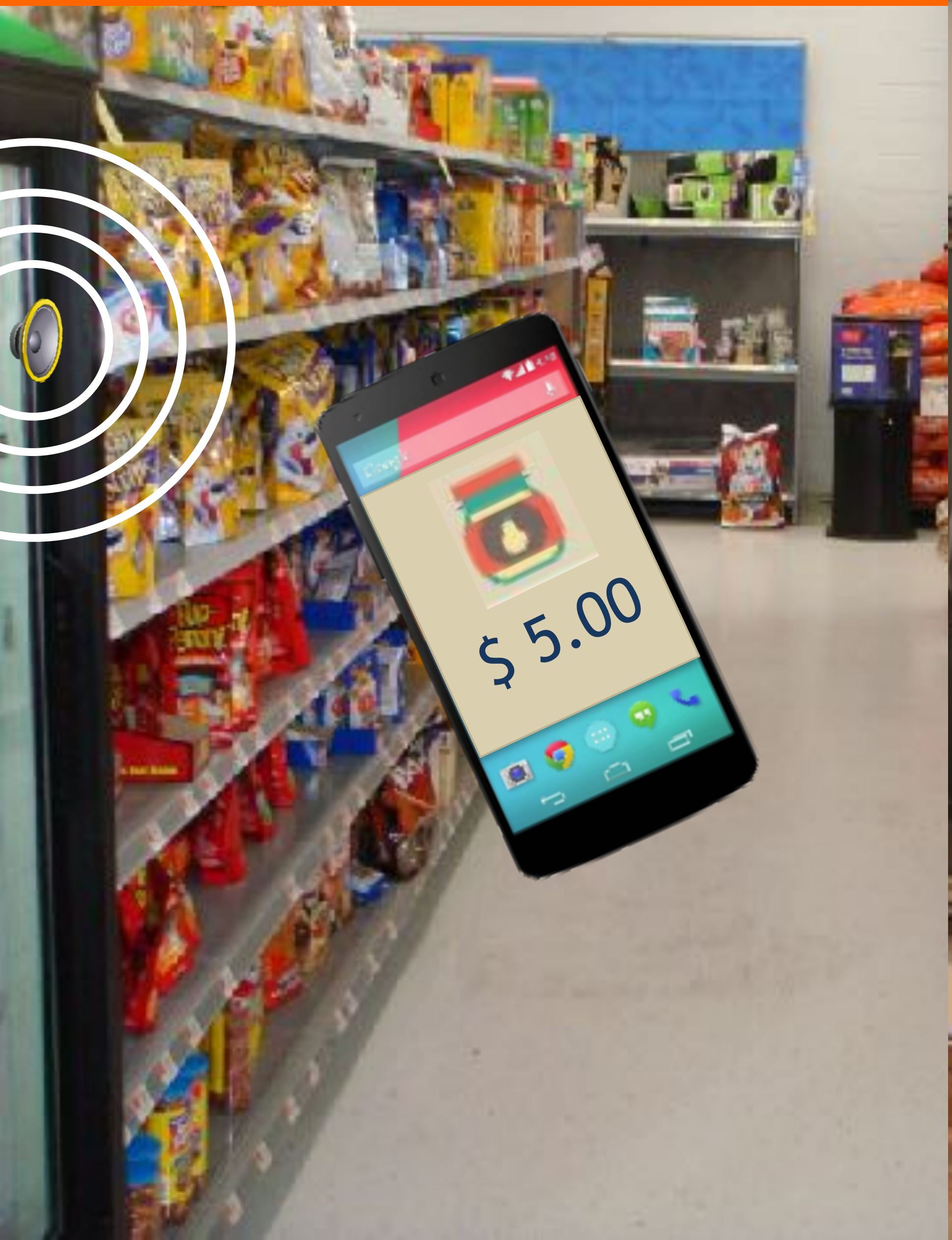
# Exploiting fundamental nonlinearity



# What can we do with it?

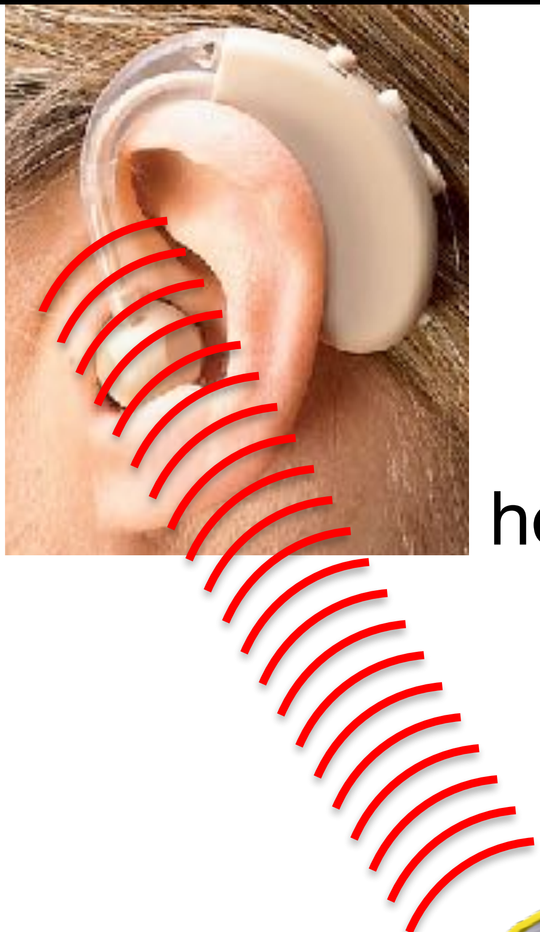
# Application: Acoustic jammer

# Application: Acoustic communication



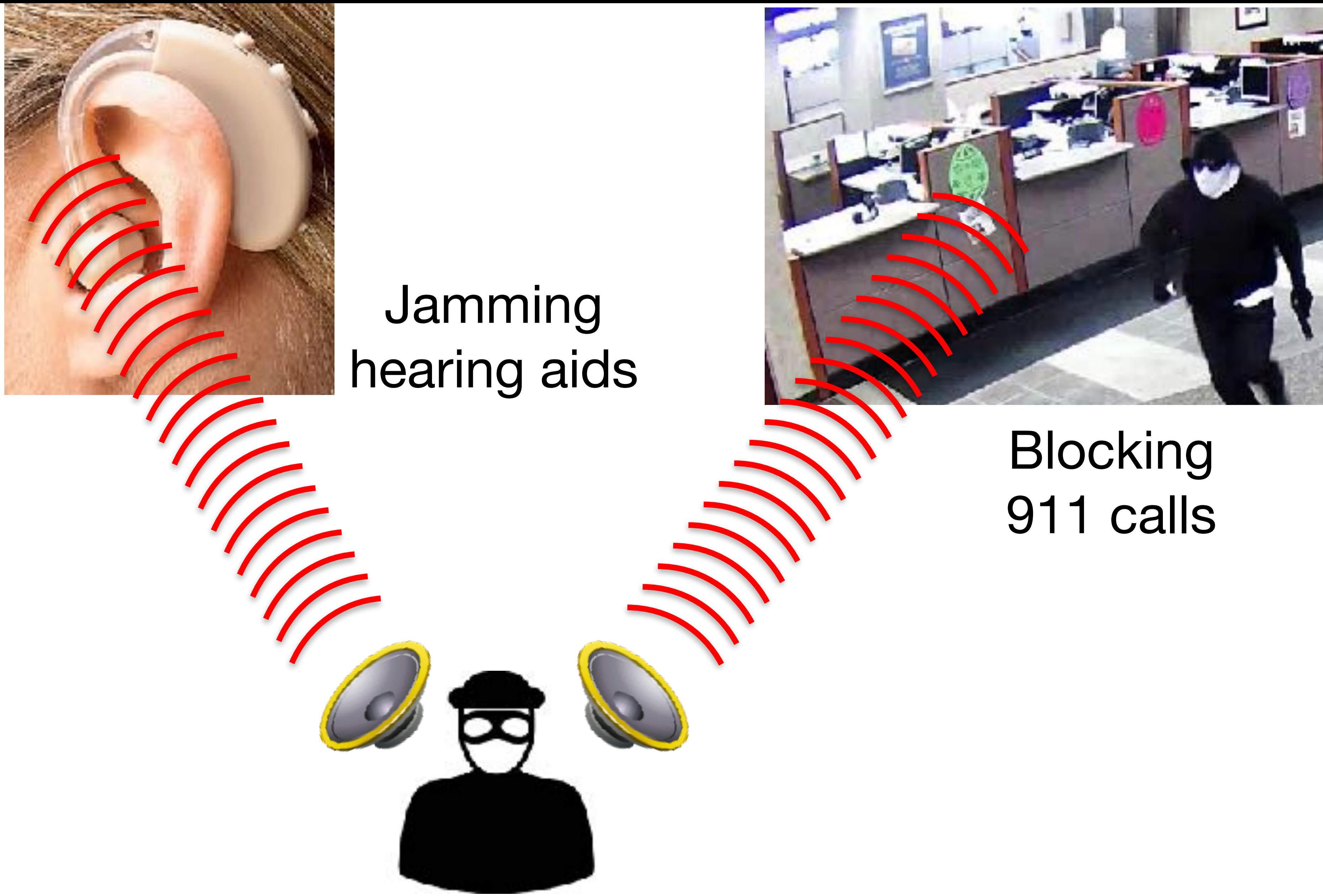

# Threat: Acoustic DOS attack

# Threat: Acoustic DOS attack



Jamming
hearing aids

# Threat: Acoustic DOS attack



# Talk outline

① Microphone Overview

② System Design

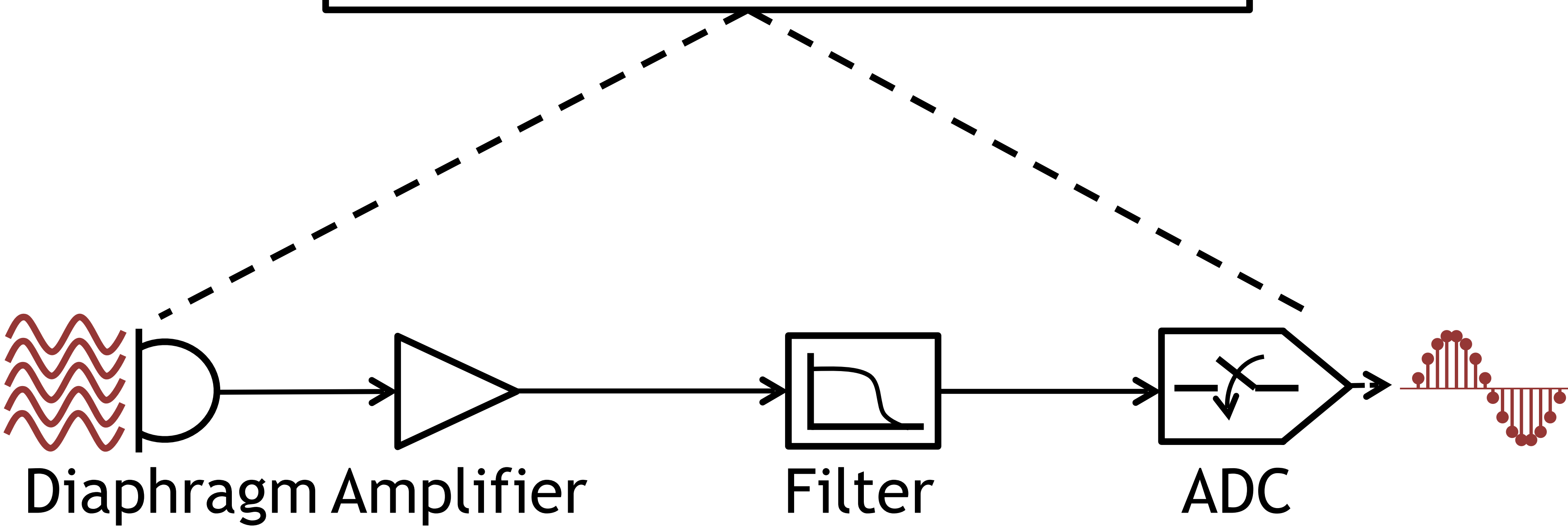
③ Challenges

④ Evaluation

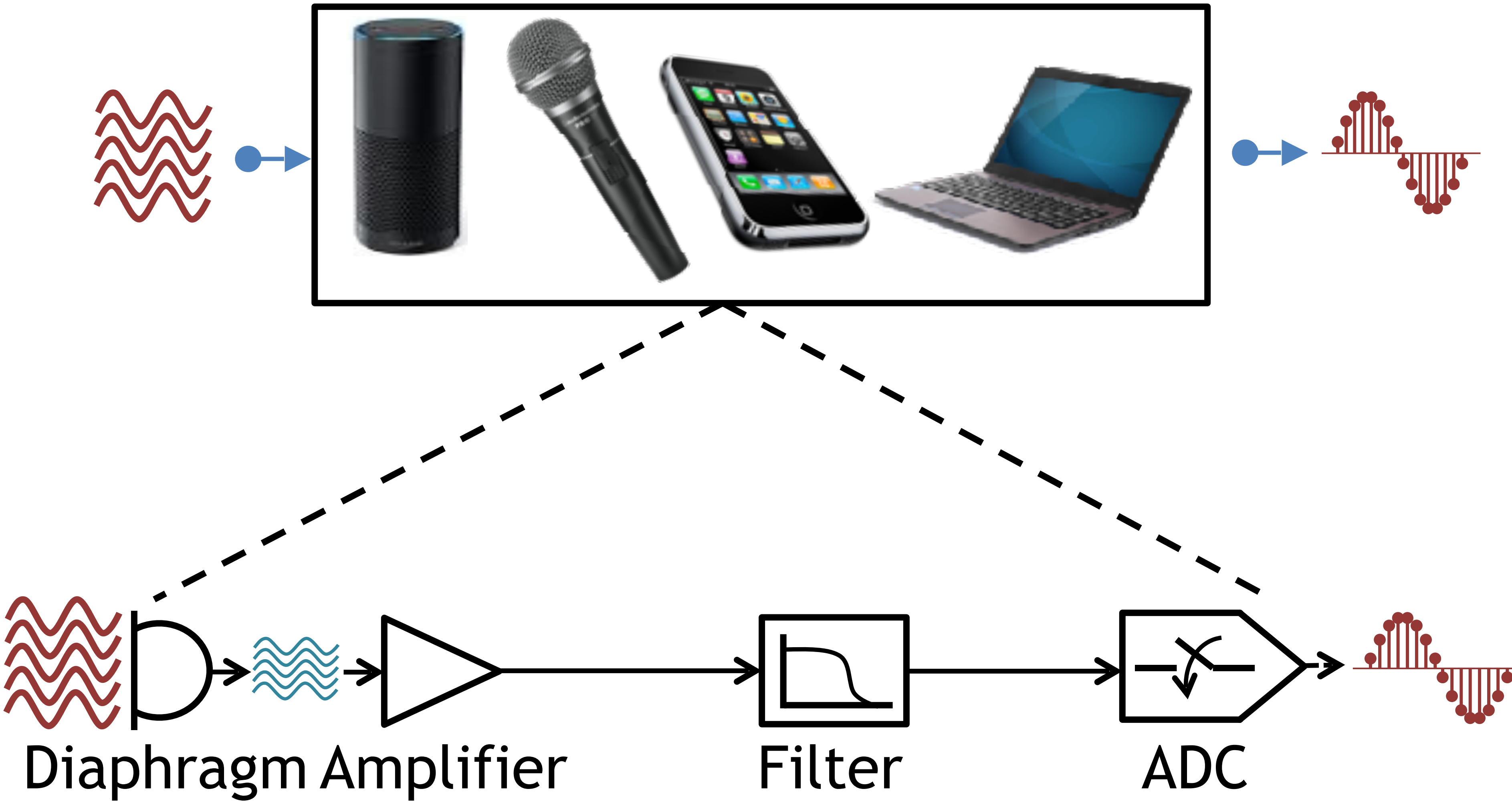
# Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

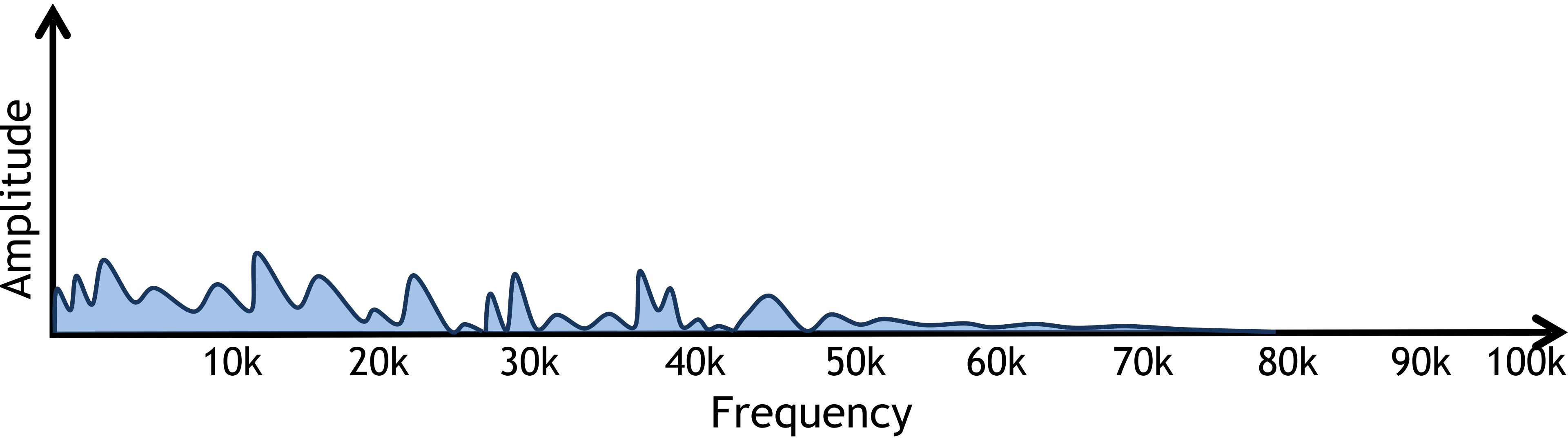
# Microphone working principle

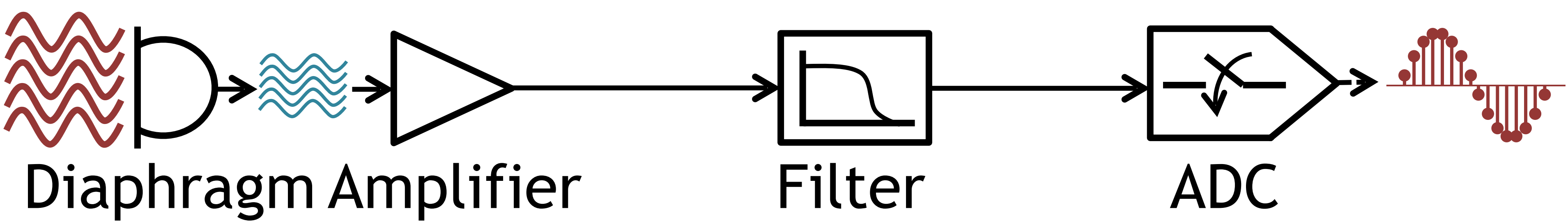


# Microphone working principle

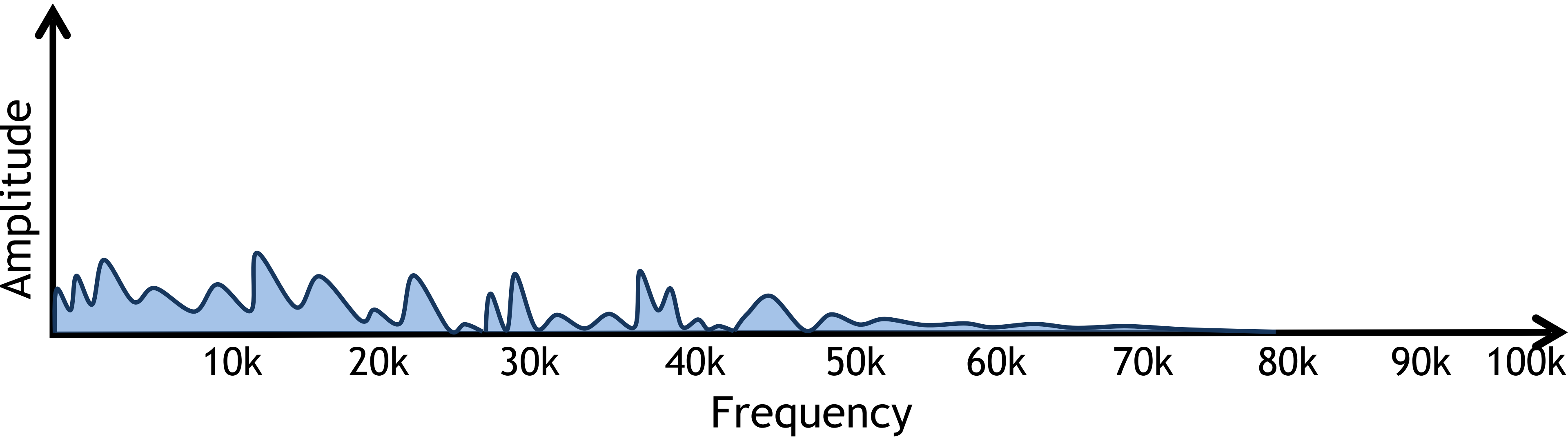


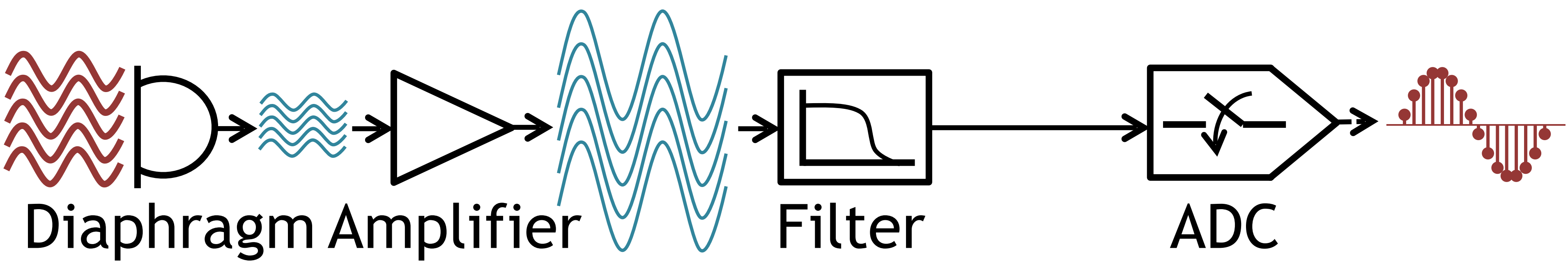
# Microphone working principle



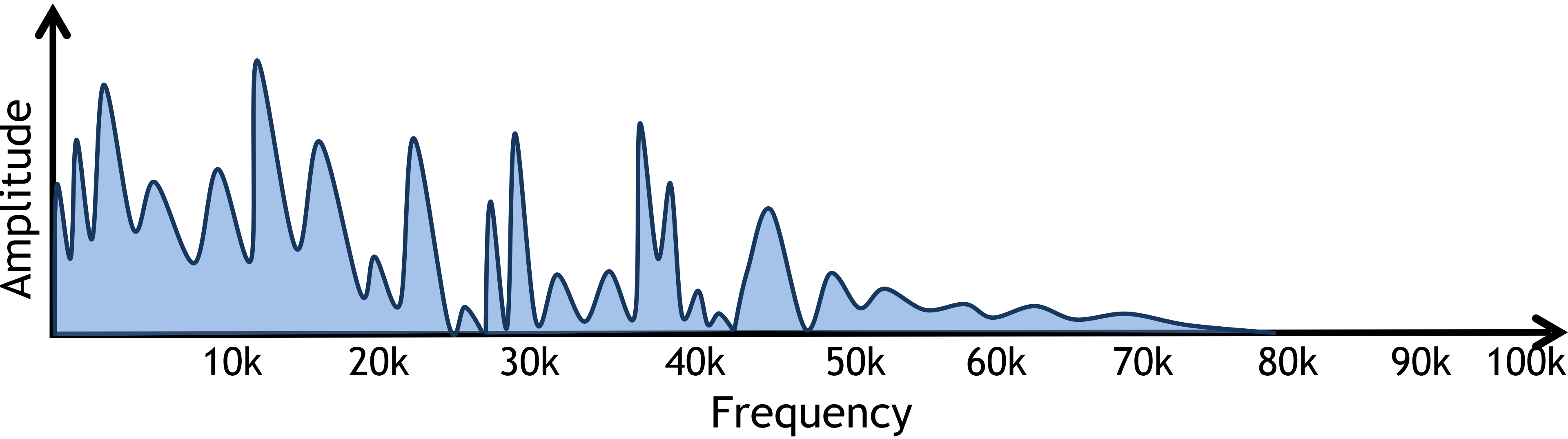



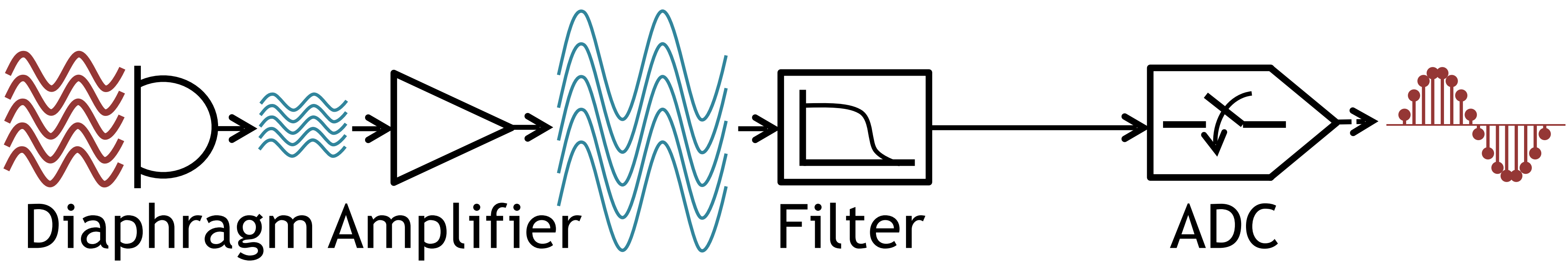
# Microphone working principle



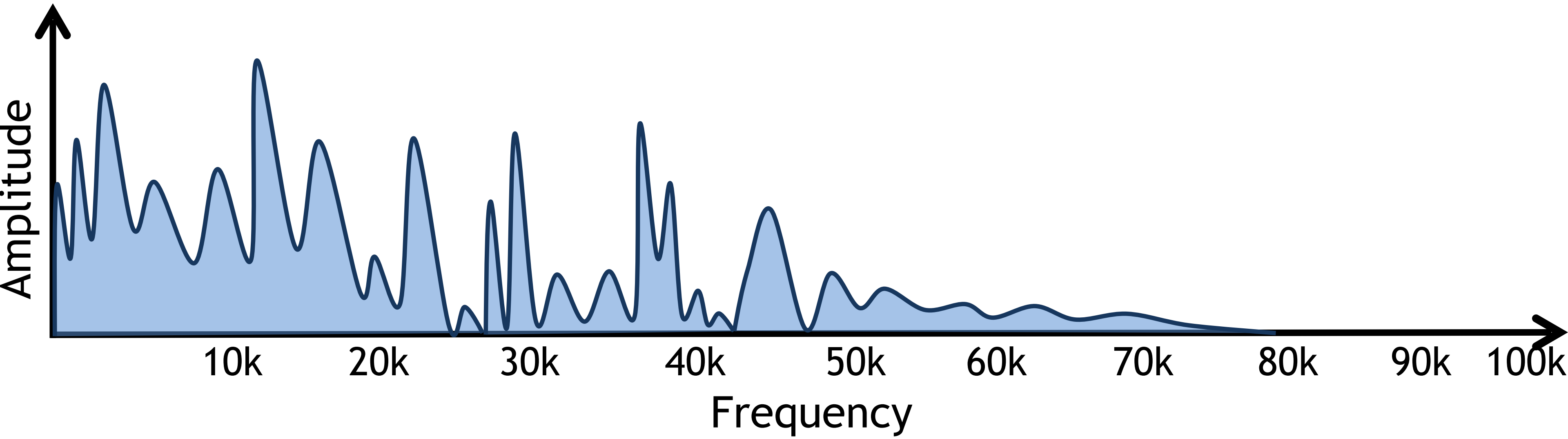



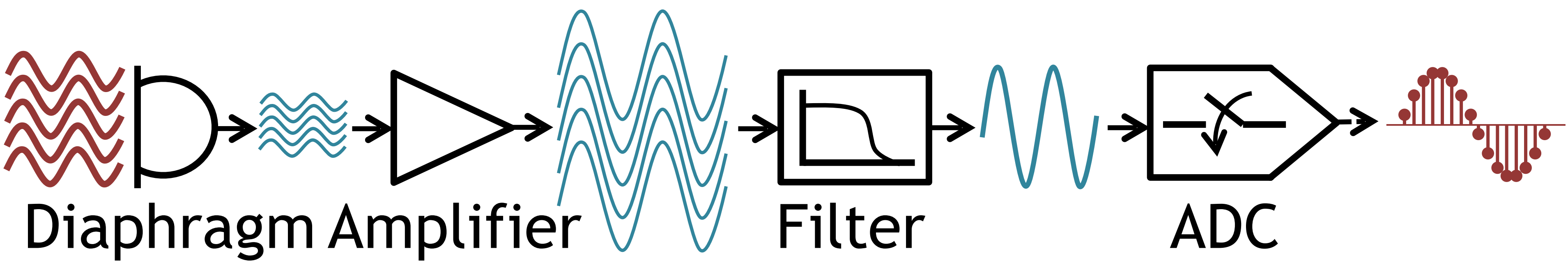
# Microphone working principle



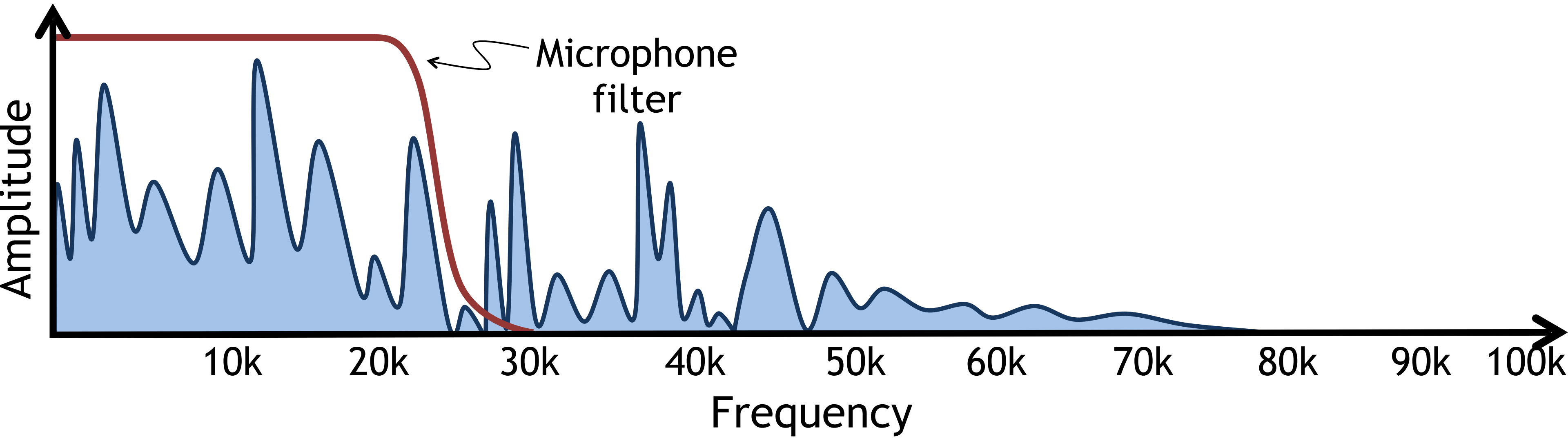



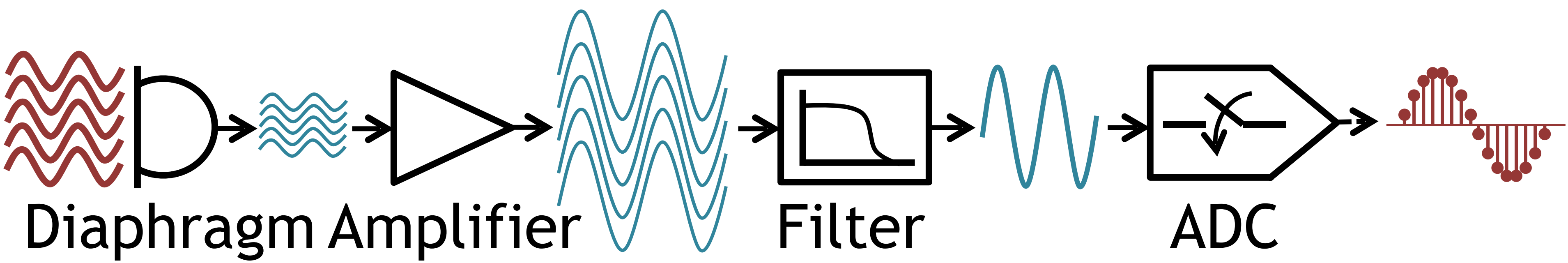
# Microphone working principle



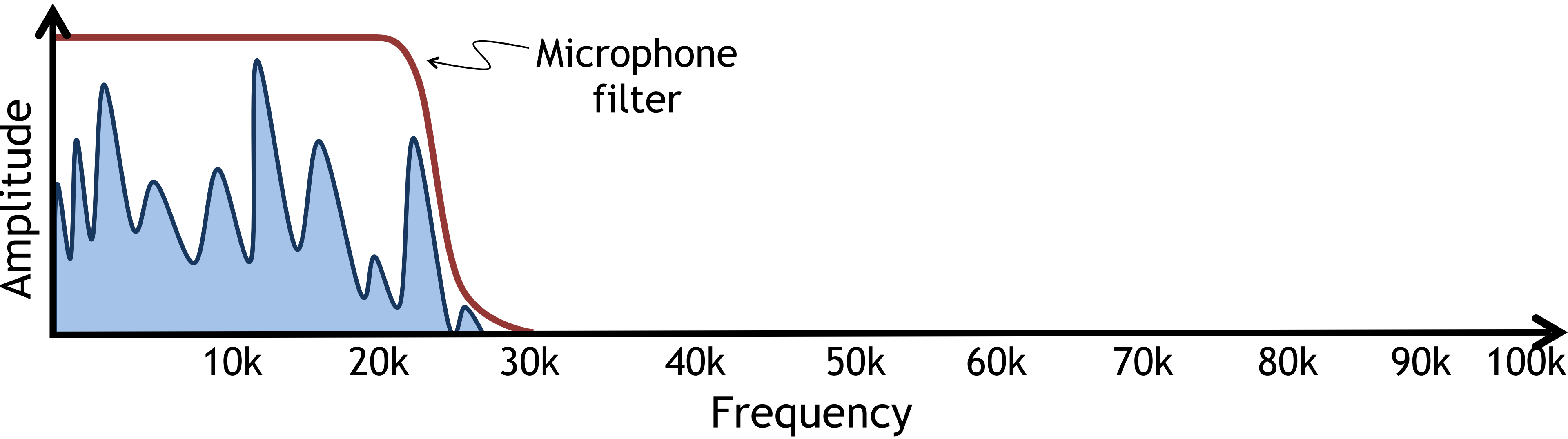



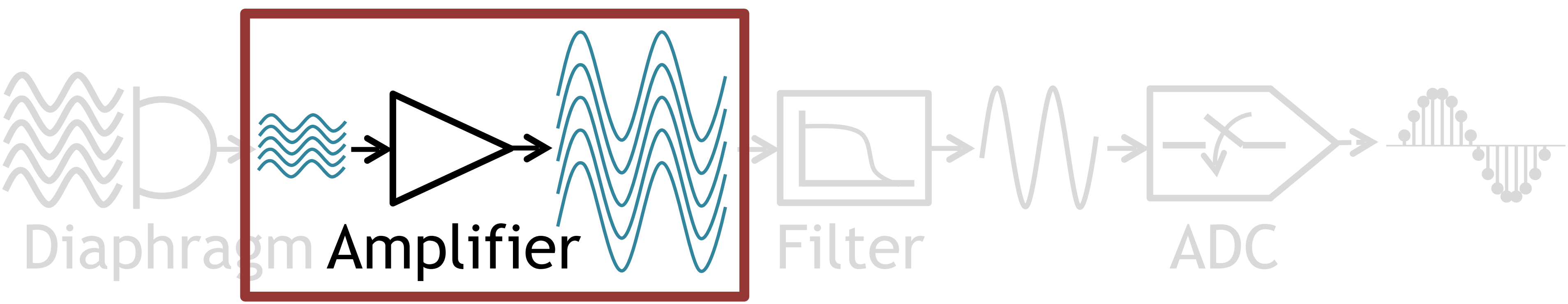
# Microphone working principle



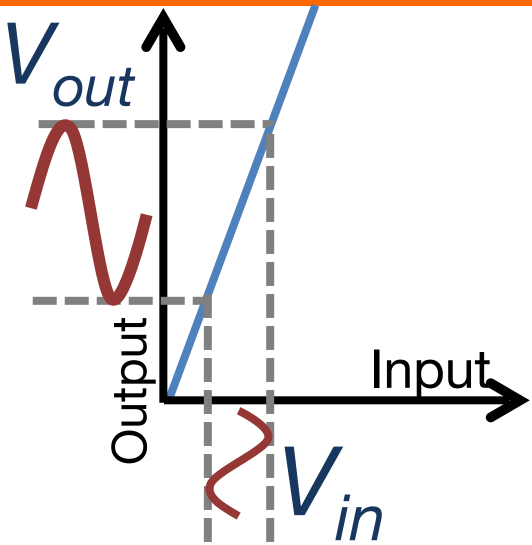



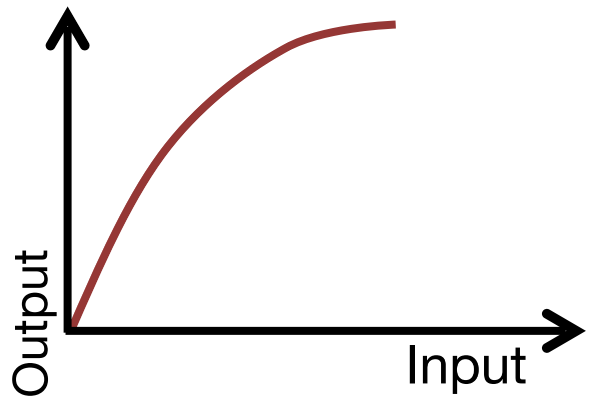
# Microphone working principle



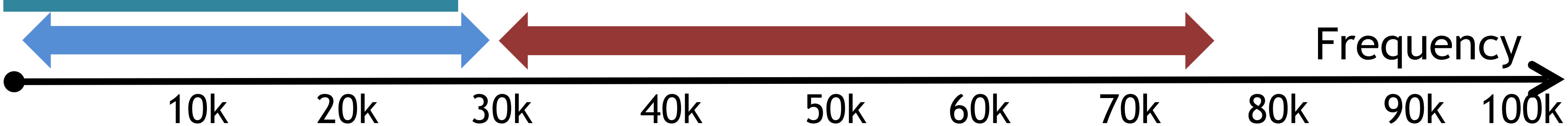
# Microphone working principle

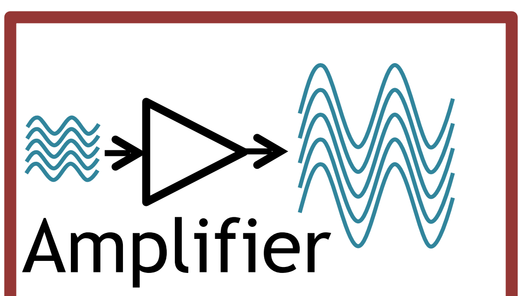


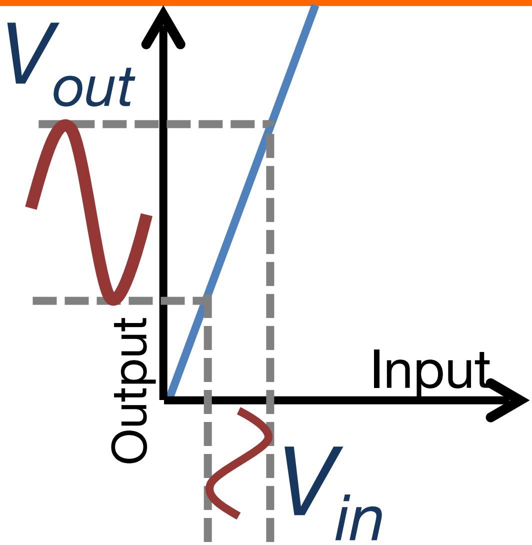

$$V_{out} = a_1 V_{in}$$

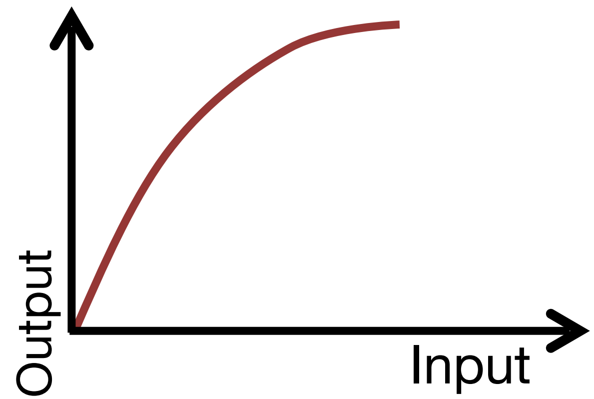
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$$



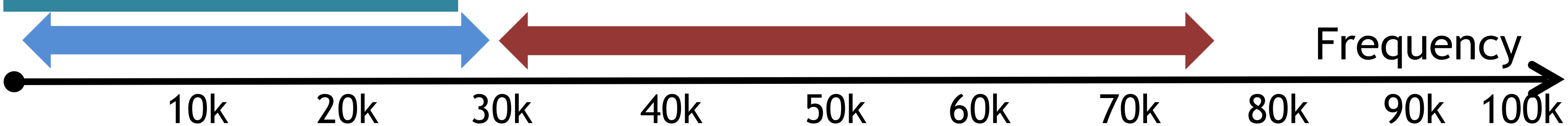
# Microphone working principle

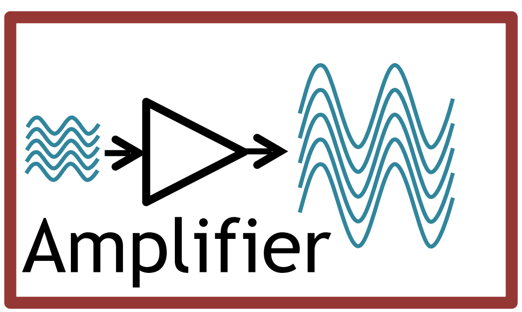


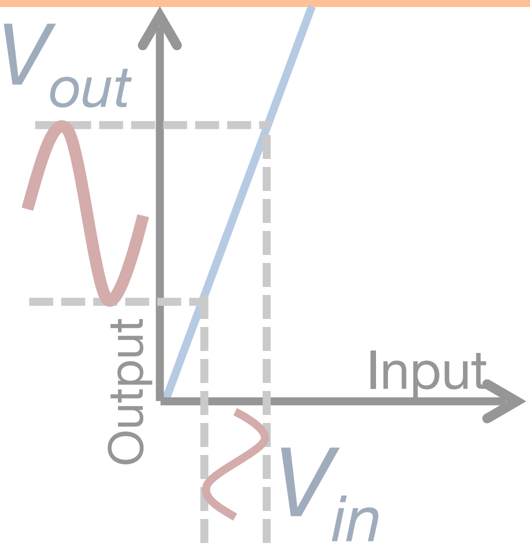

$$V_{out} = a_1 V_{in}$$

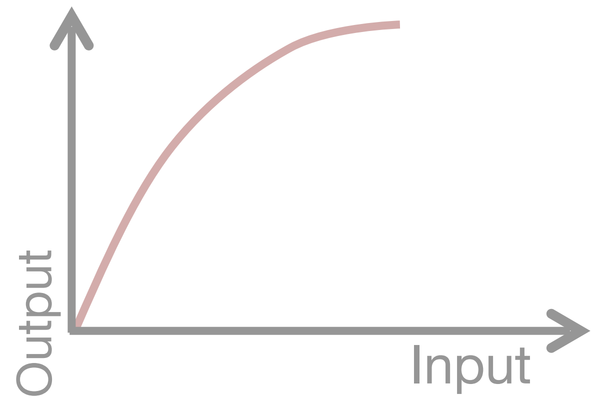
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$



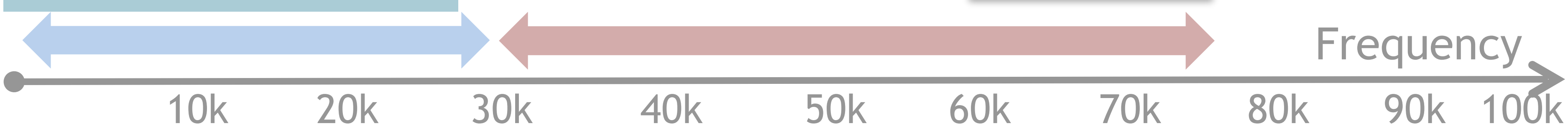
# Microphone working principle

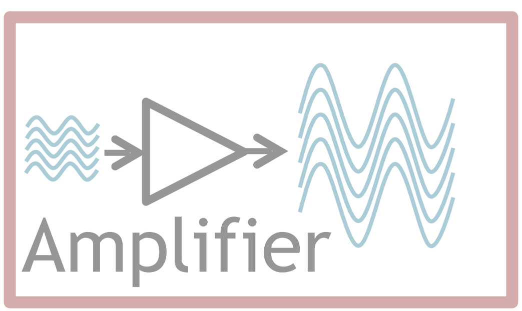



$$V_{out} = a_1 V_{in}$$

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



# Talk outline

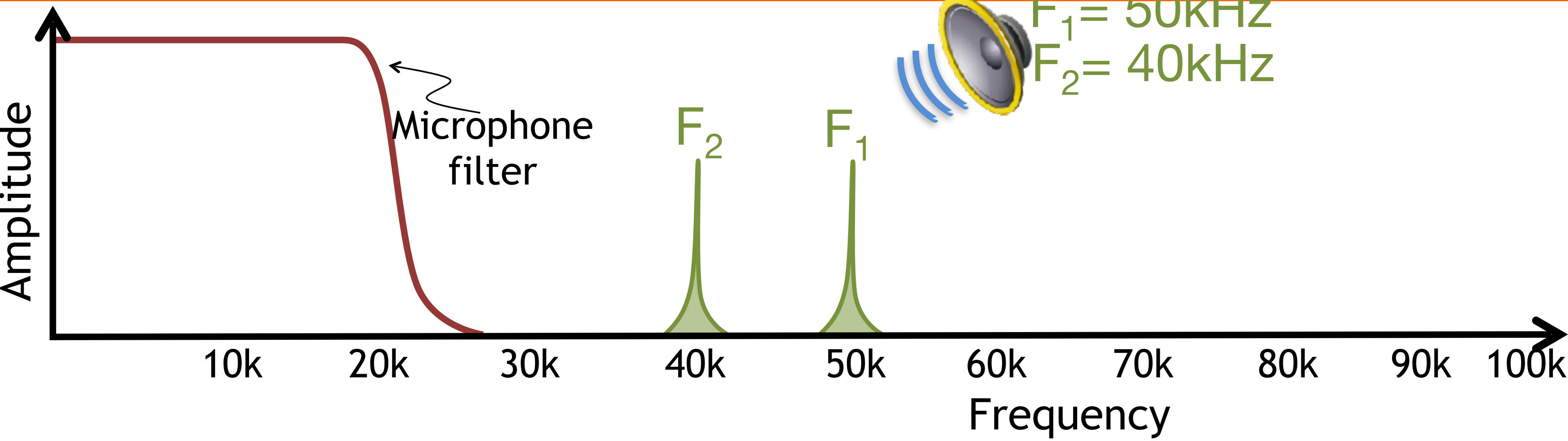
① Microphone Overview

② System Design

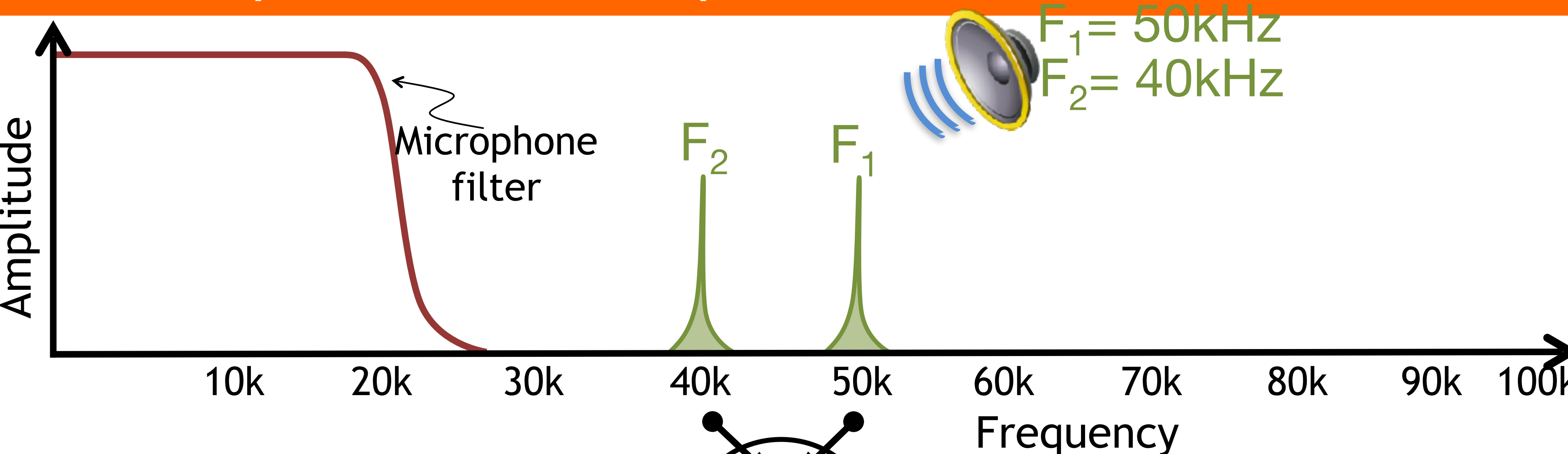
③ Challenges

④ Evaluation

# Exploiting amplifier non-linearity



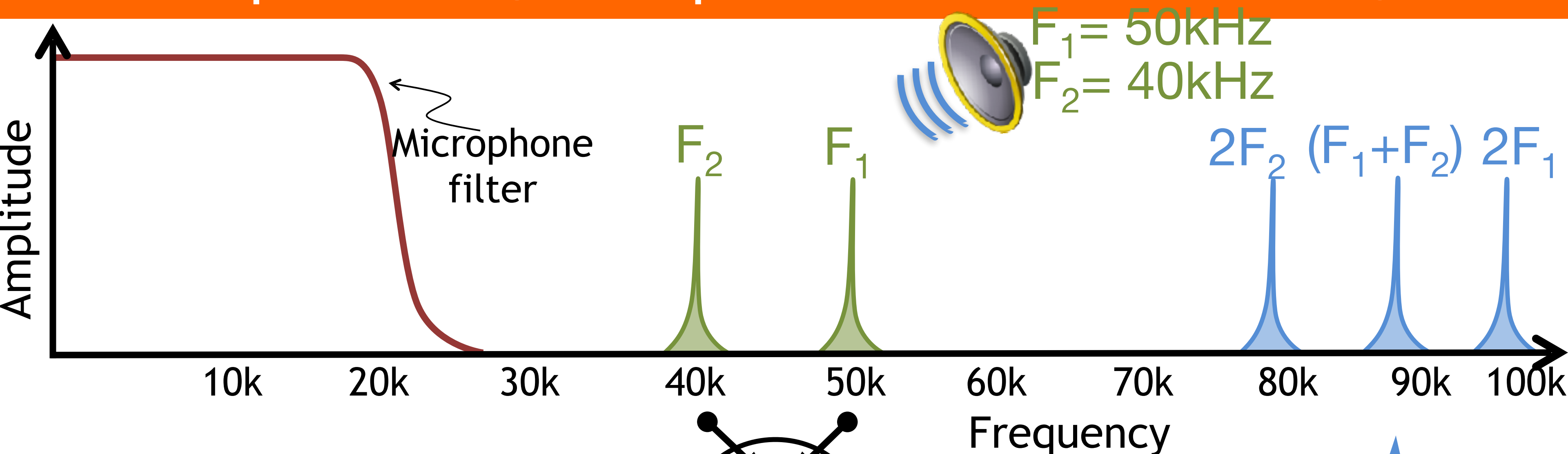
# Exploiting amplifier non-linearity




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

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

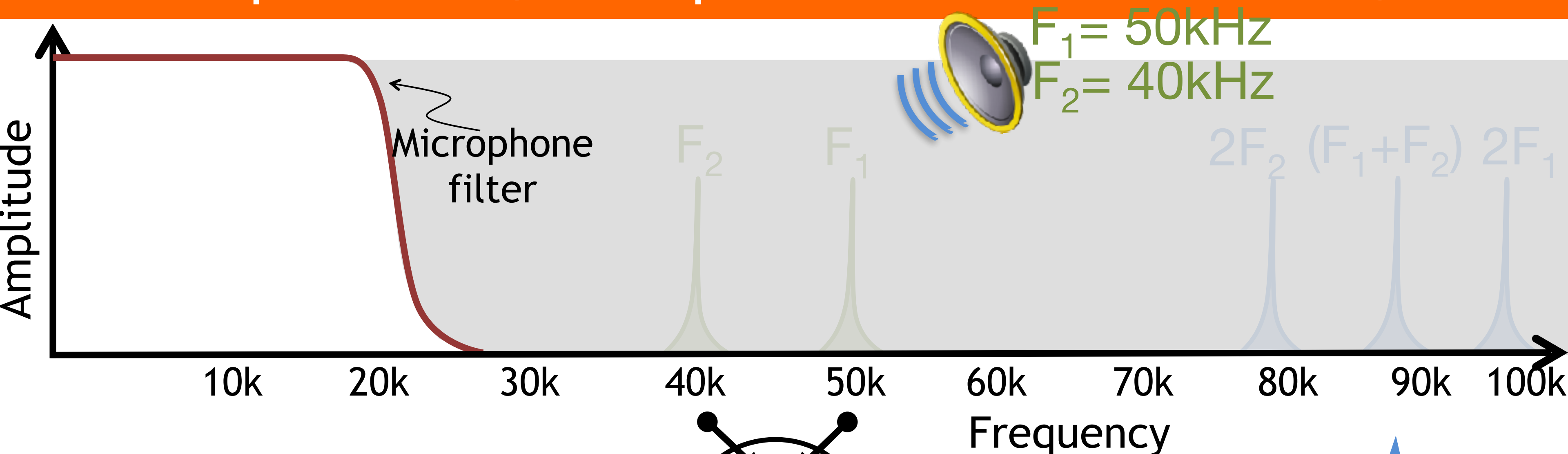
# Exploiting amplifier non-linearity




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

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

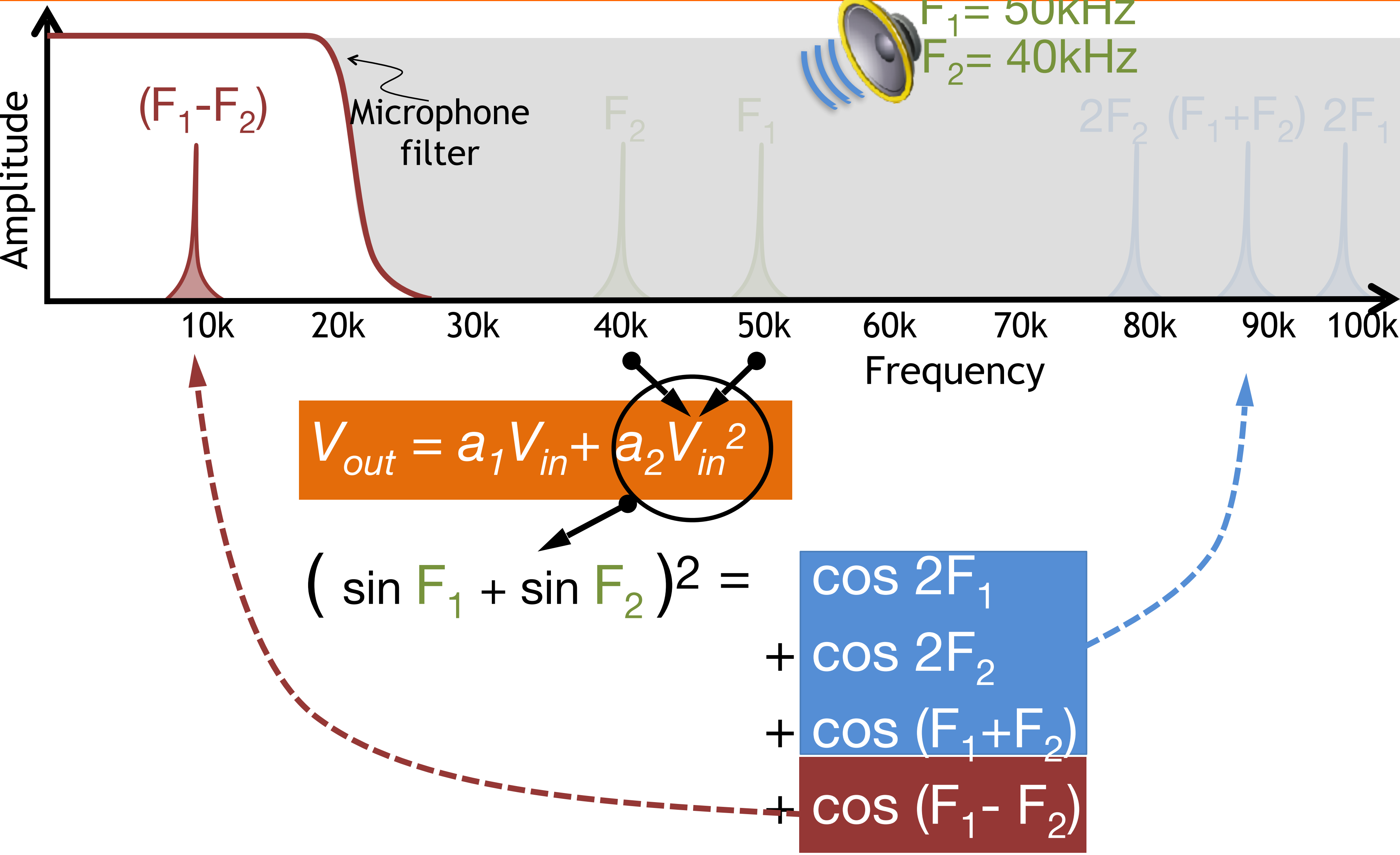
# Exploiting amplifier non-linearity



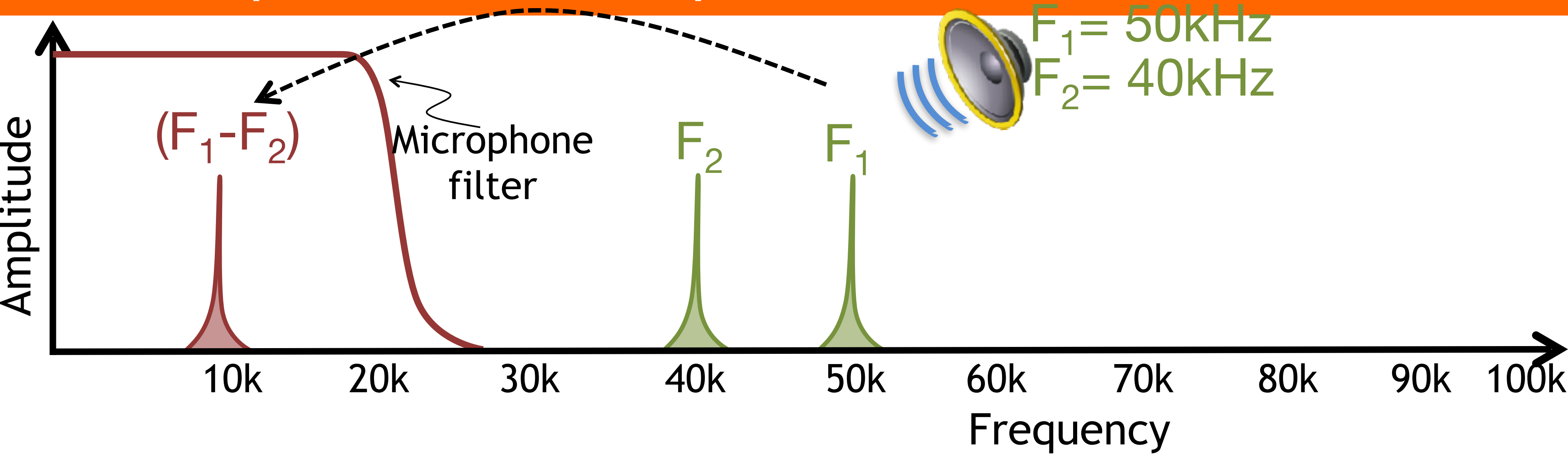

$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

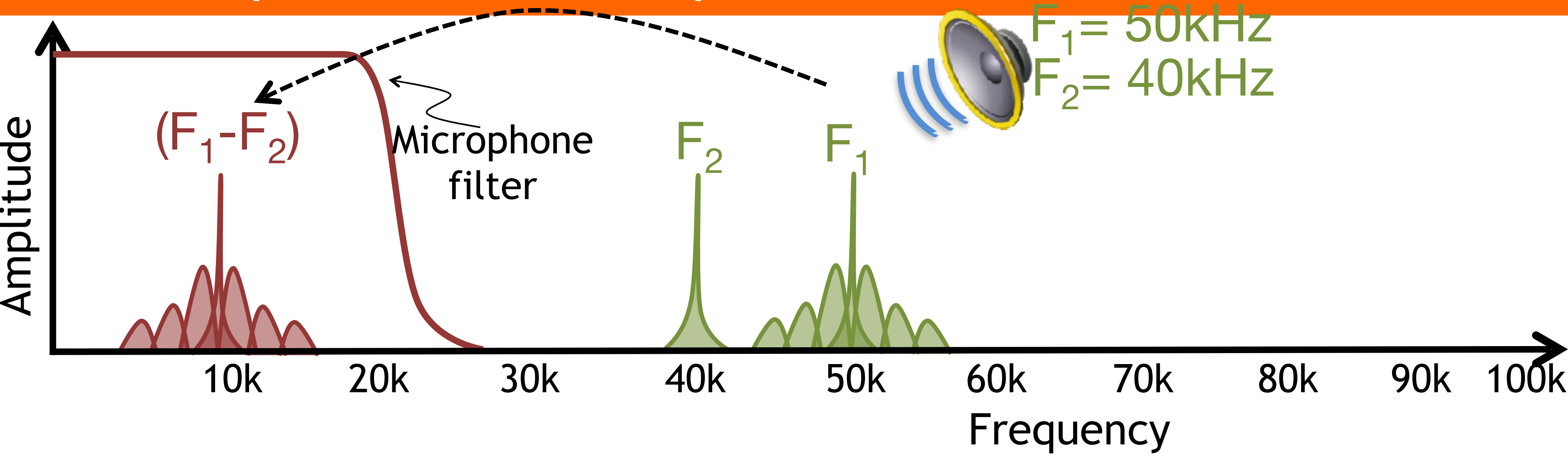
# Exploiting amplifier non-linearity



# Exploiting amplifier non-linearity



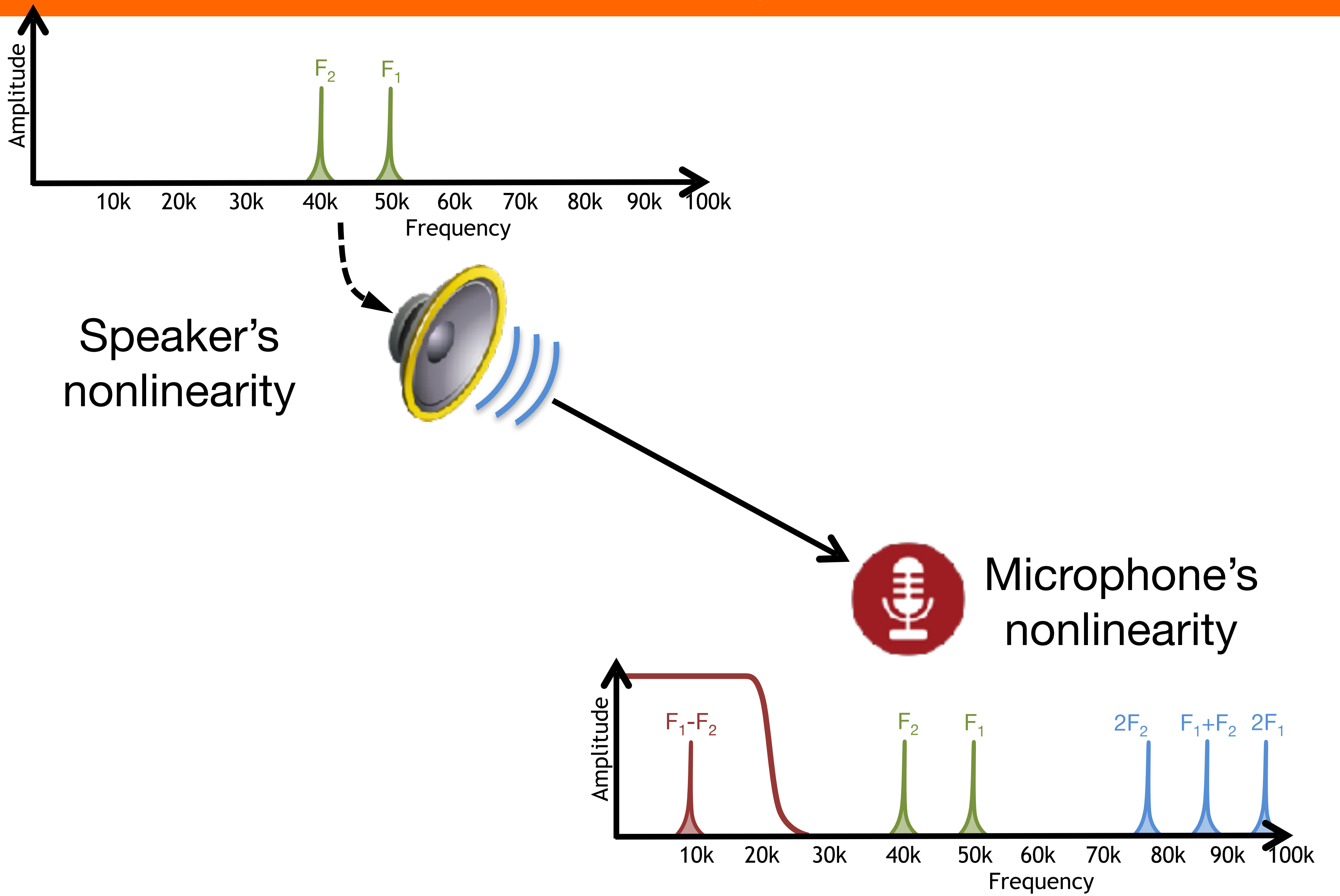
# Exploiting amplifier non-linearity



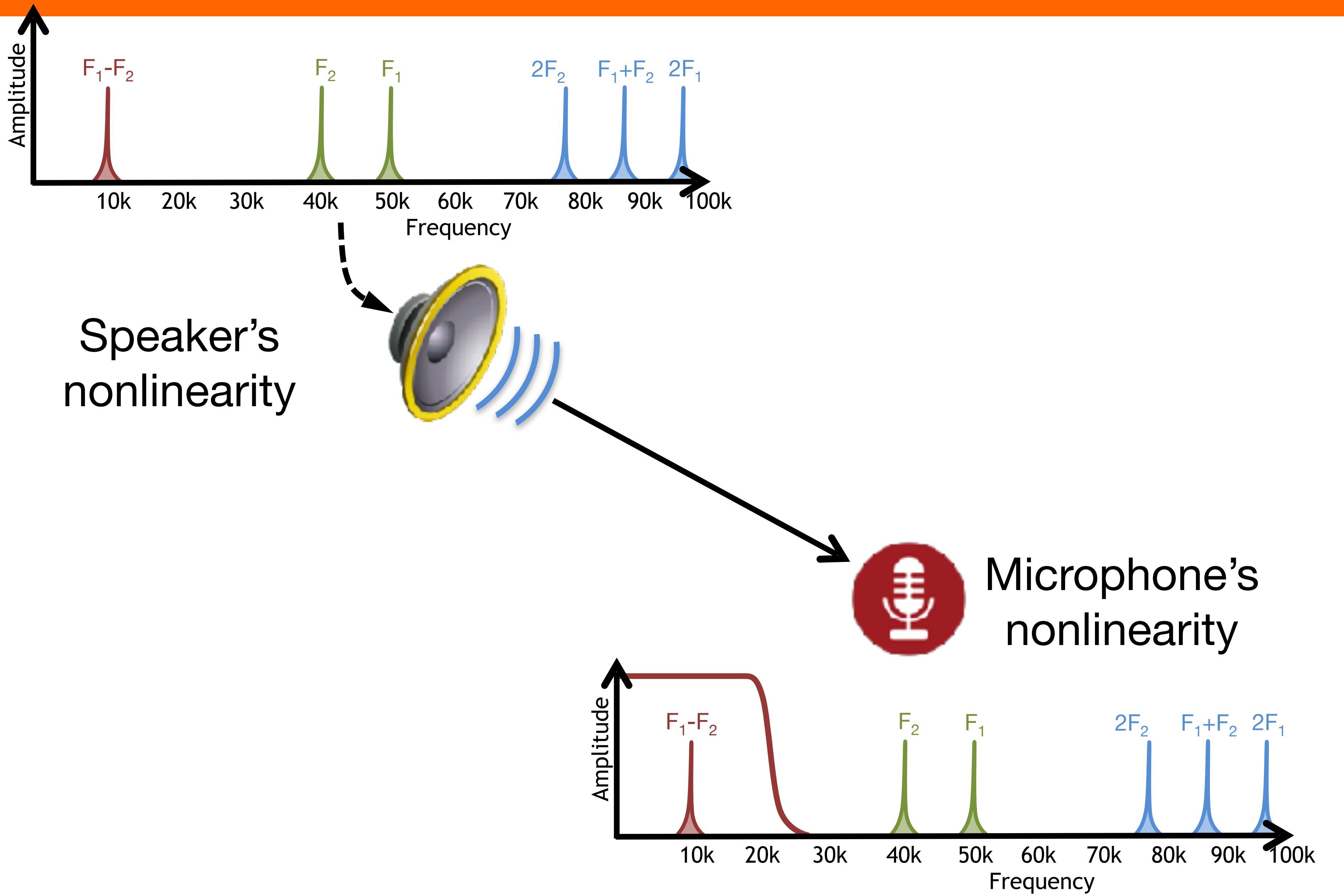
# Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

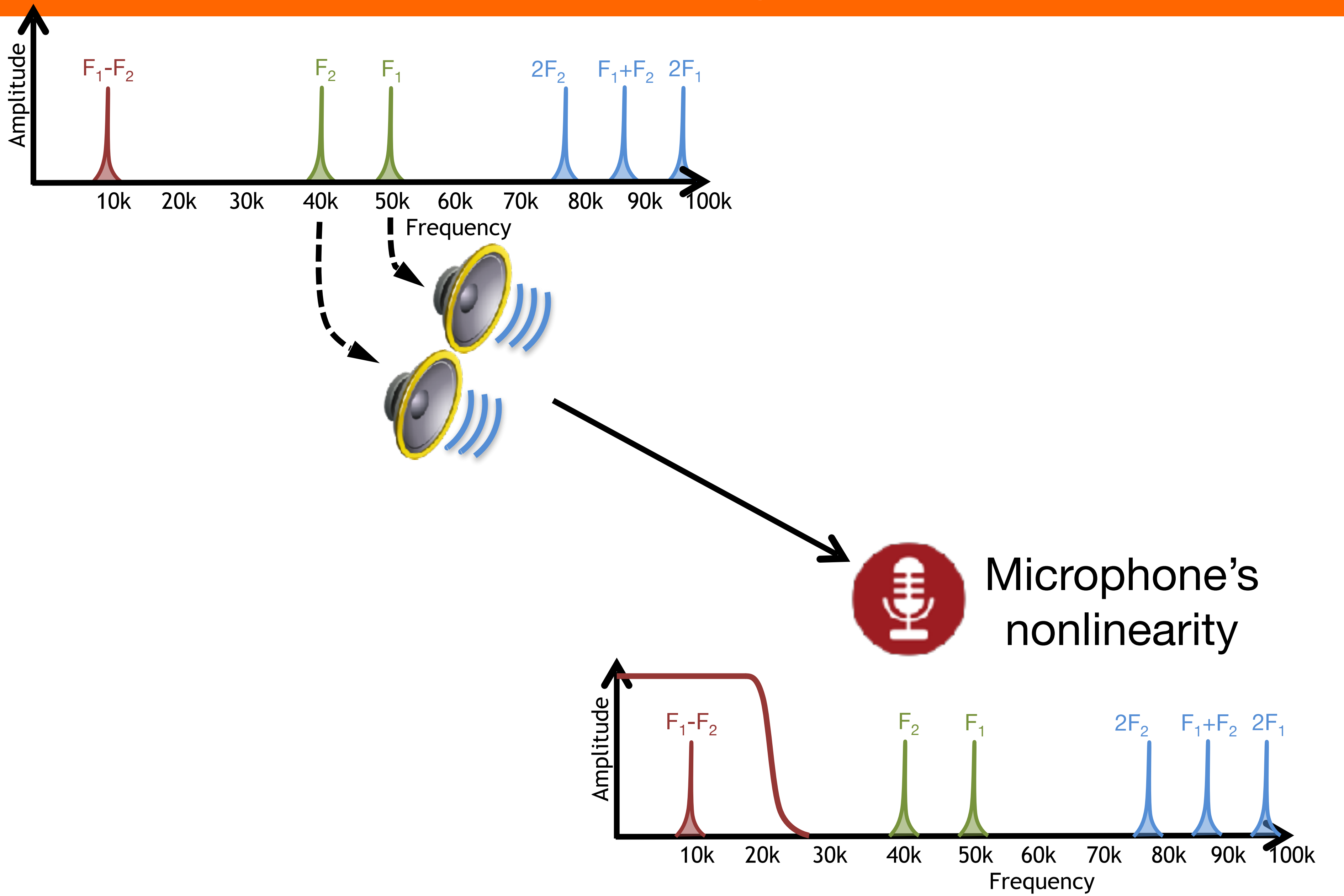
# Challenges


Amplitude
F2
F1
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency
Speaker's nonlinearity
Microphone's nonlinearity
Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency

# Challenges

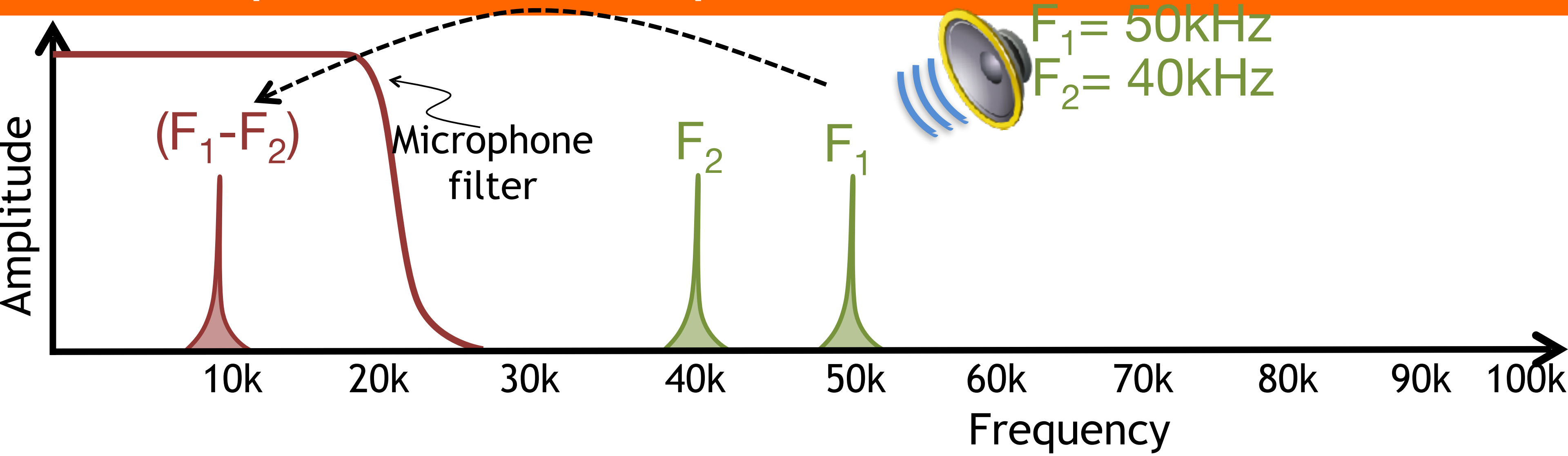

Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency
Speaker's nonlinearity
Microphone's nonlinearity
Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k 20k 30k 40k 50k 60k 70k 80k 90k 100k
Frequency

# Challenges



Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency
Microphone's nonlinearity
Amplitude
F1-F2
F2
F1
2F2
F1+F2
2F1
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency

# Exploiting amplifier non-linearity



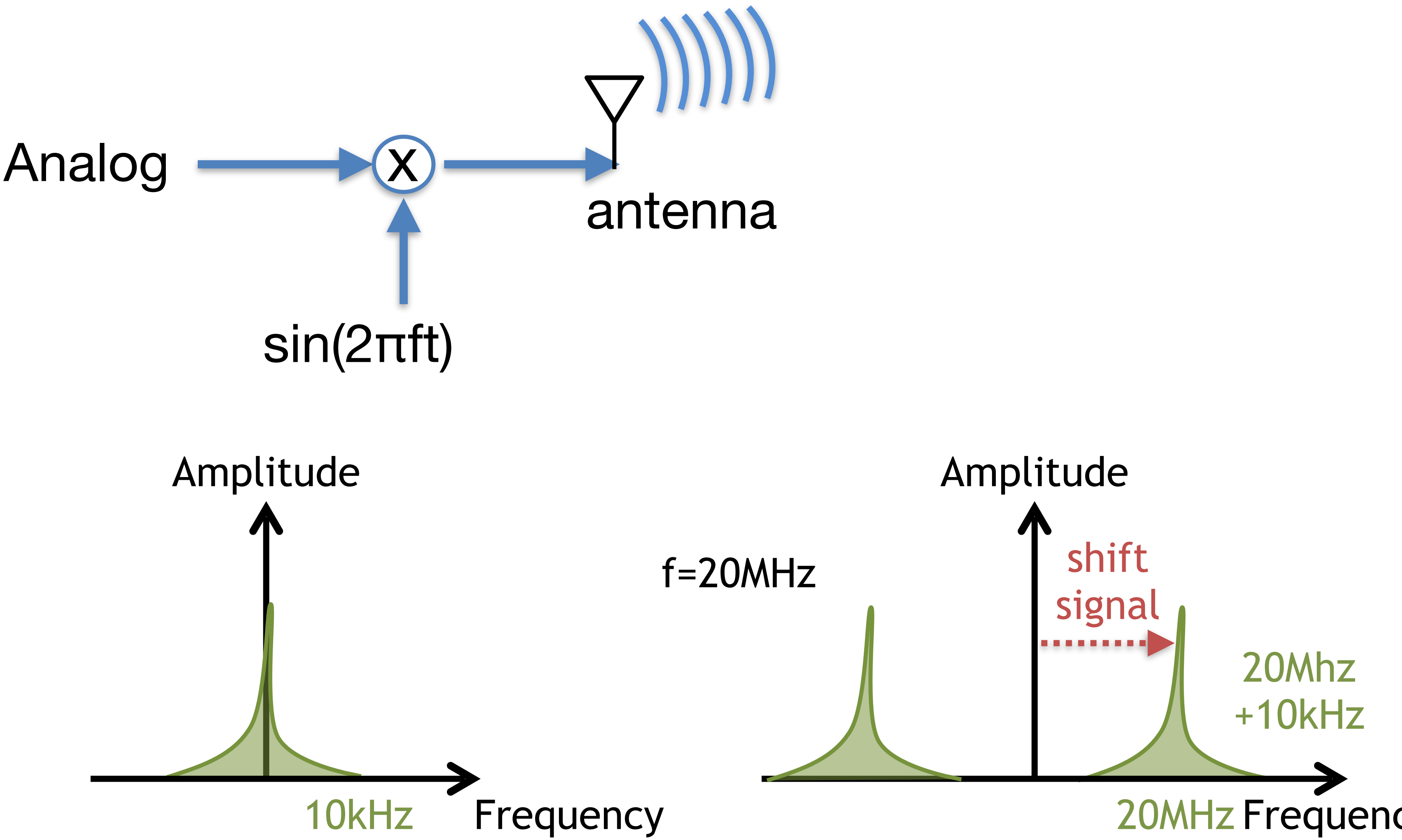

Not sending a single “tone” (sine wave), but sending a command.

How can we send this command?

Reminder on
Modulation

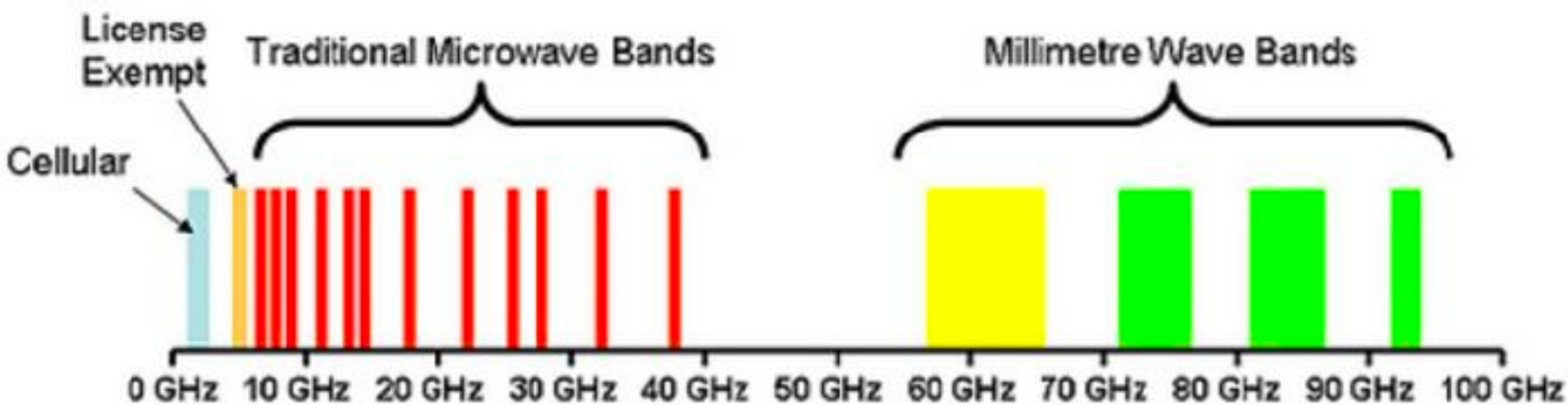
E.g., We send WiFi at 2.4GHz or 5GHz
What does this mean and Why?

# Reminder on Modulation



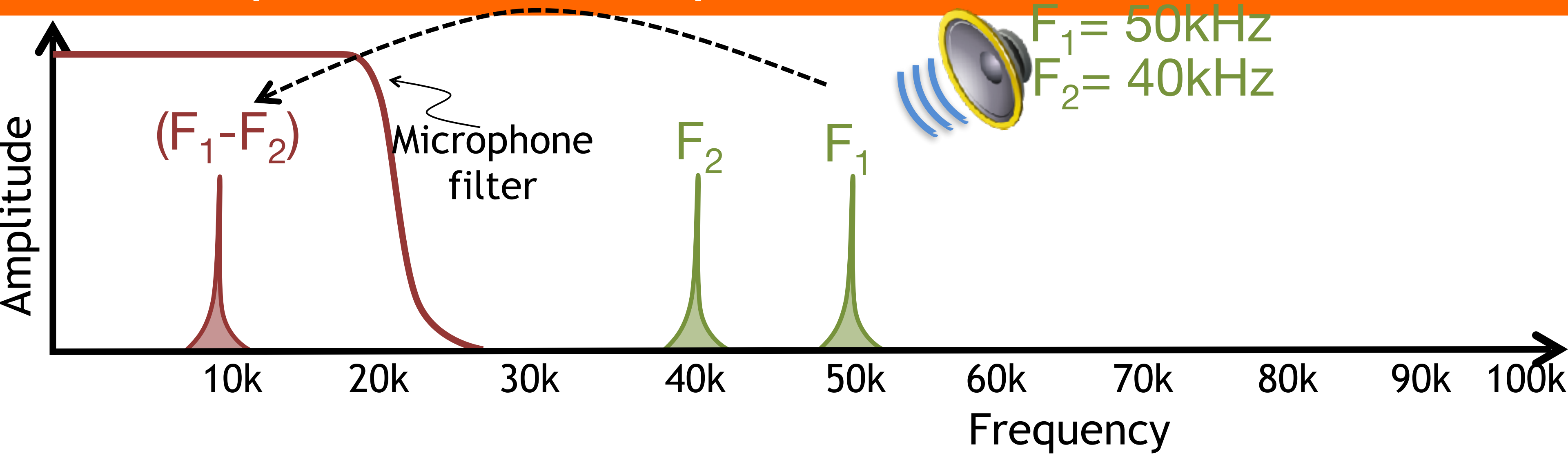
# Why is Modulation useful?

1. Interference, Technology Co-existence
2. Spectrum Access (Legal)
3. Antenna size (wavelength/4)




WiFi? LTE? 5G?

# Exploiting amplifier non-linearity




Not sending a single "tone" (sine wave), but sending a command/message.

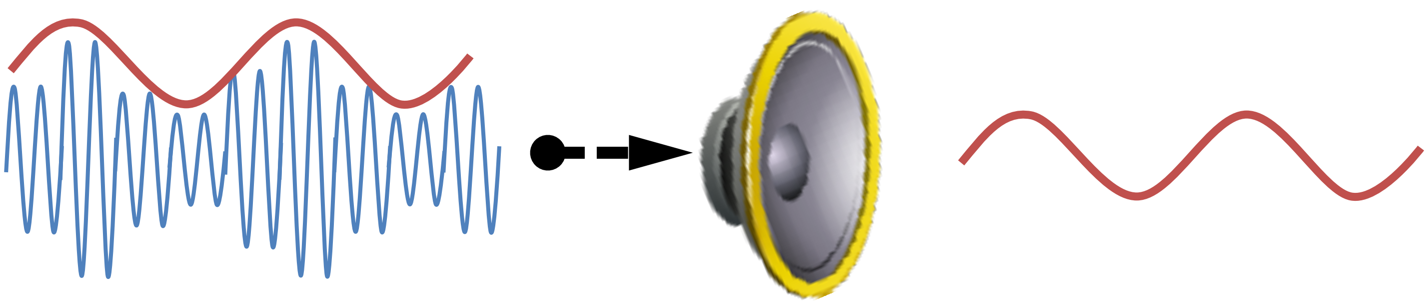
How can we send this command message m(t)?

$$m(t) \times \sin(2\pi f t)$$

# Challenges

Amplitude modulation

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



Ultrasonic speaker

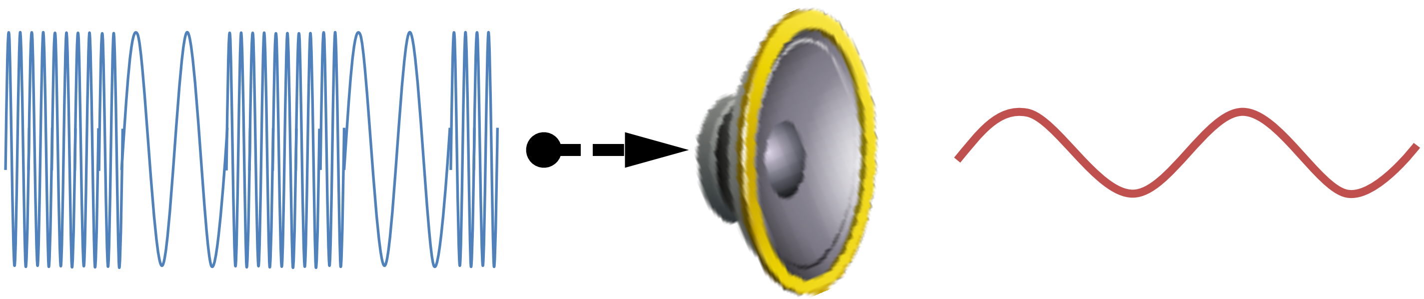
$$\begin{aligned} S^2_{out,AM} &= A_2\{aSin(\omega_m t).Sin(\omega_c t)\}^2 \\ &= -A_2\frac{a^2}{4}\{Cos(\omega_c t - \omega_m t) - Cos(\omega_c t + \omega_m t)\}^2 \\ &= -A_2\frac{a^2}{4}Cos(2\omega_m t) + (terms\ with\ frequencies \\ &\qquad\qquad above\ \omega_c\ and\ DC) \end{aligned}$$

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

# Challenges

Frequency modulation

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

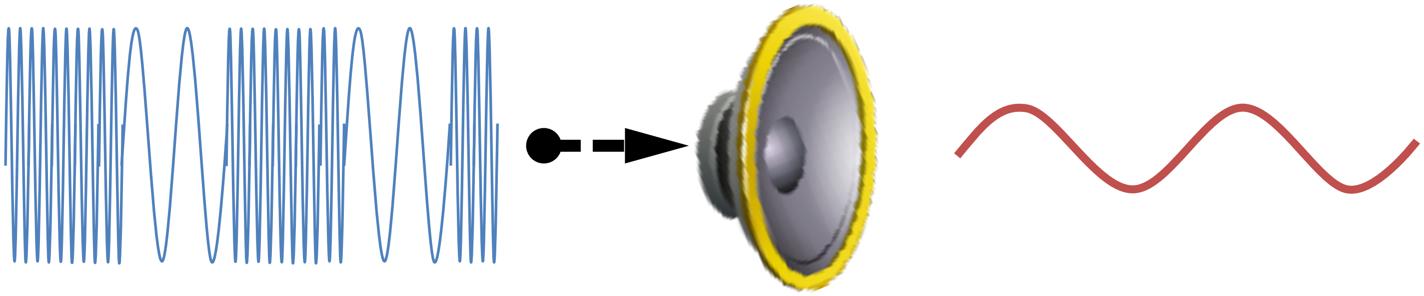


Ultrasonic speaker

# Challenges

Frequency modulation

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

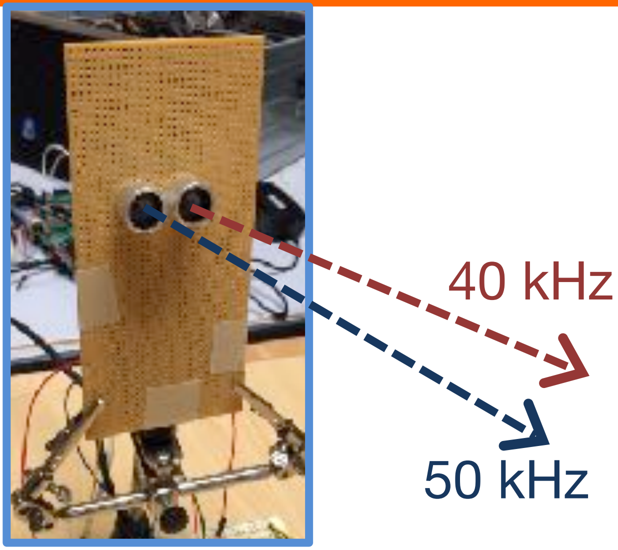


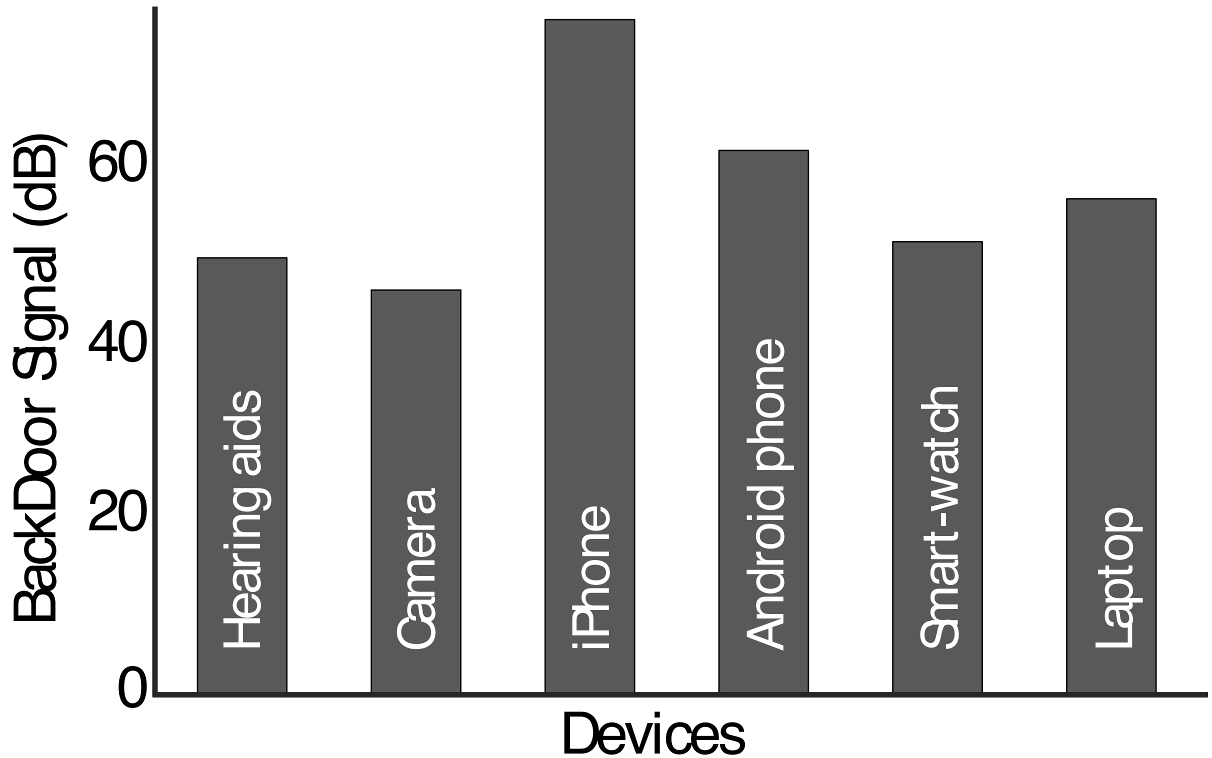
Ultrasonic speaker

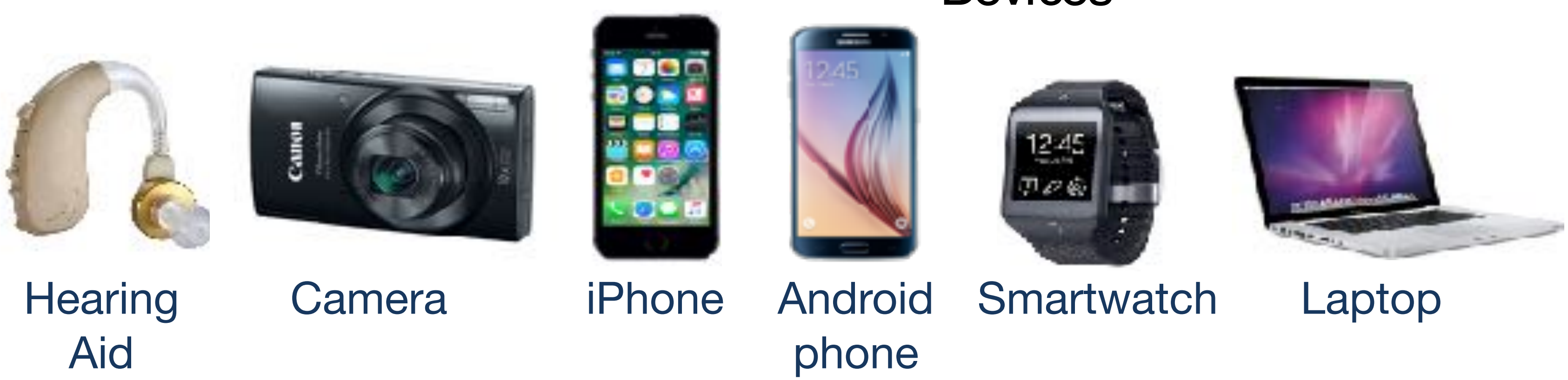
# Talk outline

1. Microphone Overview
2. System Design
3. Challenges
4. Evaluation

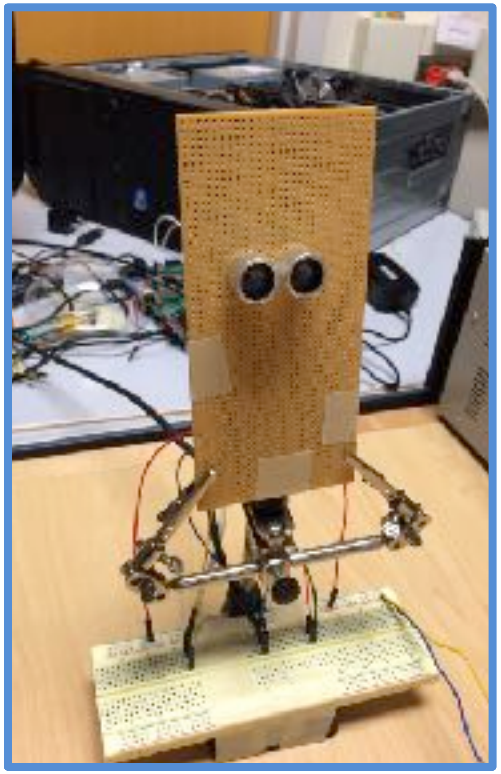
# Hardware generalizability



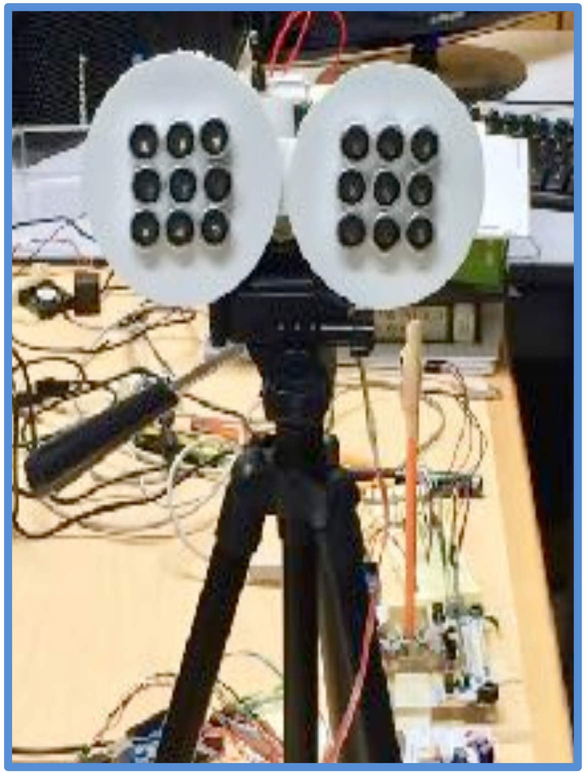



# Implementation

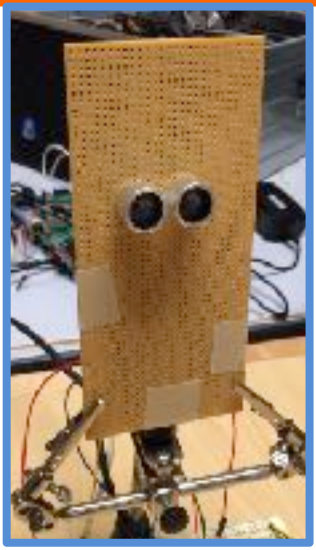


Communication prototype



Jammer prototype

# Communication performance

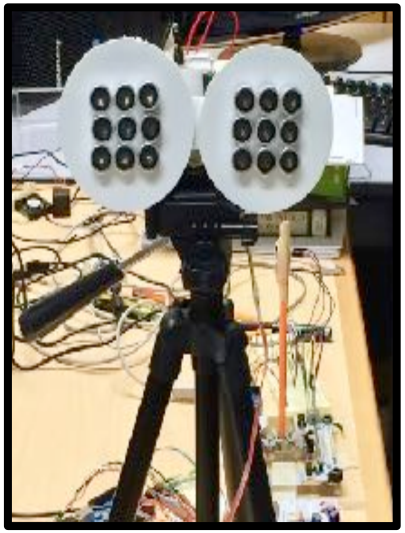


FM data packets


4kbps
up to 1 meter

More power can increase the distance

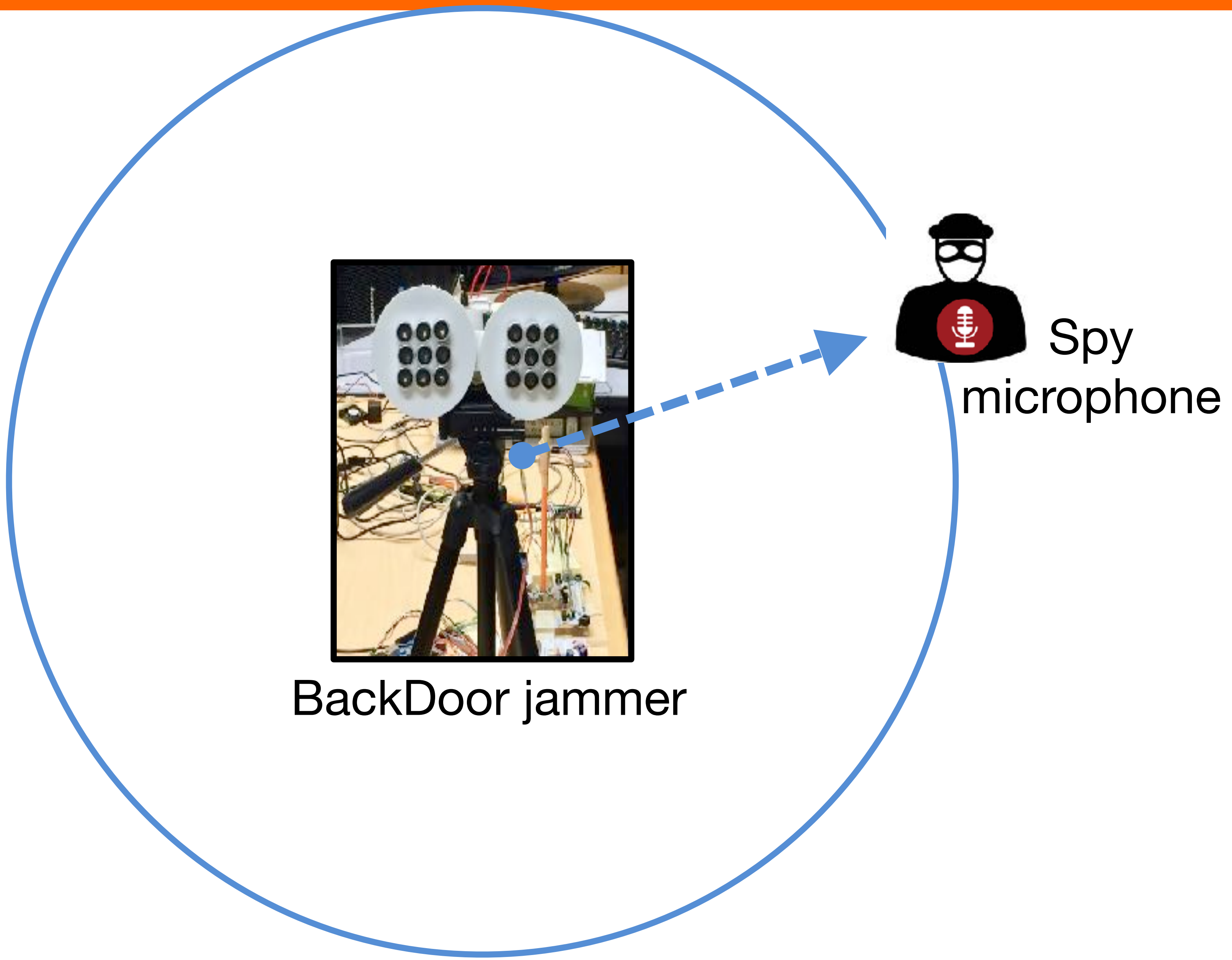
# Jamming performance



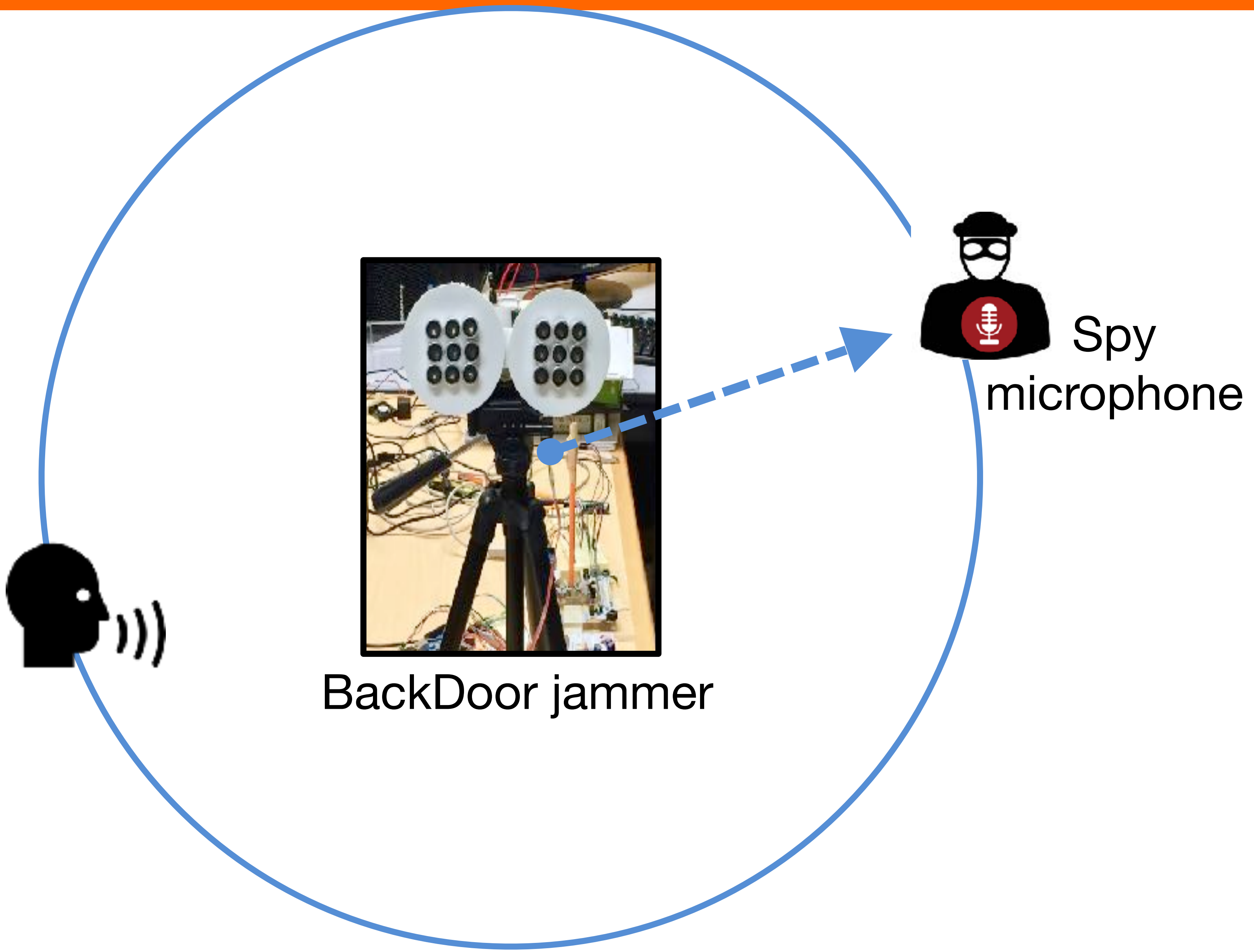
BackDoor jammer

Spy microphone

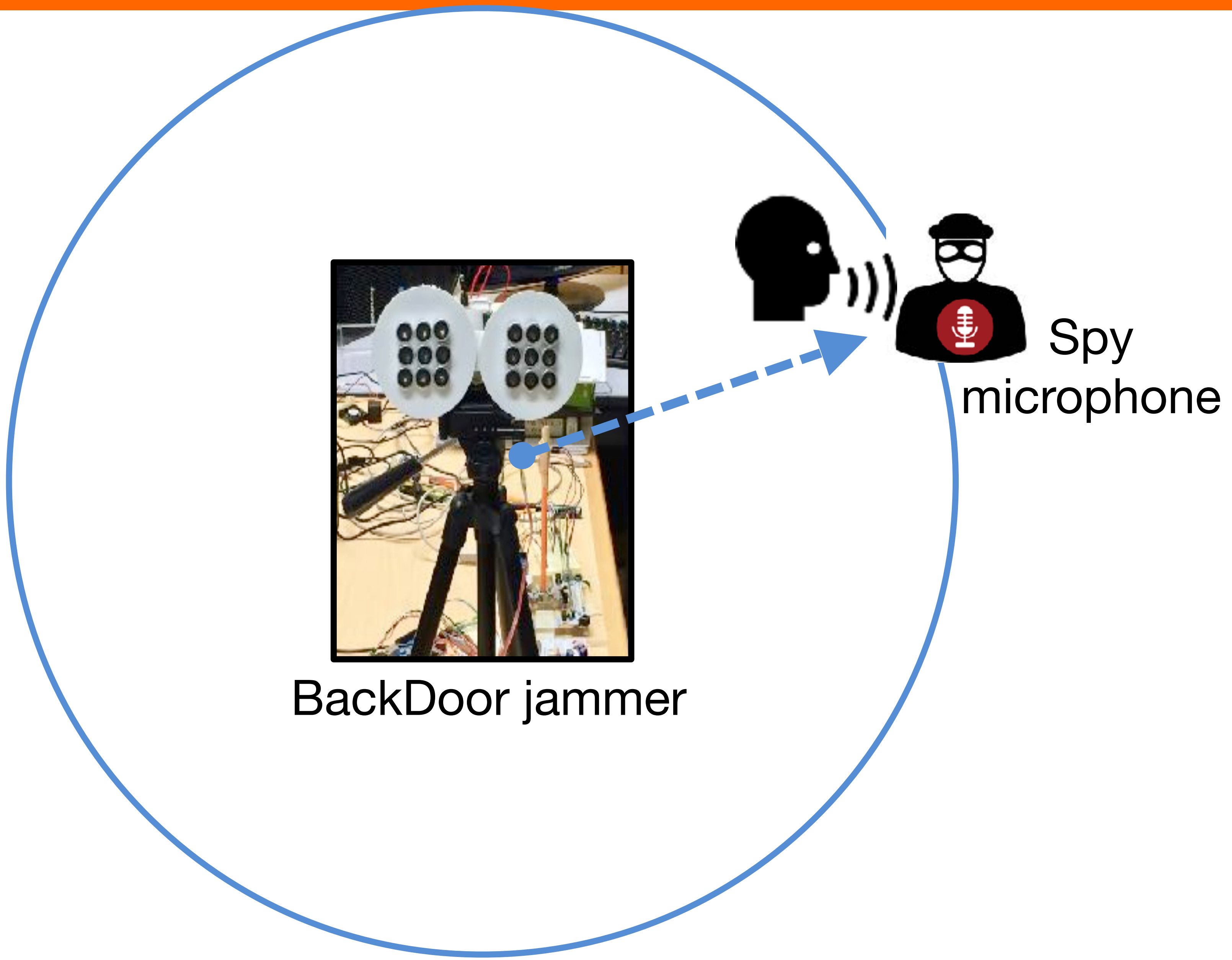
# Jamming performance



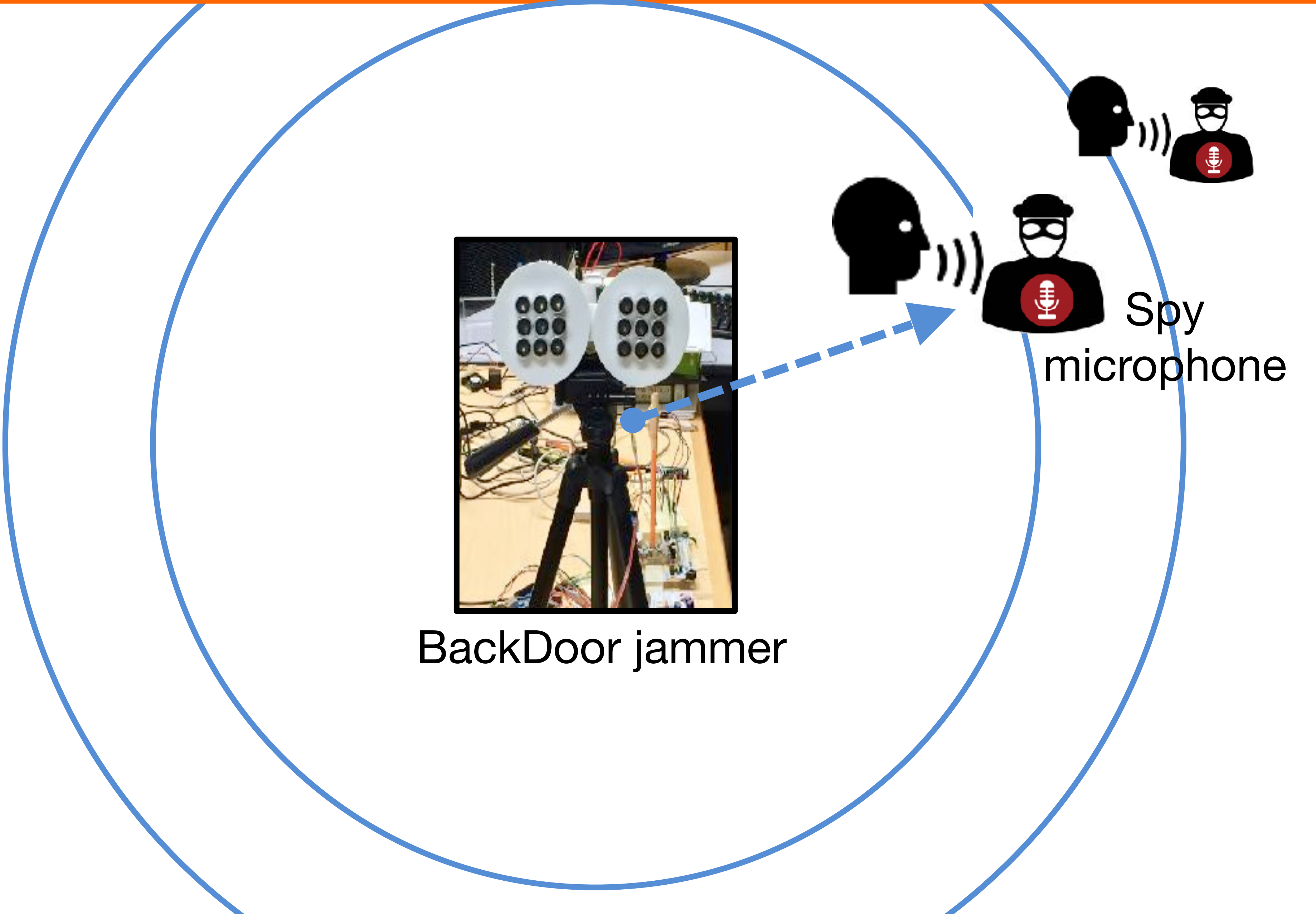
# Jamming performance



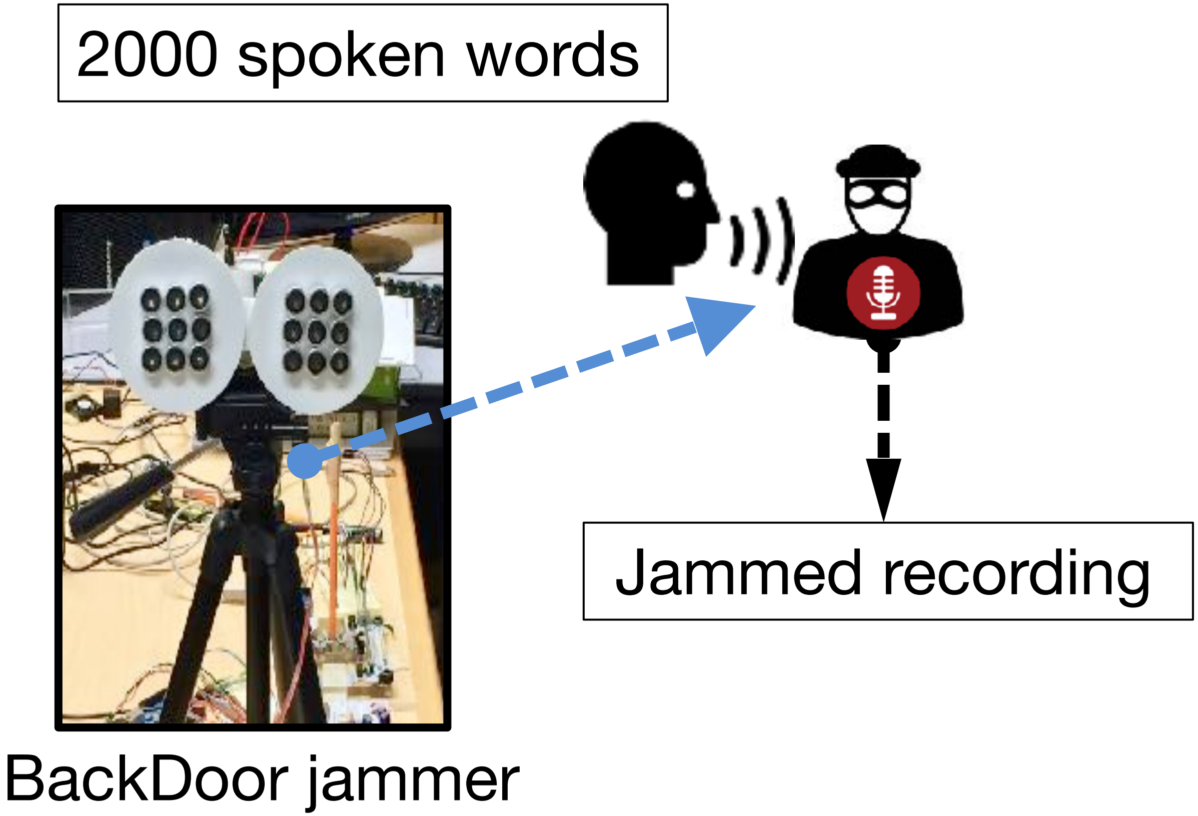
# Jamming performance



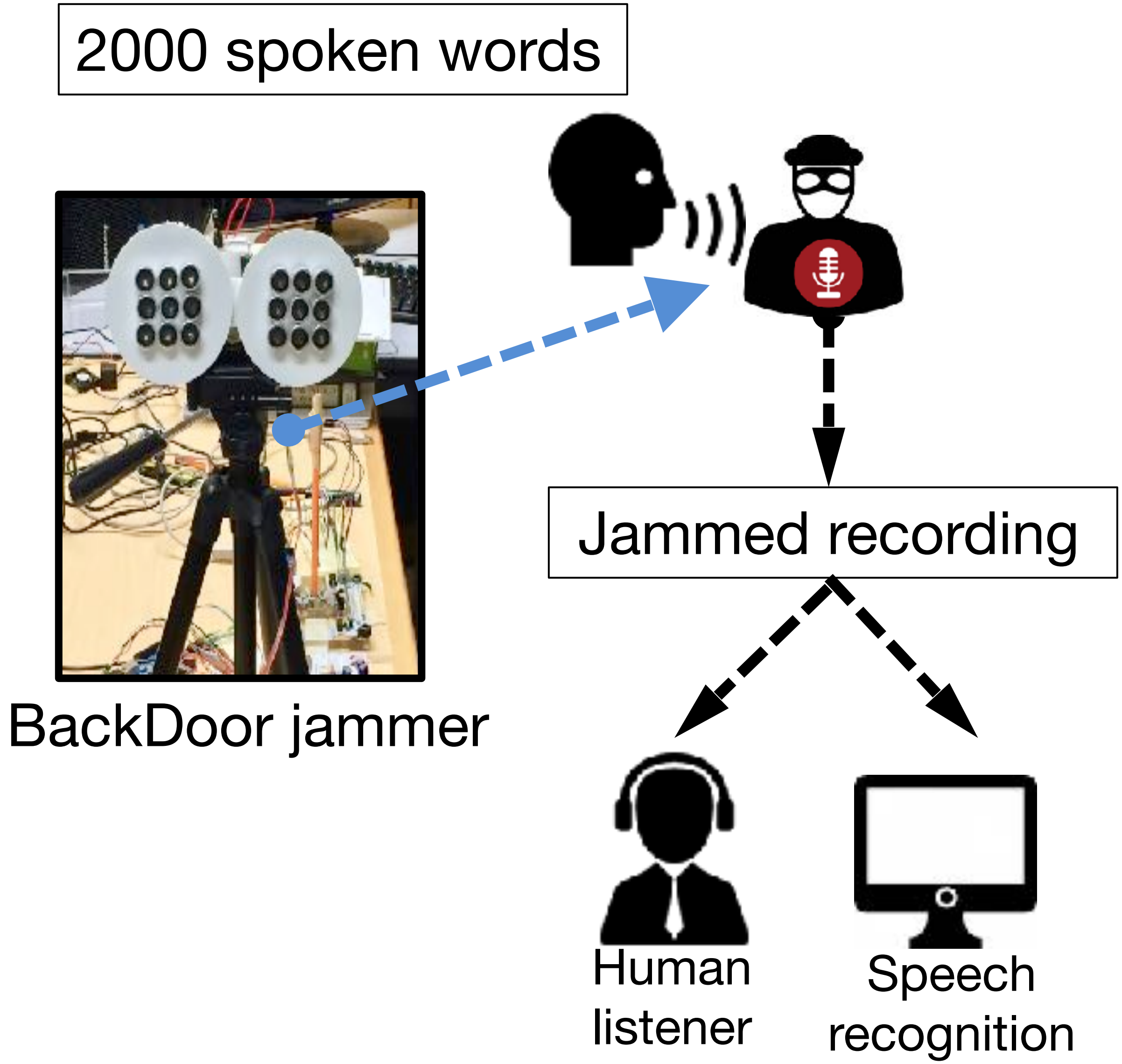
# Jamming performance



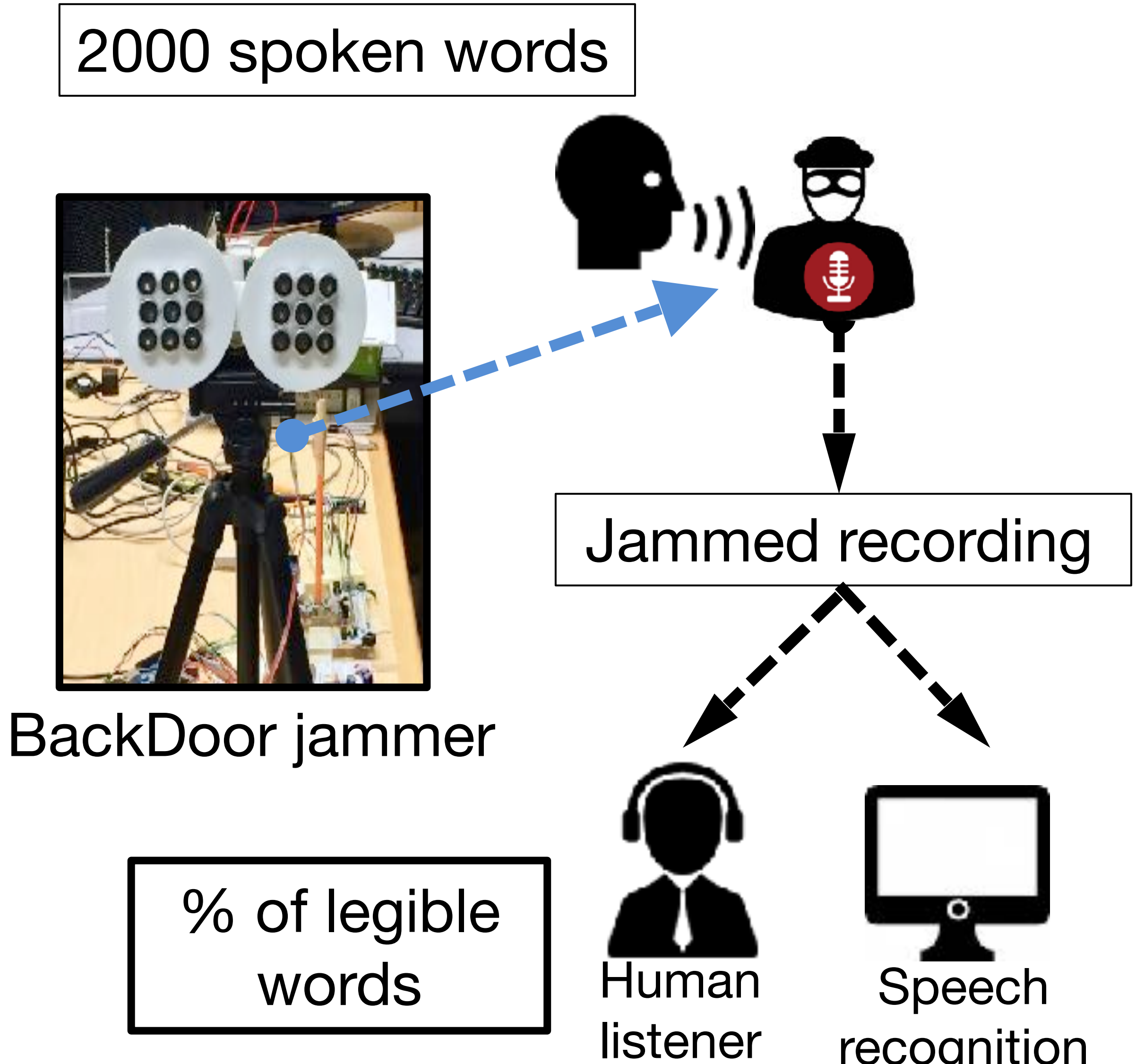
# Jamming performance



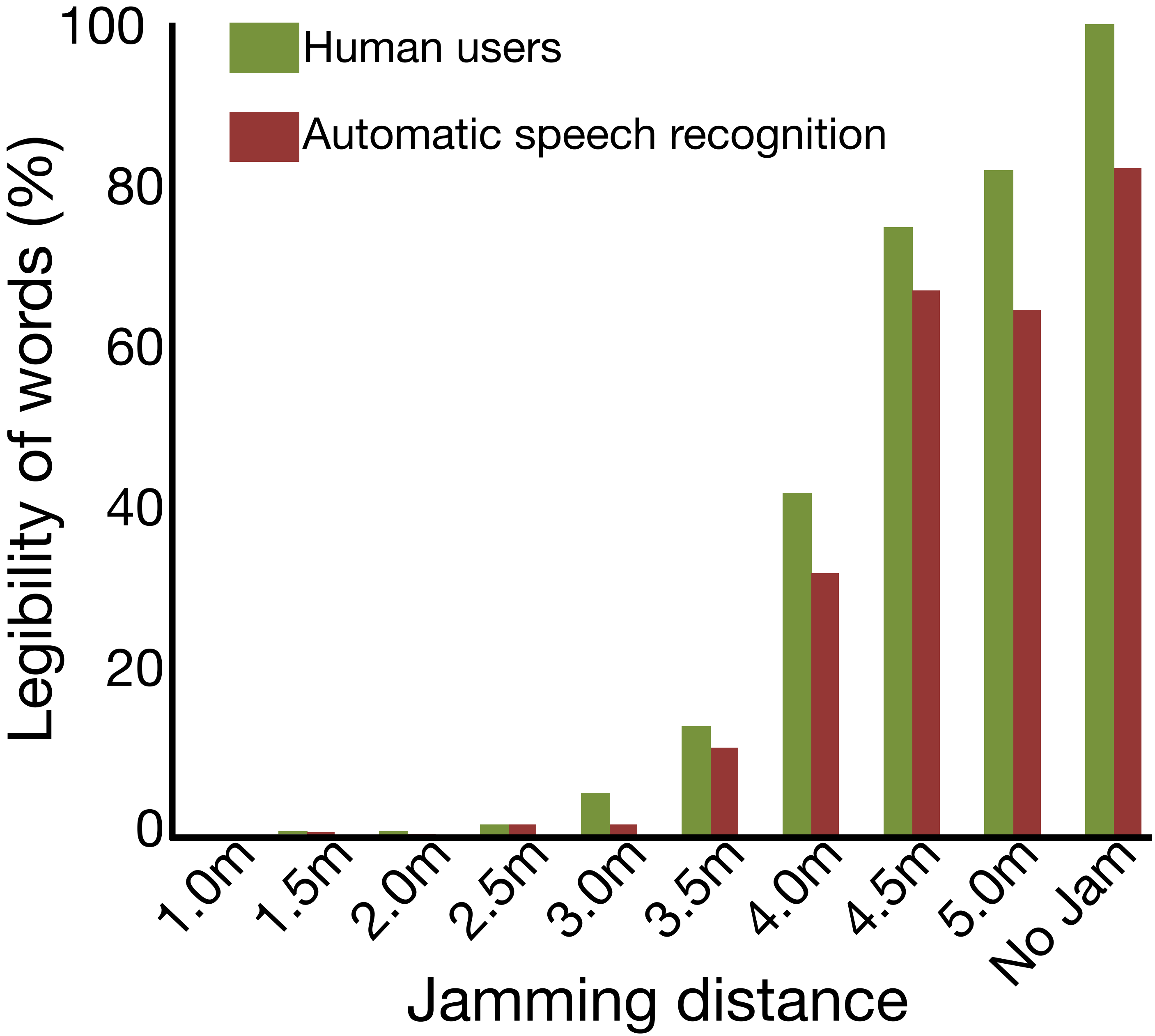
# Jamming performance



# Jamming performance



# Jamming performance



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

# Objectives of Today's Lecture

Learn the fundamentals, applications, and implications of **hacking physical sensors**

1. What are the general principles of injection attacks into physical sensors?
2. What are some examples of injection attacks: GPS, pacemakers, Alexa/Google Home/Fitbit?
3. How do acoustic attacks work on Alexa/Google Home/etc?
4. How can we protect against physical sensor attacks?

# Project Timeline

**Oct. 20**
Project Proposal

**Oct. 24**
Project Meetings

**Nov. 10**
Progress Report 1

**Dec. 2**
Project Report 2

**Dec. 12**
Final Presentation

**Dec. 14**
Final Report

Feedback to refine your ideas

1. Feedback is to help you excel on the final project
2. Project is biggest chunk of class (47%)