CIS 3990

Mobile and IoT Computing

https://penn-waves-lab.github.io/cis3990-24spring

Lecture 12: Security

Instructor: Mingmin Zhao (mingminz@cis.upenn.edu)

TA: Haowen Lai (hwlai@cis.upenn.edu)

Some material adapted from Omid Abari (UCLA)

Mobile Security
Inaudible Voice Commands

Light Commands
Hacking using Laser

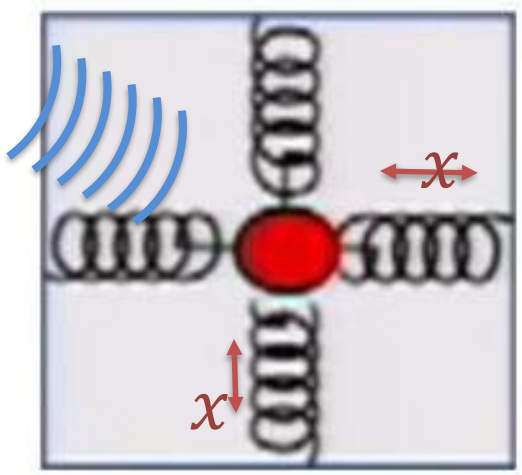

UEC
TOKYO
CSE
COMPUTER SCIENCE
AND ENGINEERING
UNIVERSITY OF MICHIGAN


LIGHT
COMMANDS

Analog Sensor Security
Acoustic Attacks on MEMS Accelerometers


TITANIUM BULLET TWEETER
PYRAMID

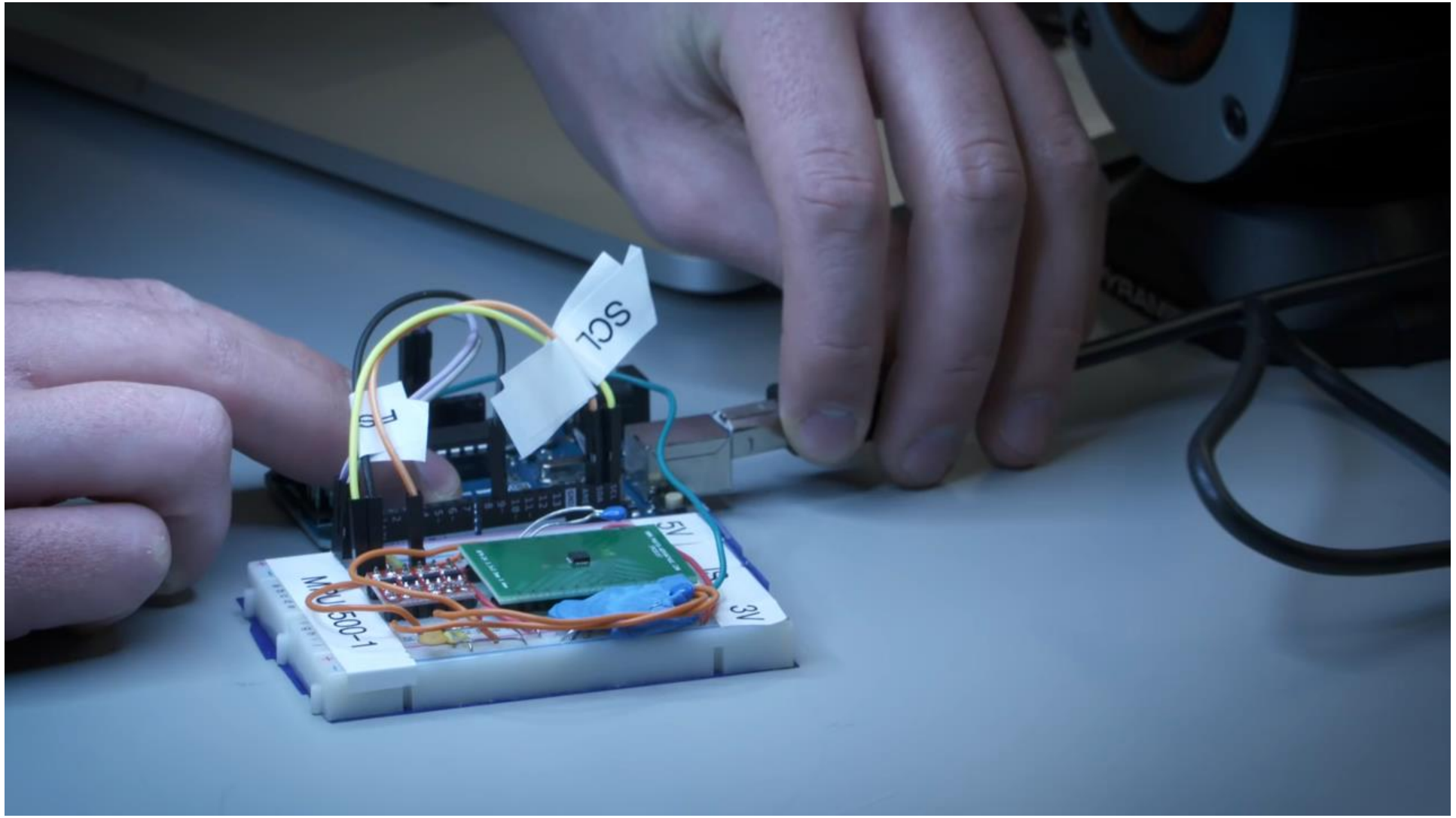
Acoustic
"pressure" waves



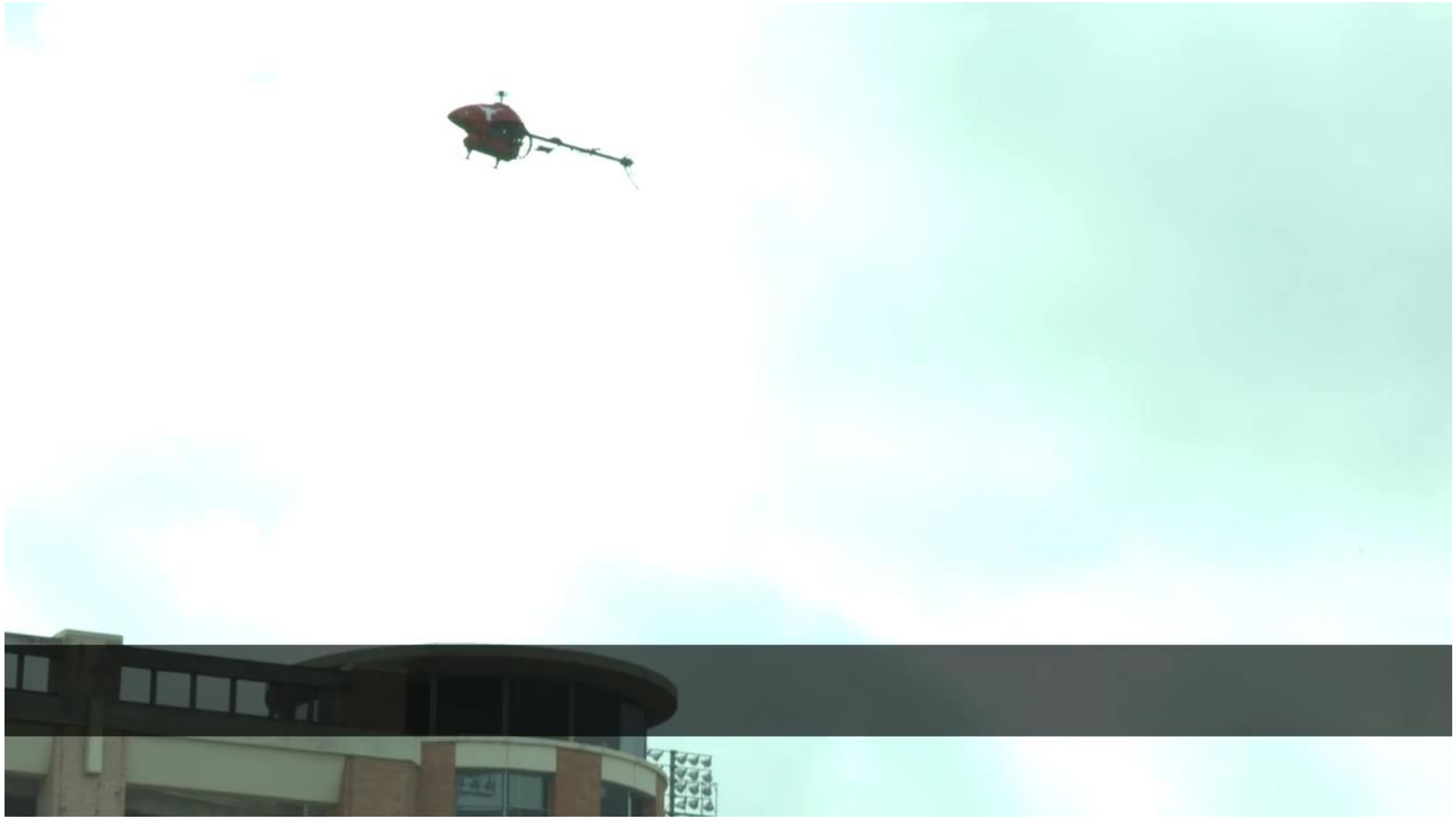
$$F = ma = kx$$

acceleration

measure
displacement

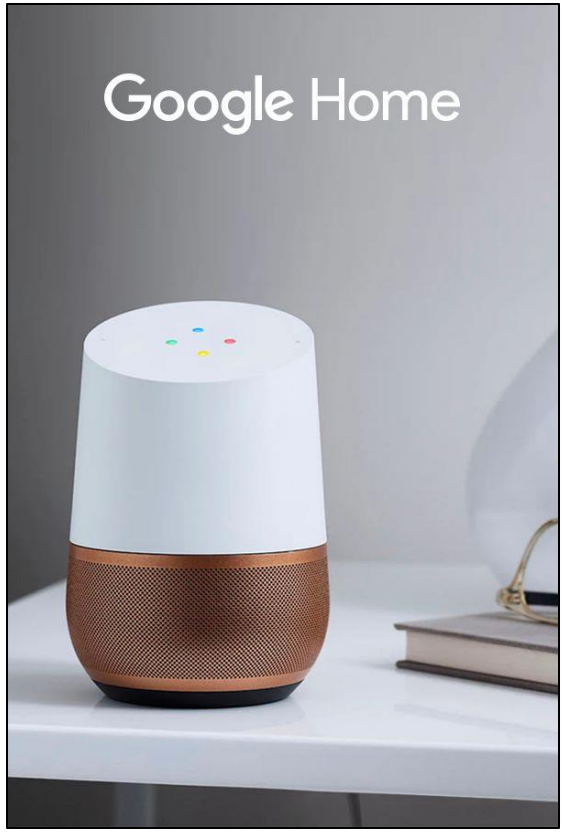

SCL
5V
3V
MPU 6500-1

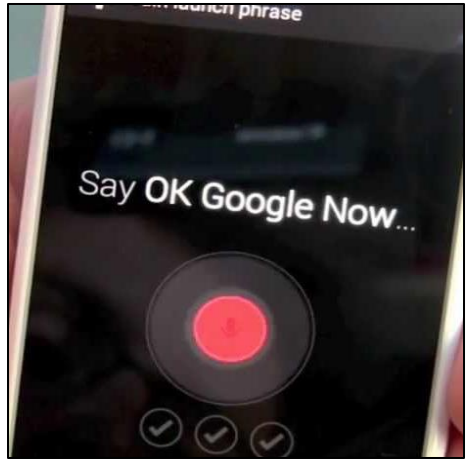
Drone Security
Spoofing GPS Signals

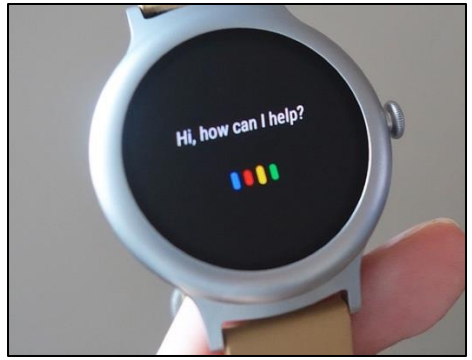


BackDoor: Making Microphones Hear Inaudible Sounds

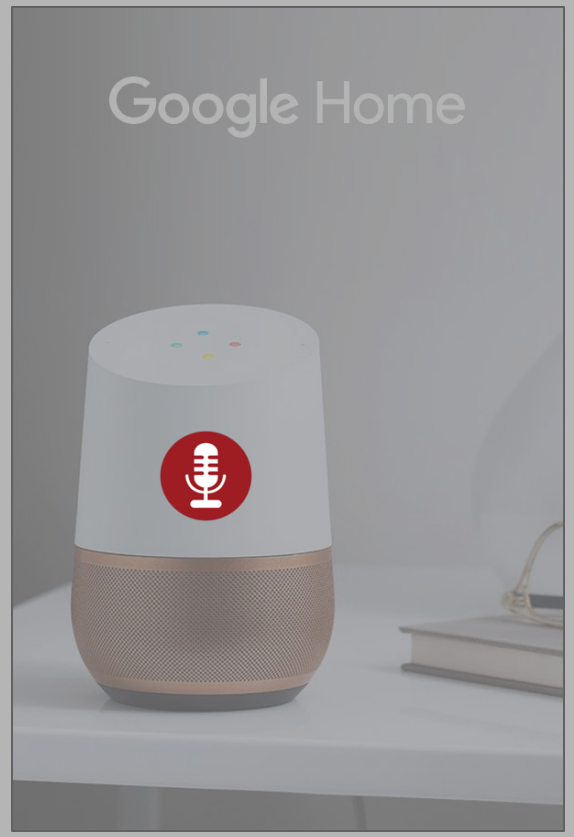
Microphones are everywhere

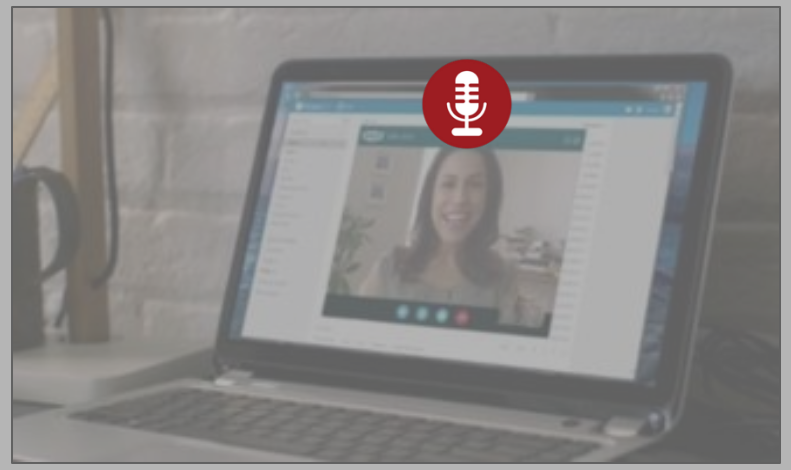


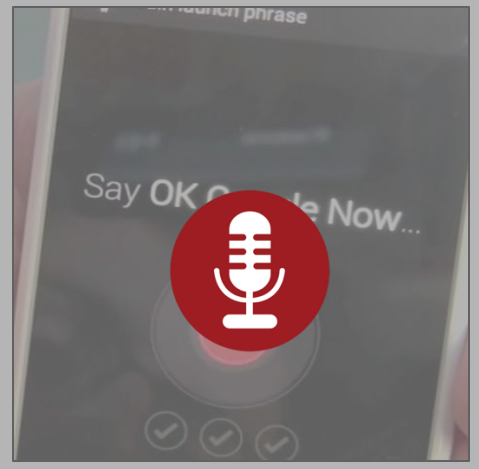


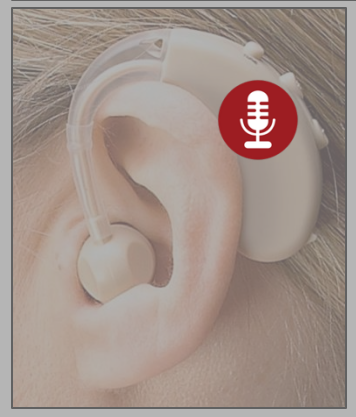


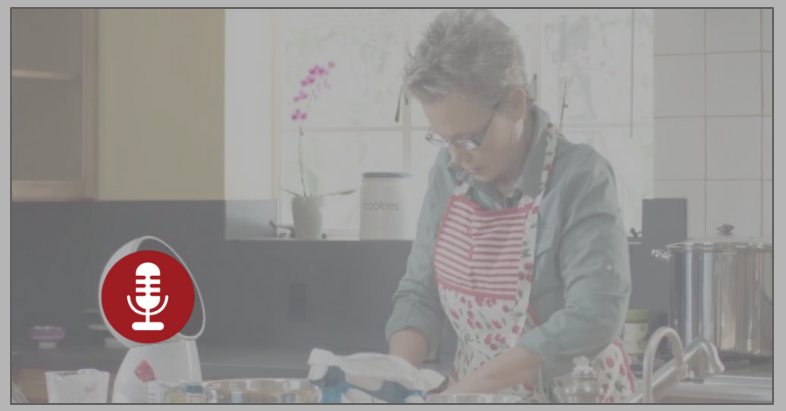
Microphones are everywhere



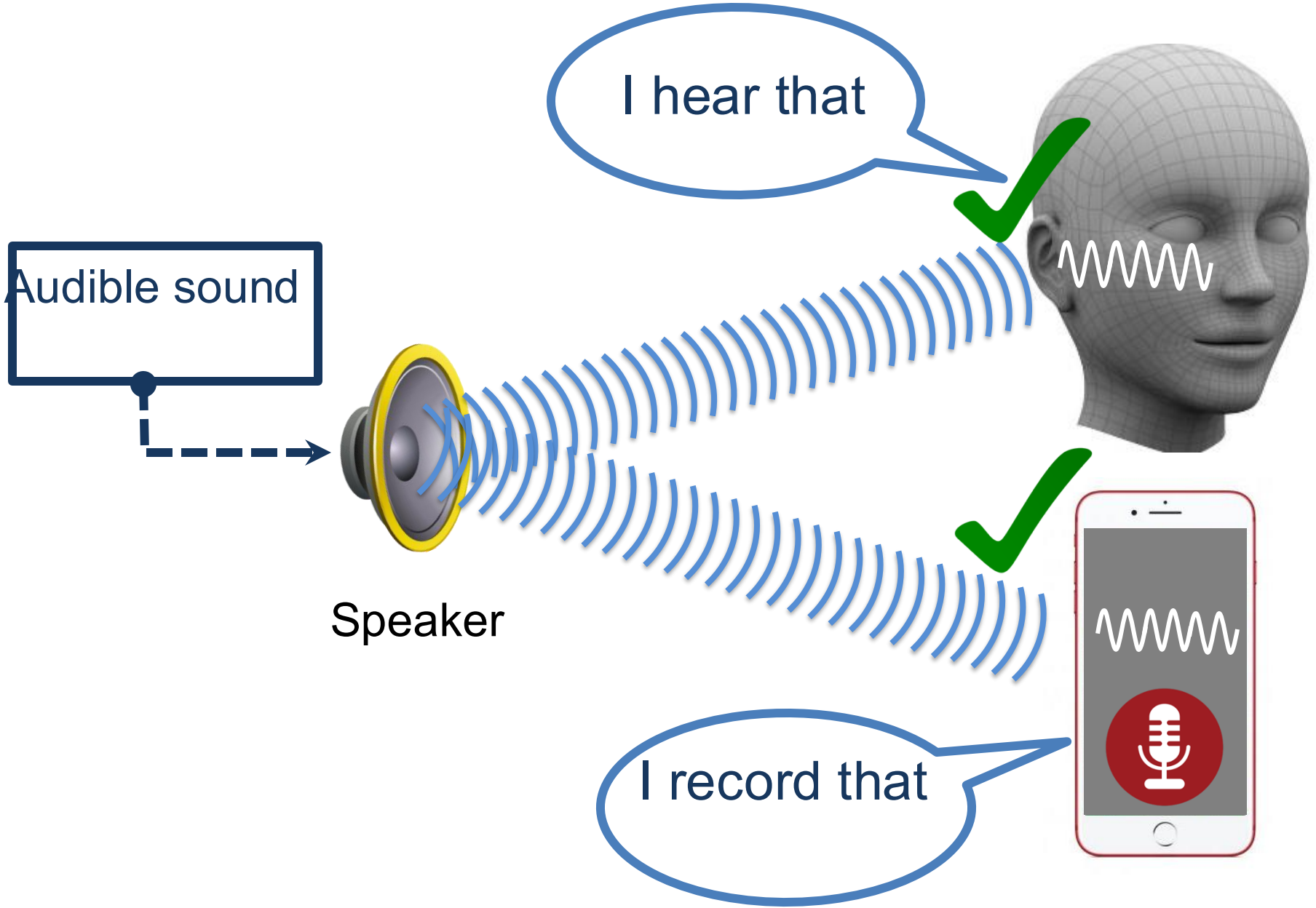




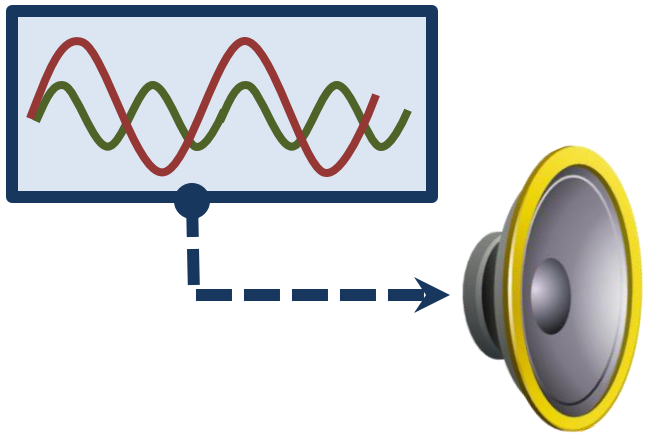




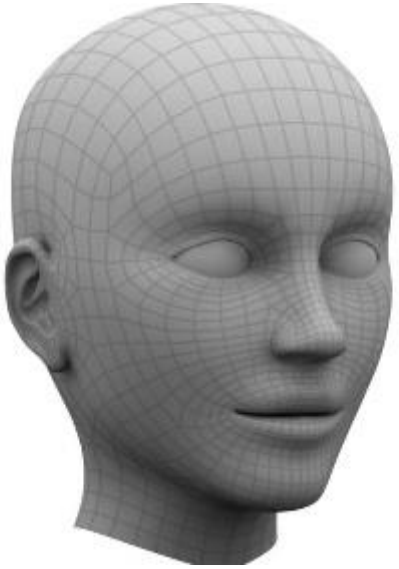
Microphones record audible sounds



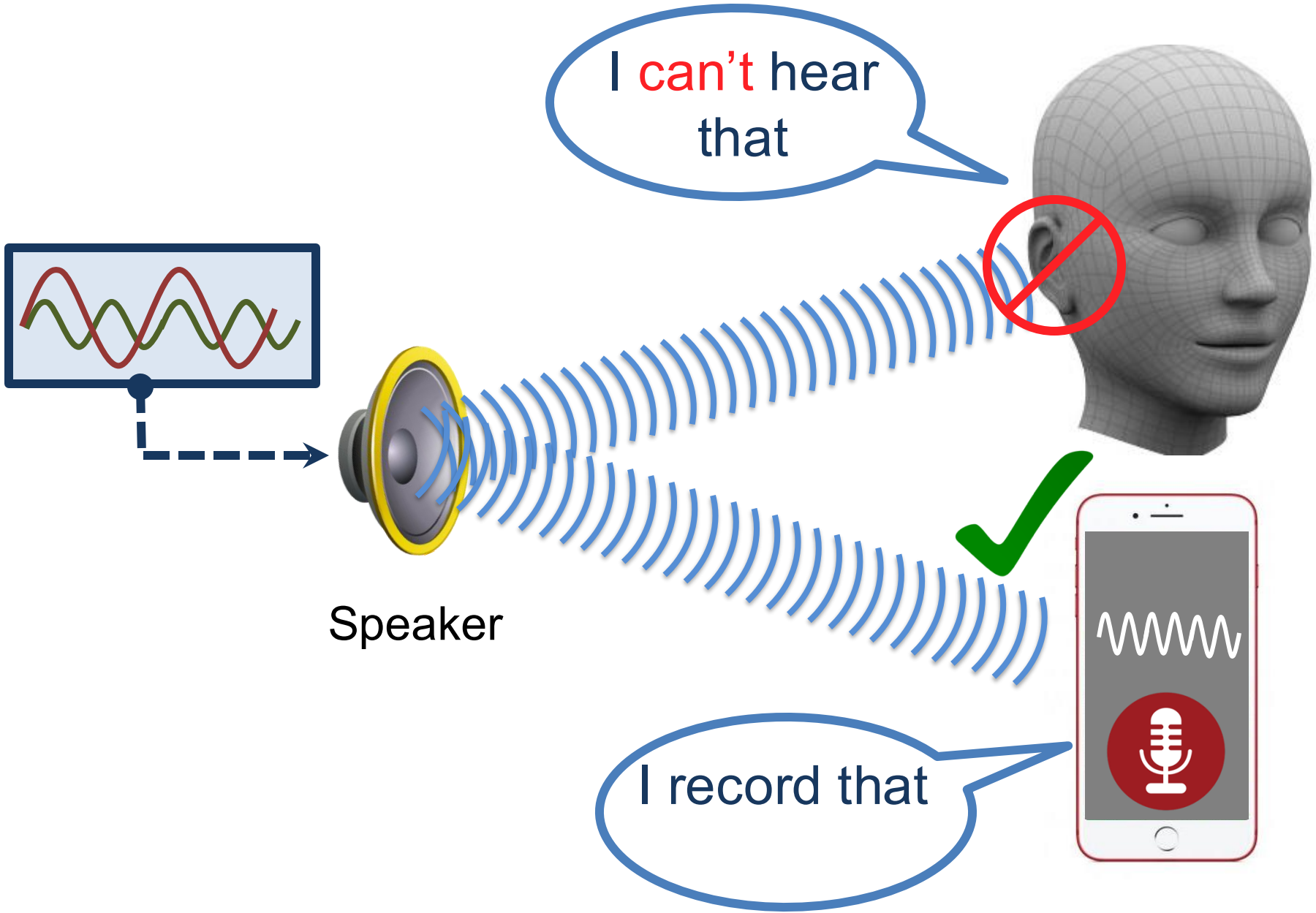
Inaudible, but recordable !



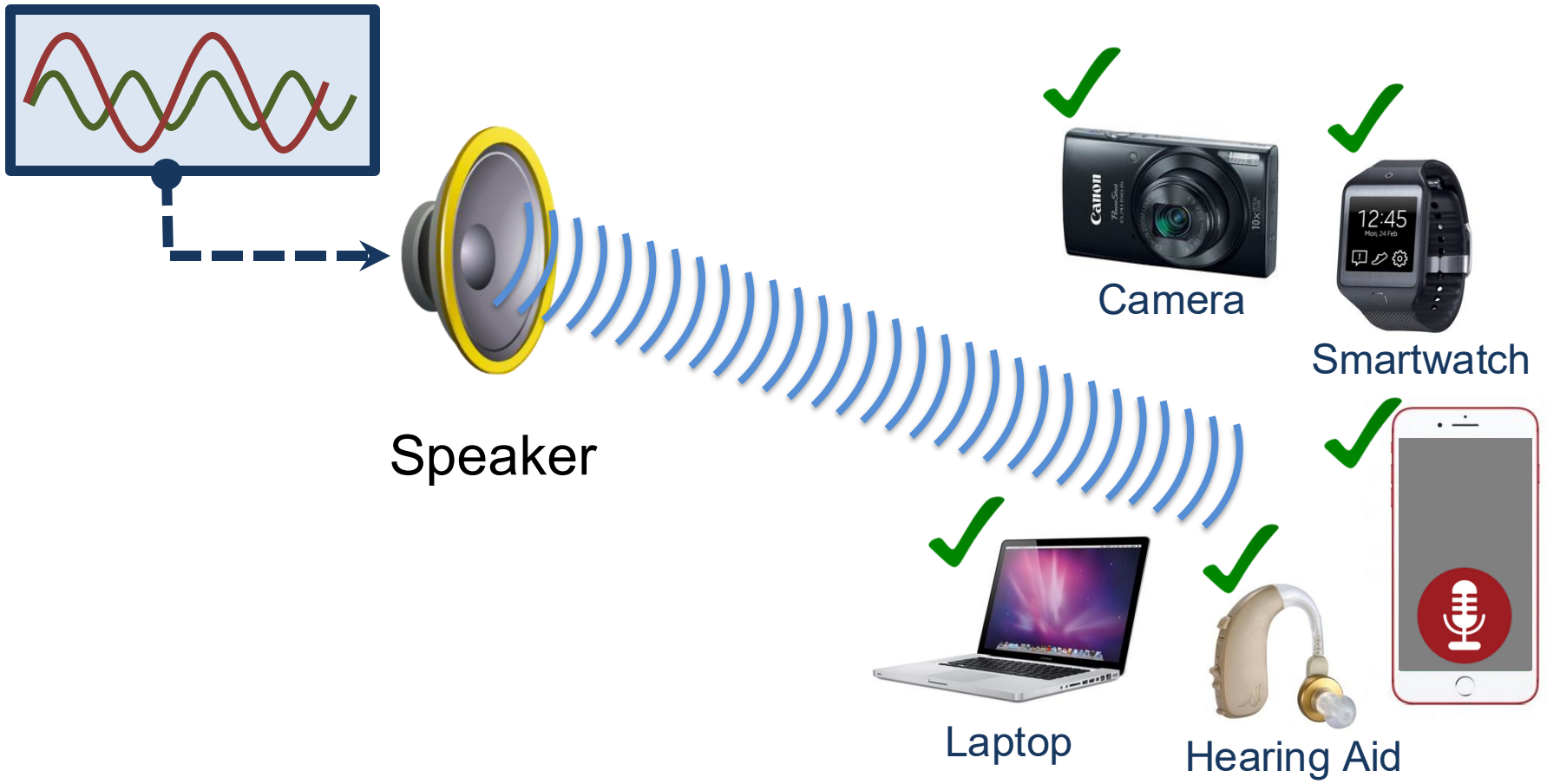
Speaker



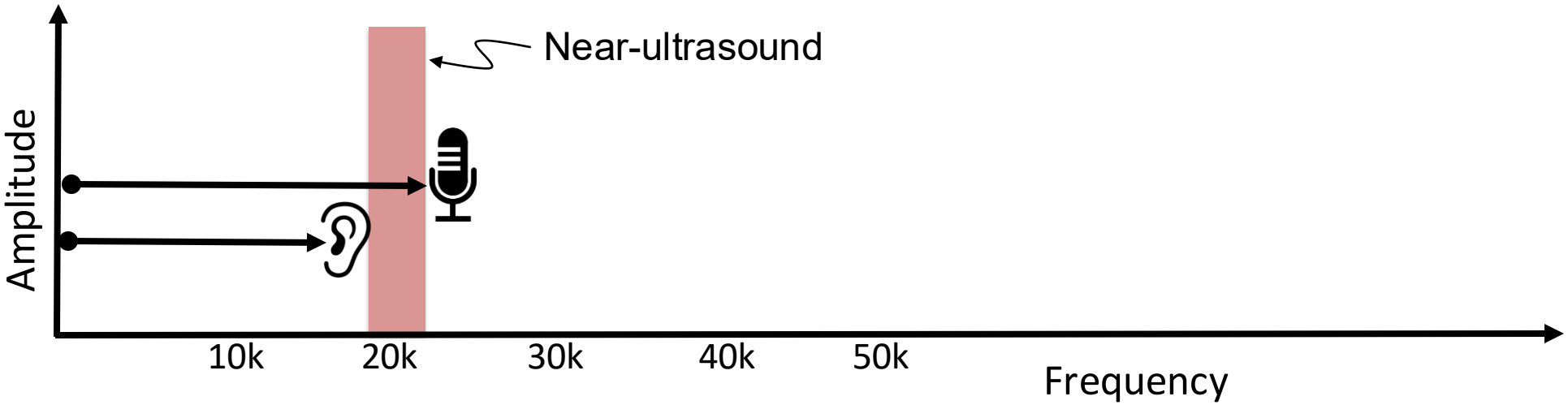
Inaudible, but recordable !



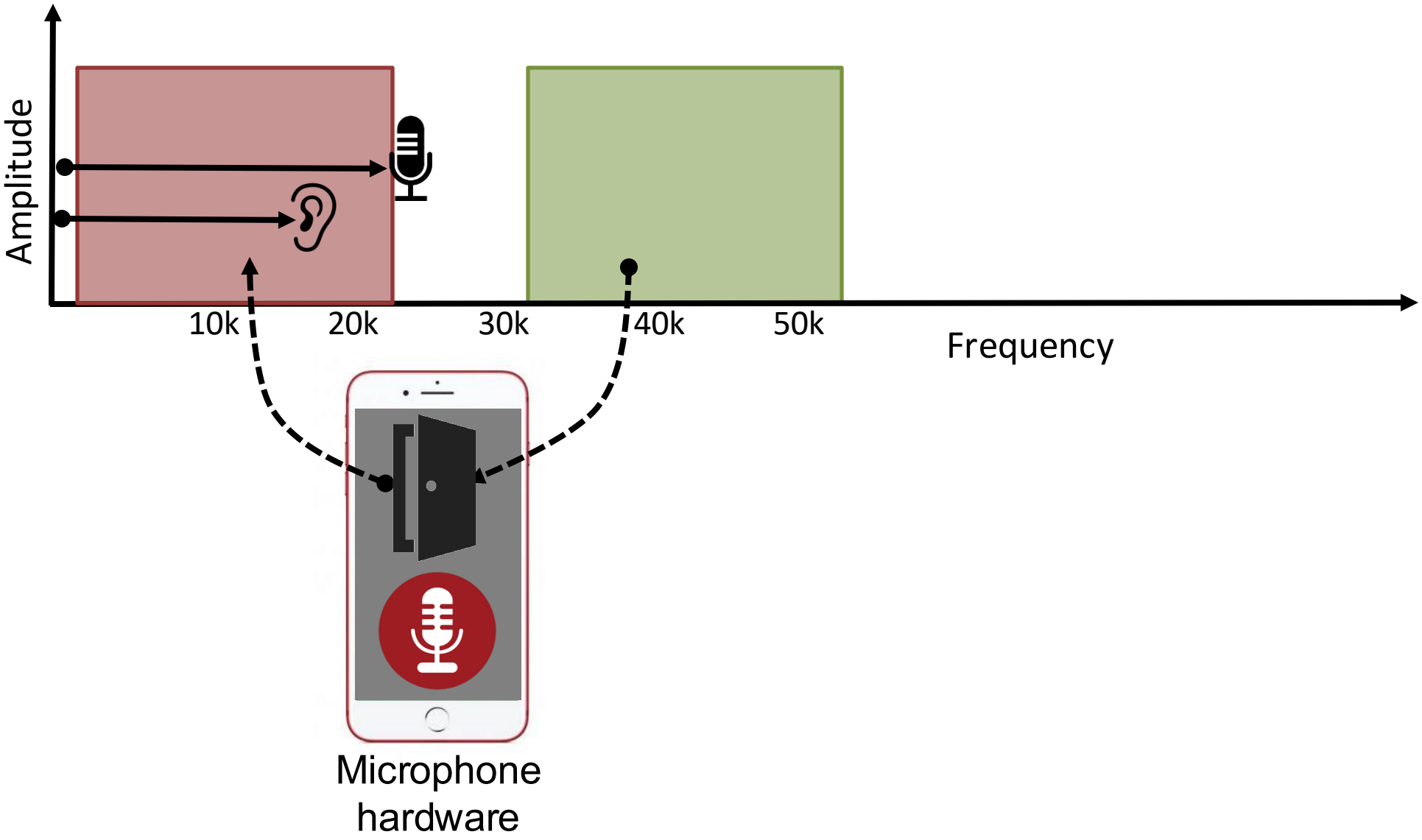
Works with unmodified devices



It's not "near-ultrasound"

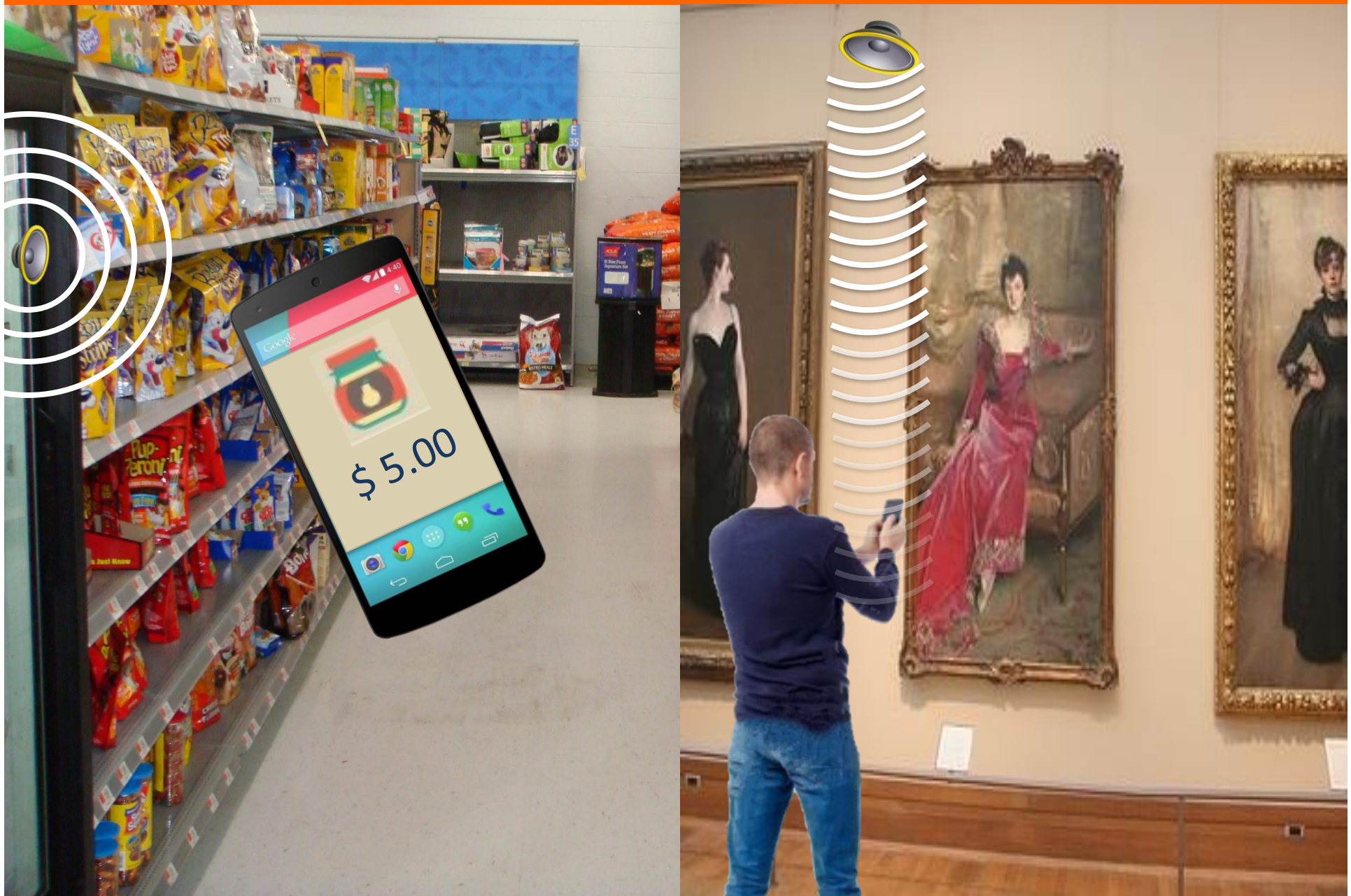


Exploiting fundamental nonlinearity

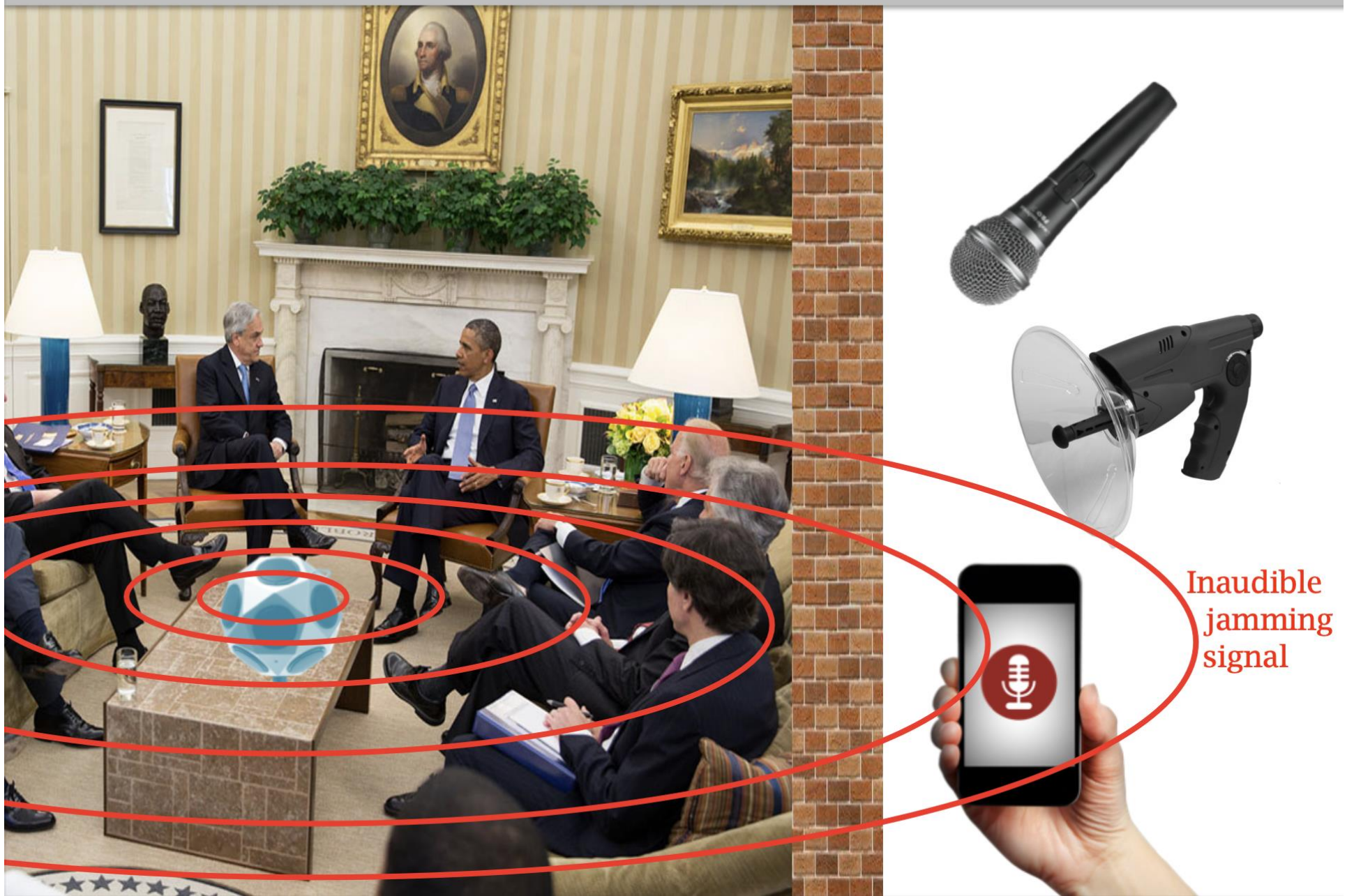


What can we do with it?

Application: Acoustic communication



Protecting Privacy (Inaudible Jammer)



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

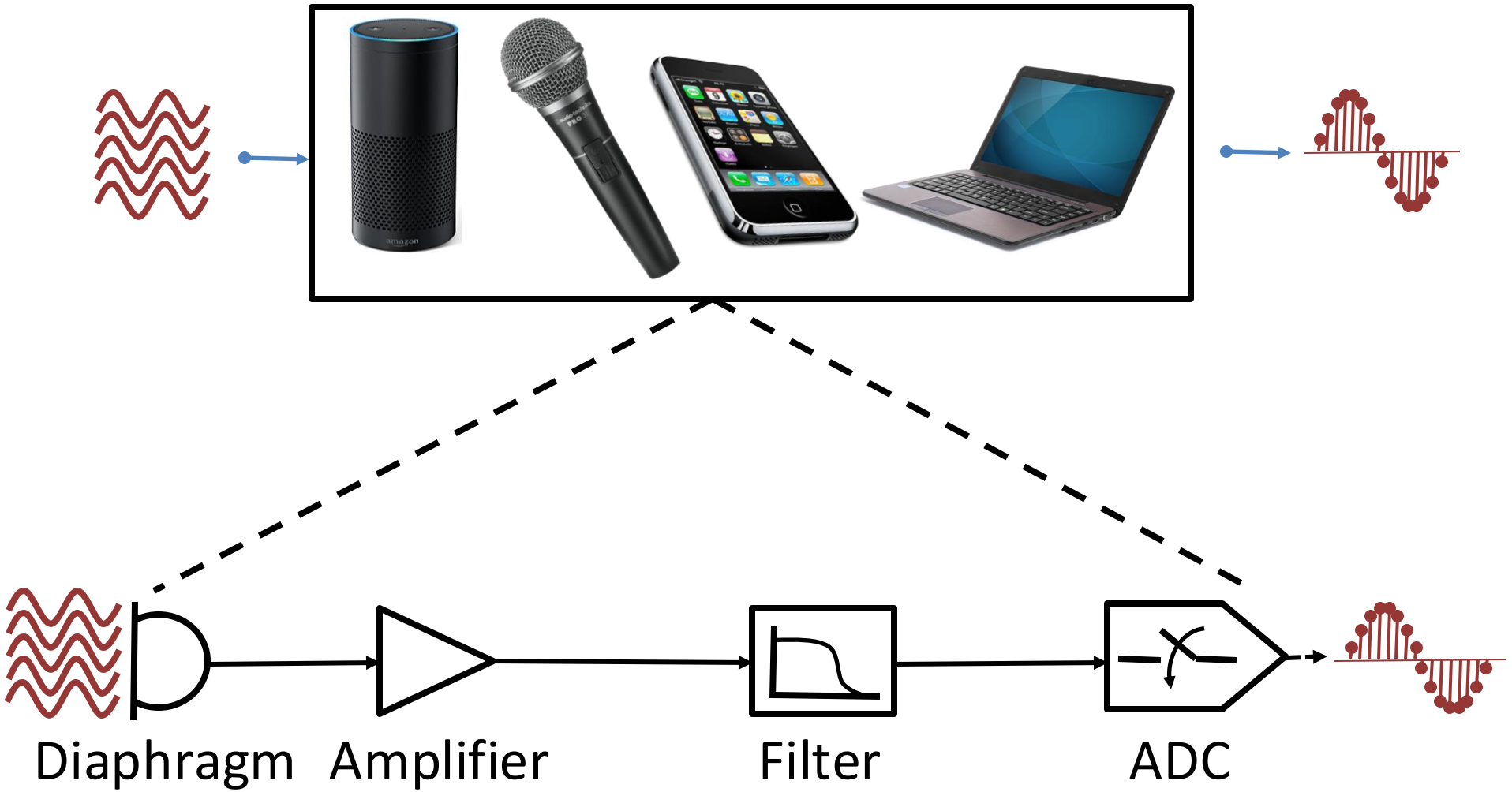
① Microphone Overview

② System Design

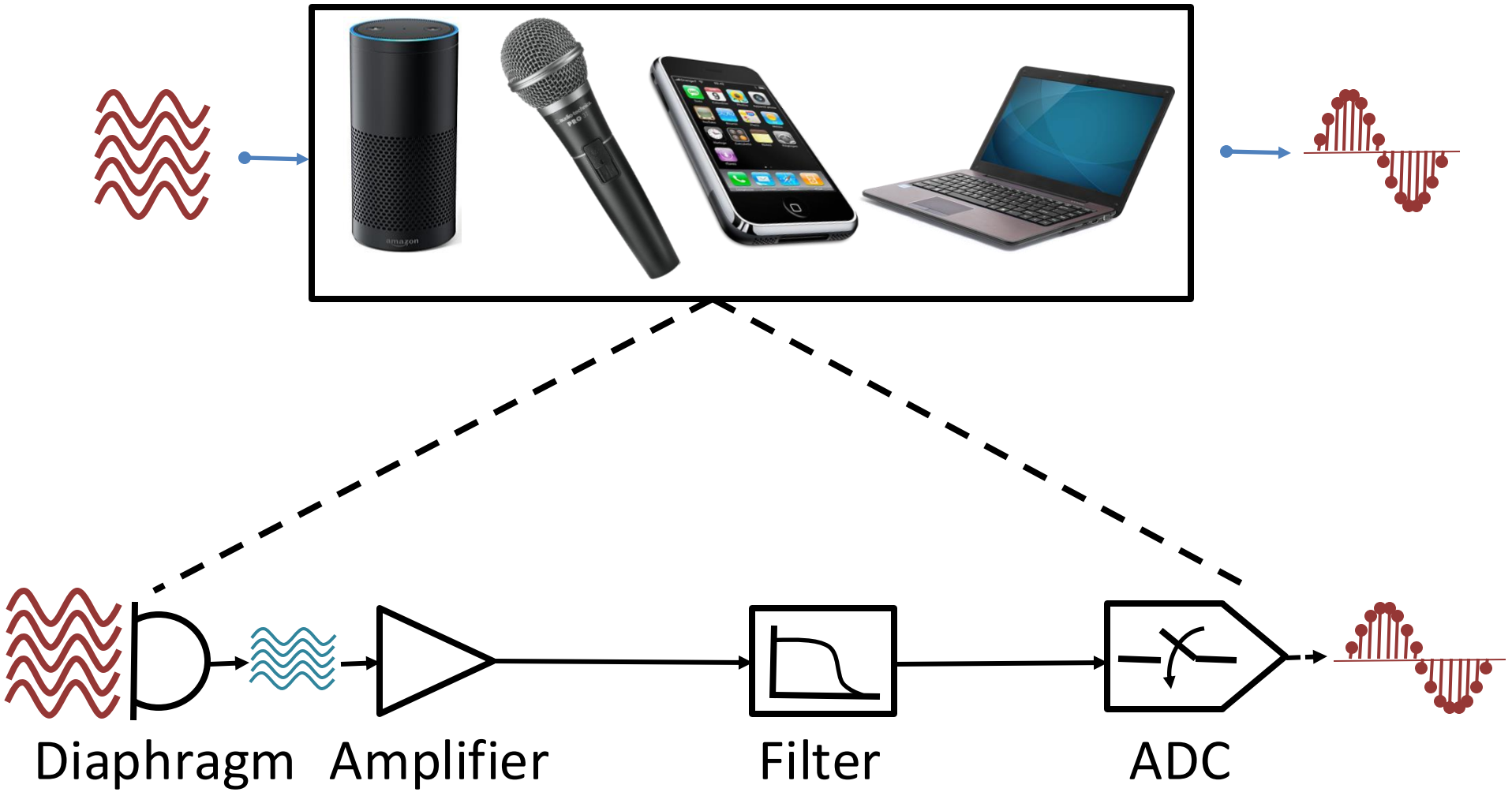
③ Challenges

④ Evaluation

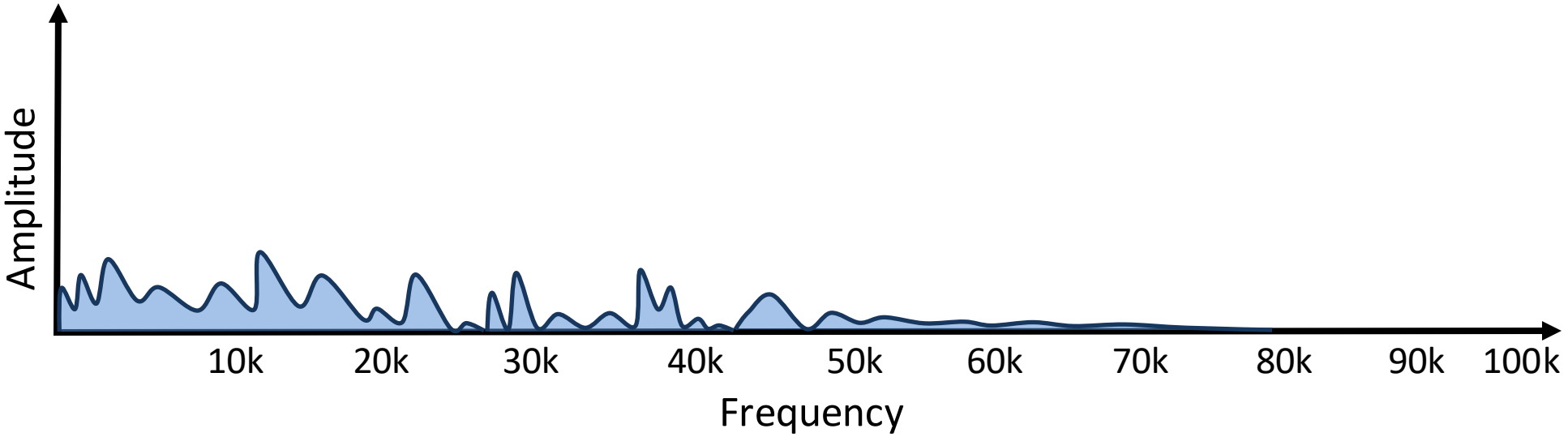
Microphone working principle

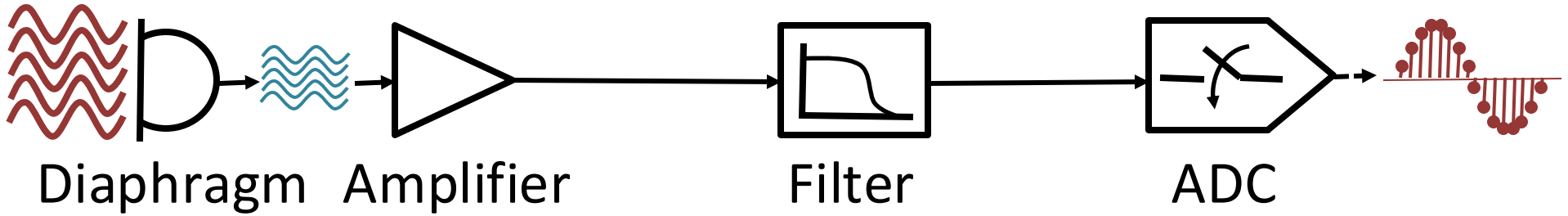


Microphone working principle

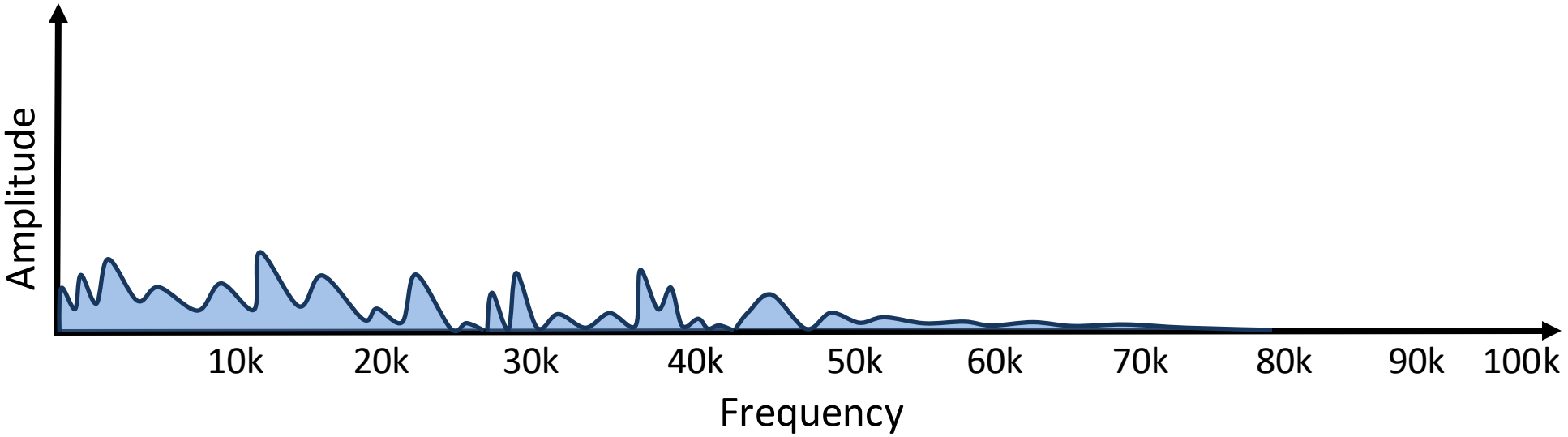


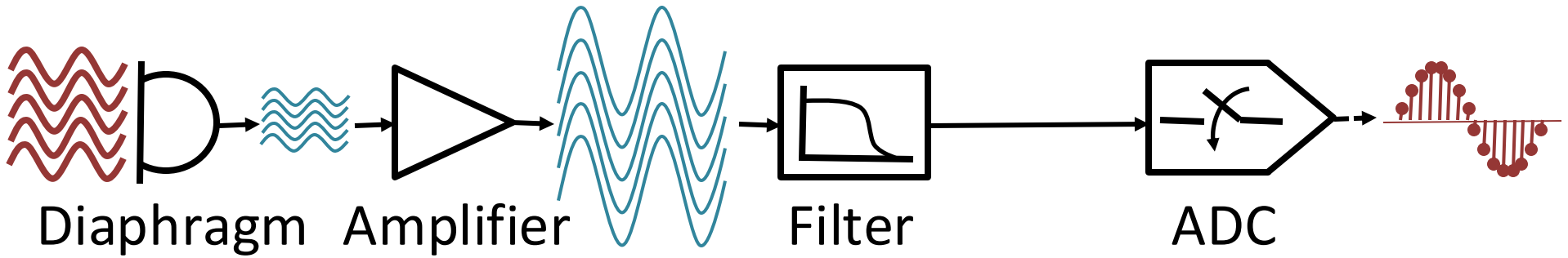
Microphone working principle



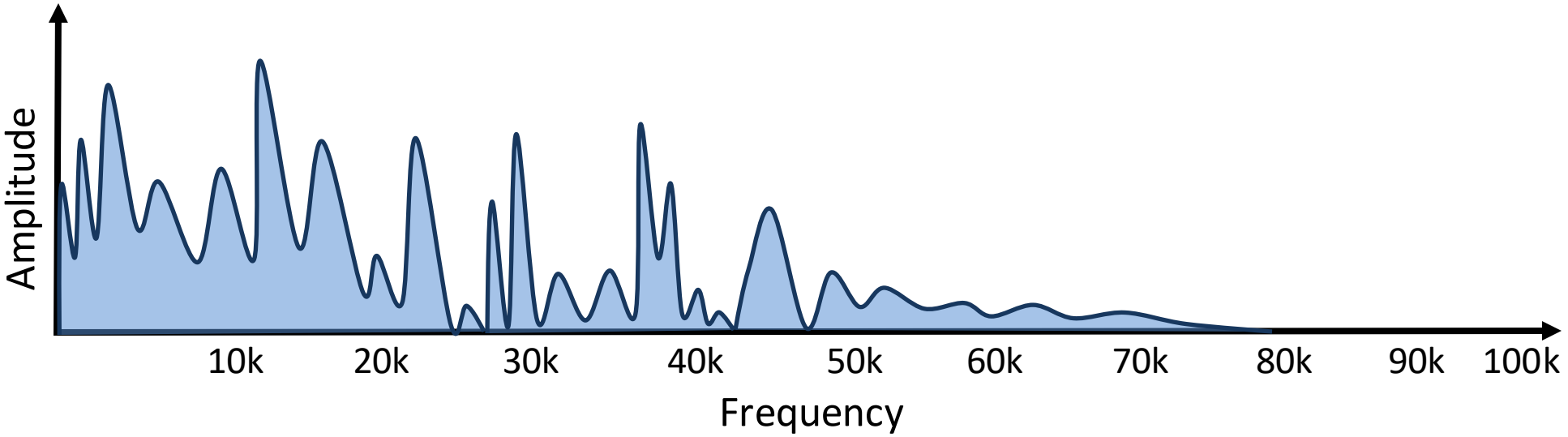


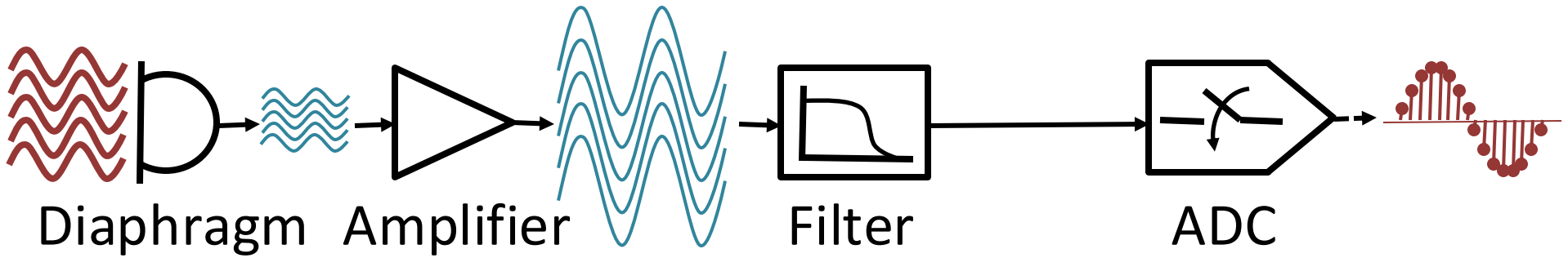
Microphone working principle



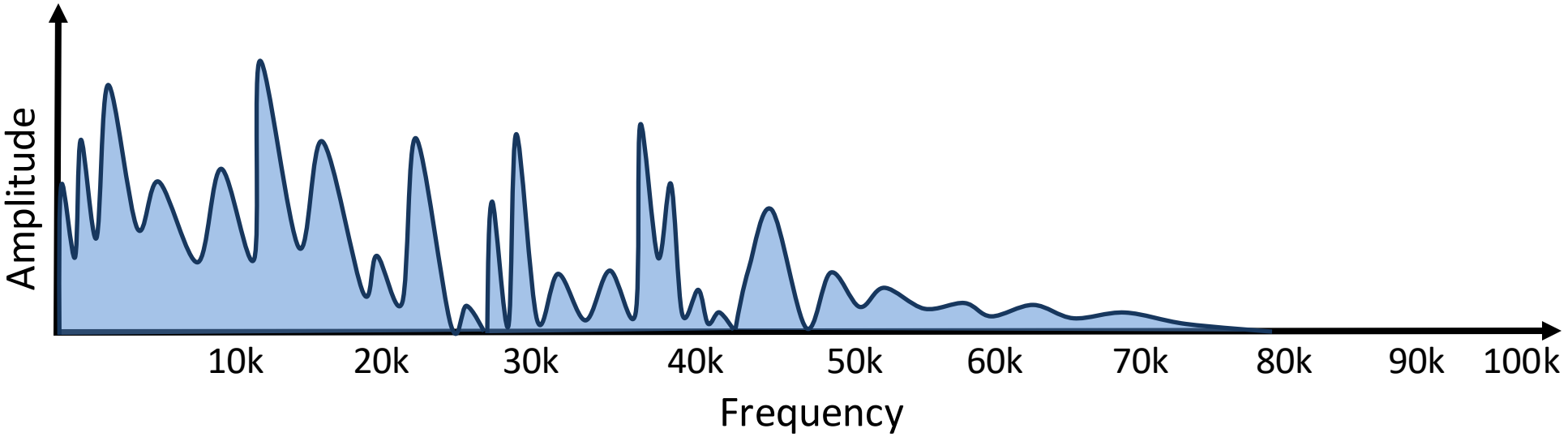


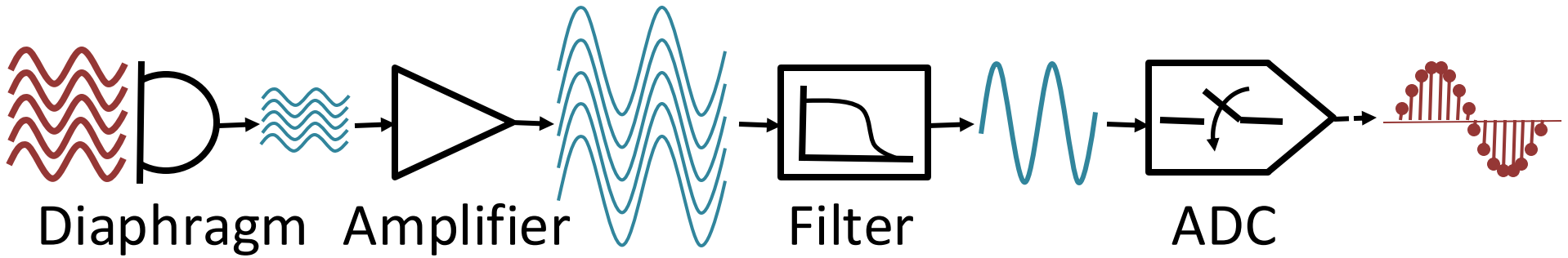
Microphone working principle



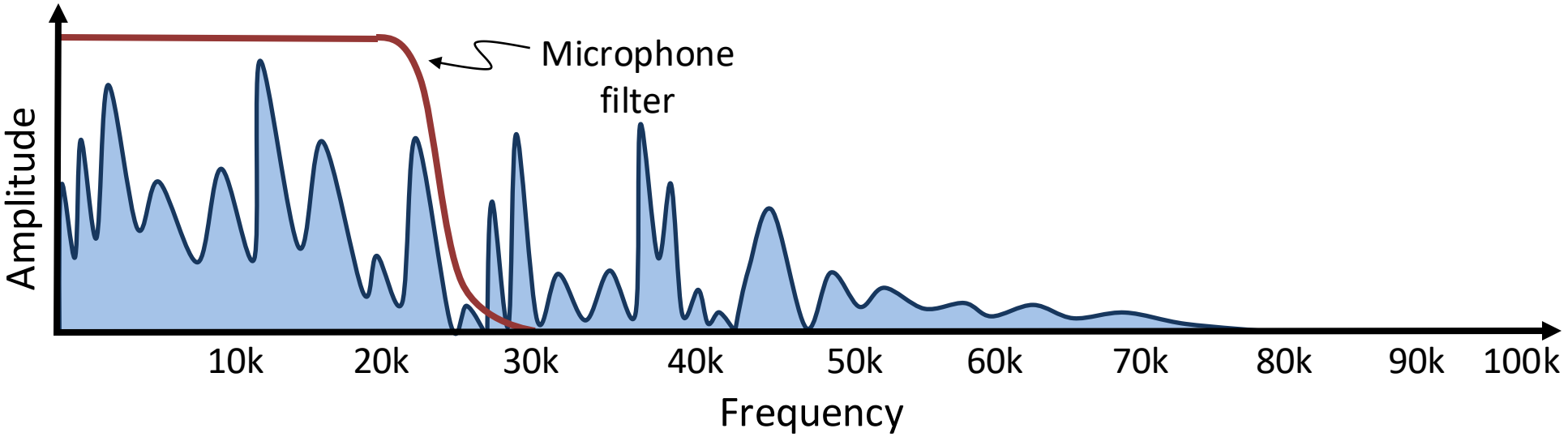


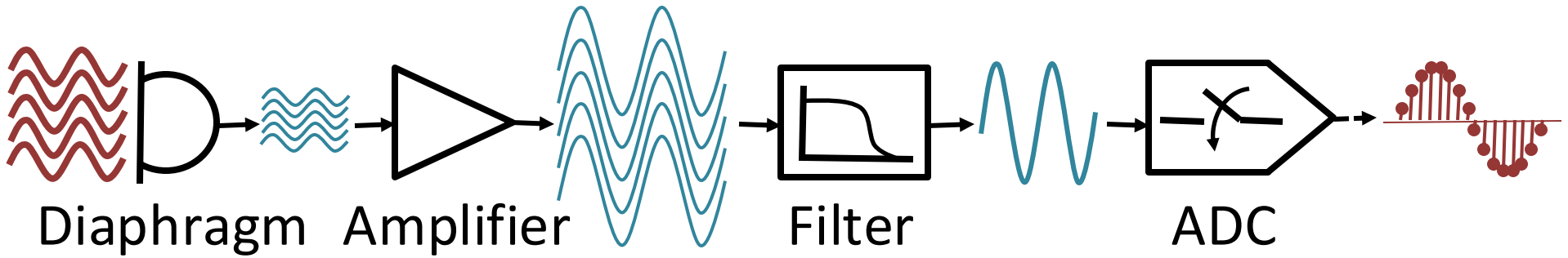
Microphone working principle



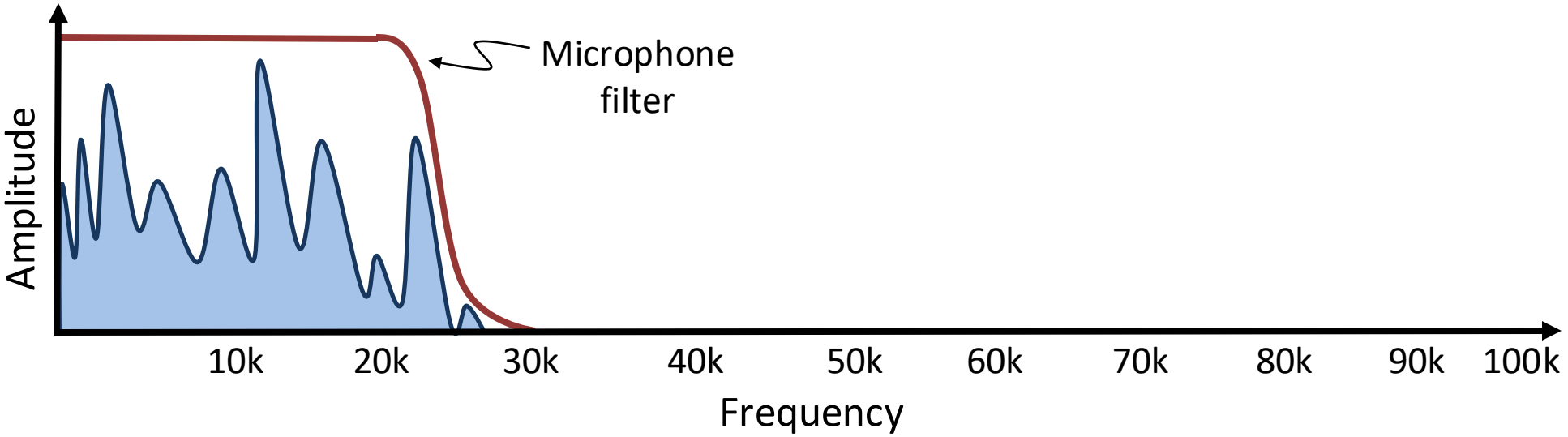


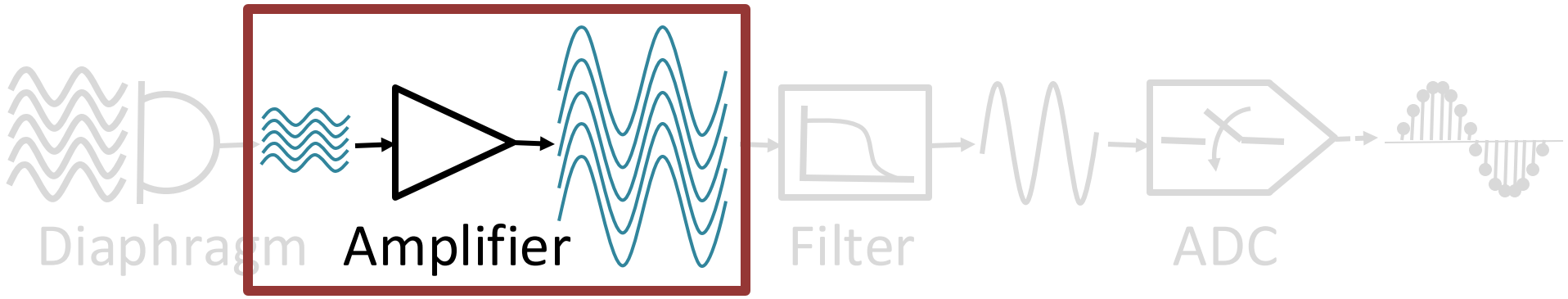
Microphone working principle



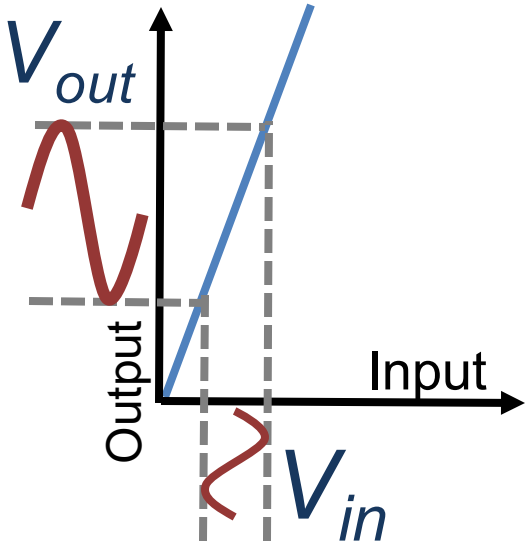


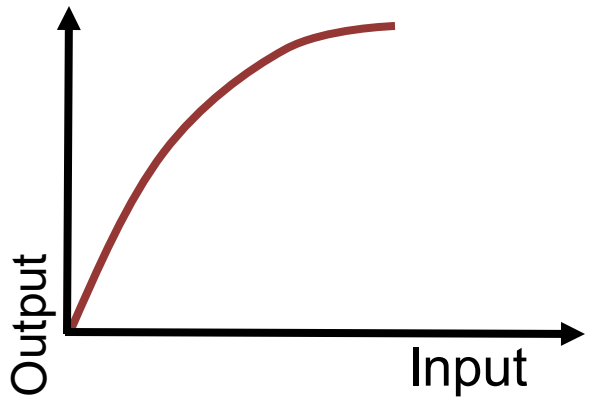
Microphone working principle





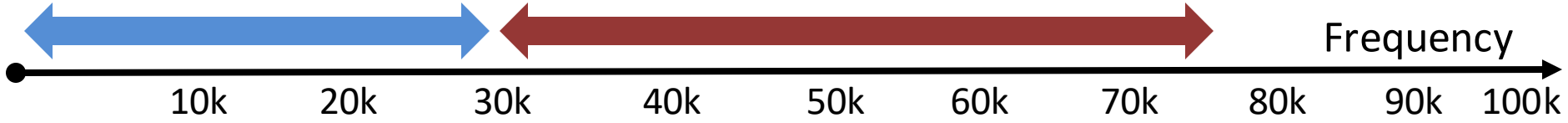
Microphone working principle

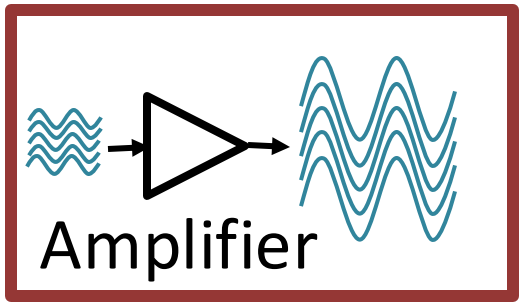




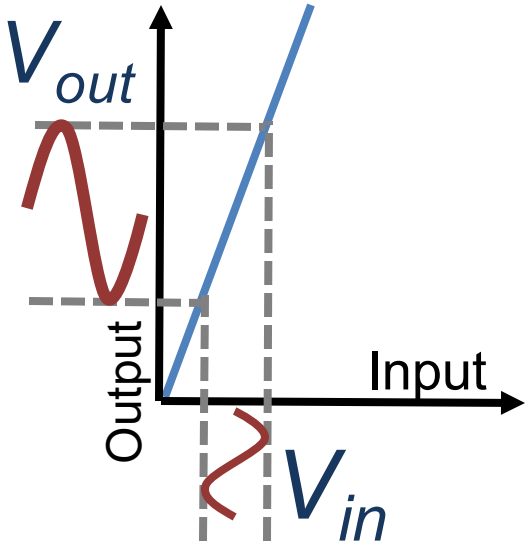
$V_{out} = a_1 V_{in}$

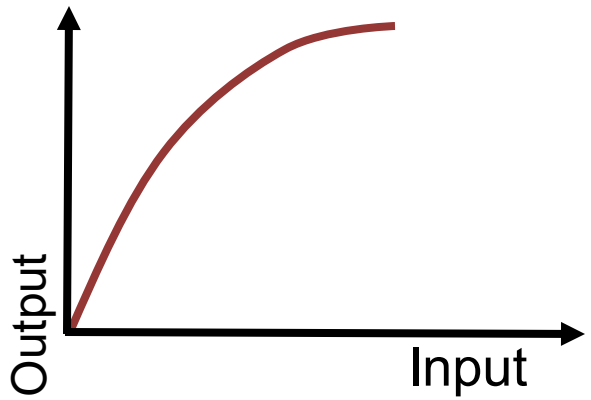
$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$





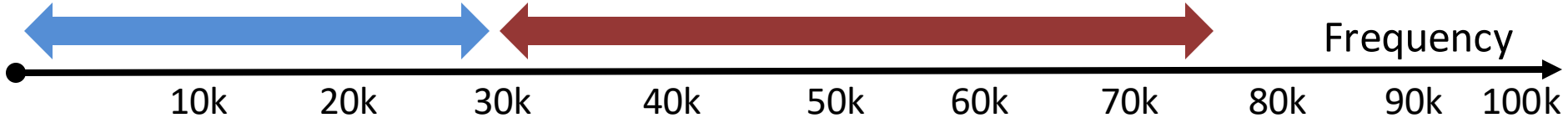
Microphone working principle

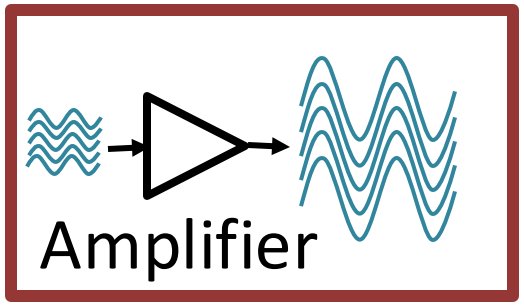




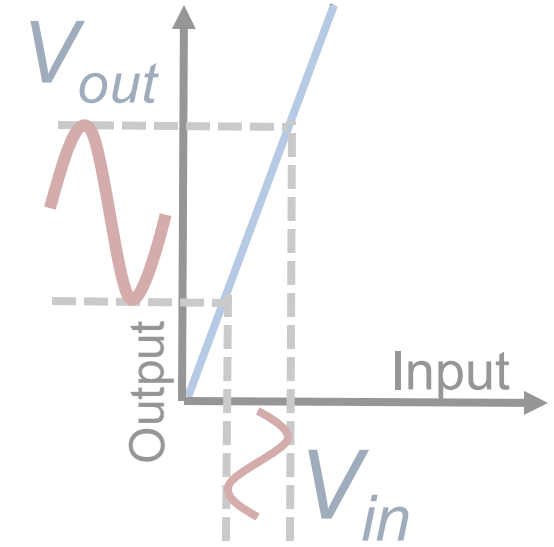
$V_{out} = a_1 V_{in}$

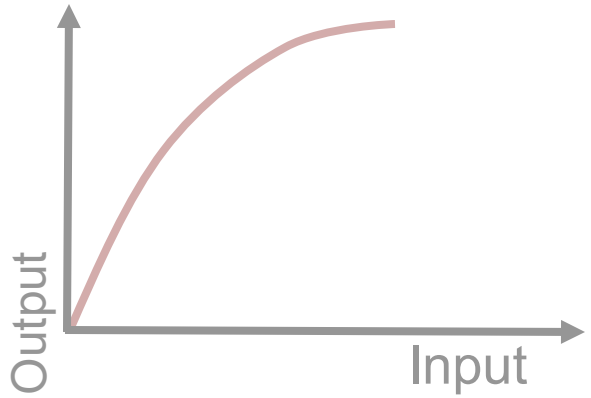
$V_{out} = a_1 V_{in} + a_2 V_{in}^2$





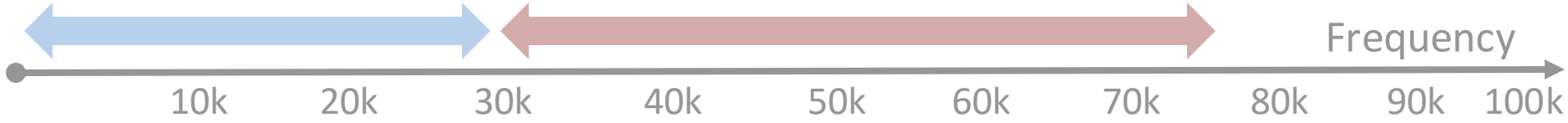
Microphone working principle

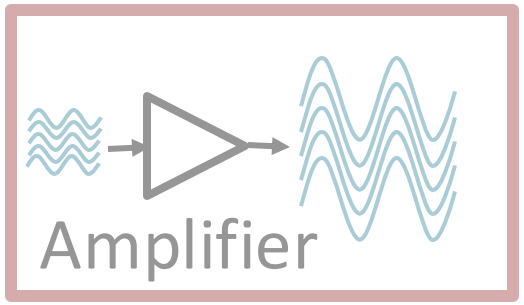




$V_{out} = a_1 V_{in}$

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





Talk outline

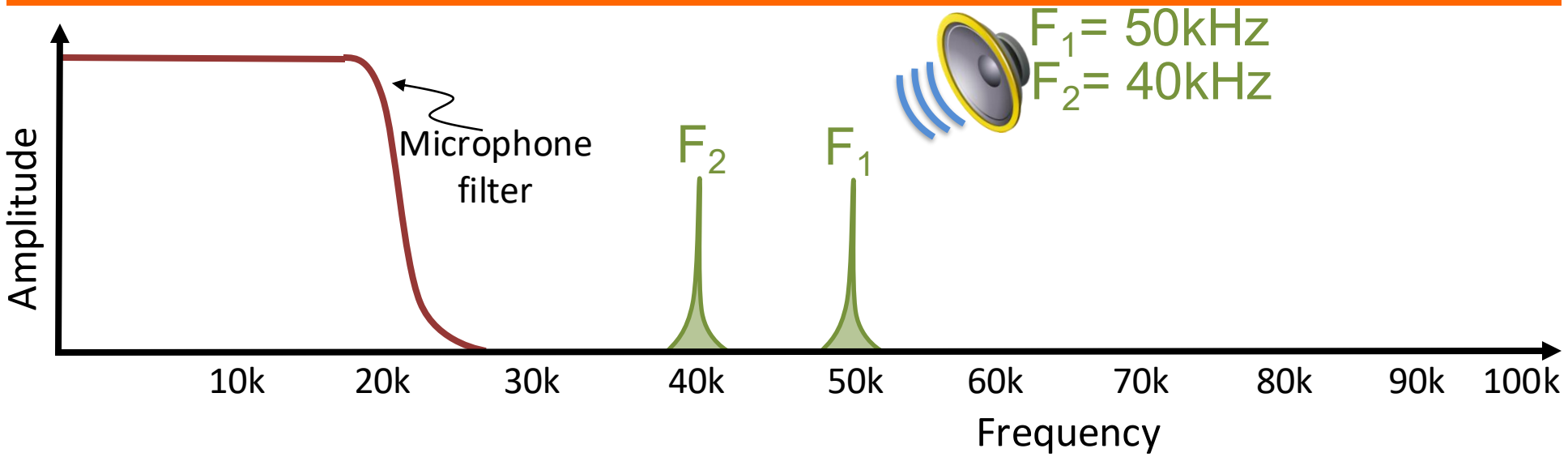
① Microphone Overview

② System Design

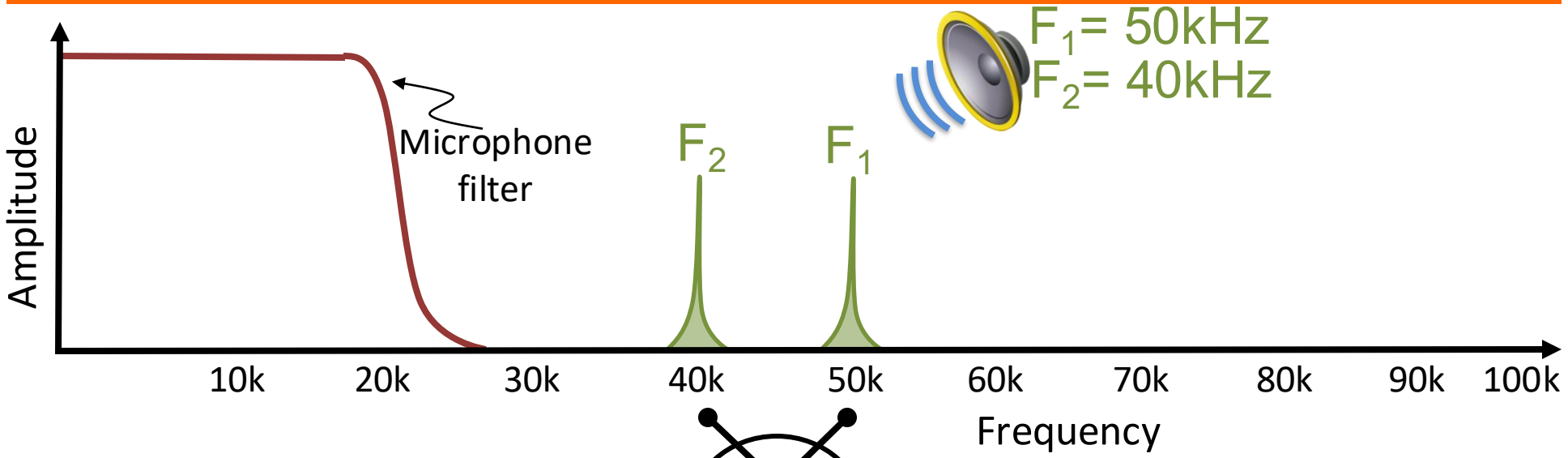
③ Challenges

④ Evaluation

Exploiting amplifier non-linearity



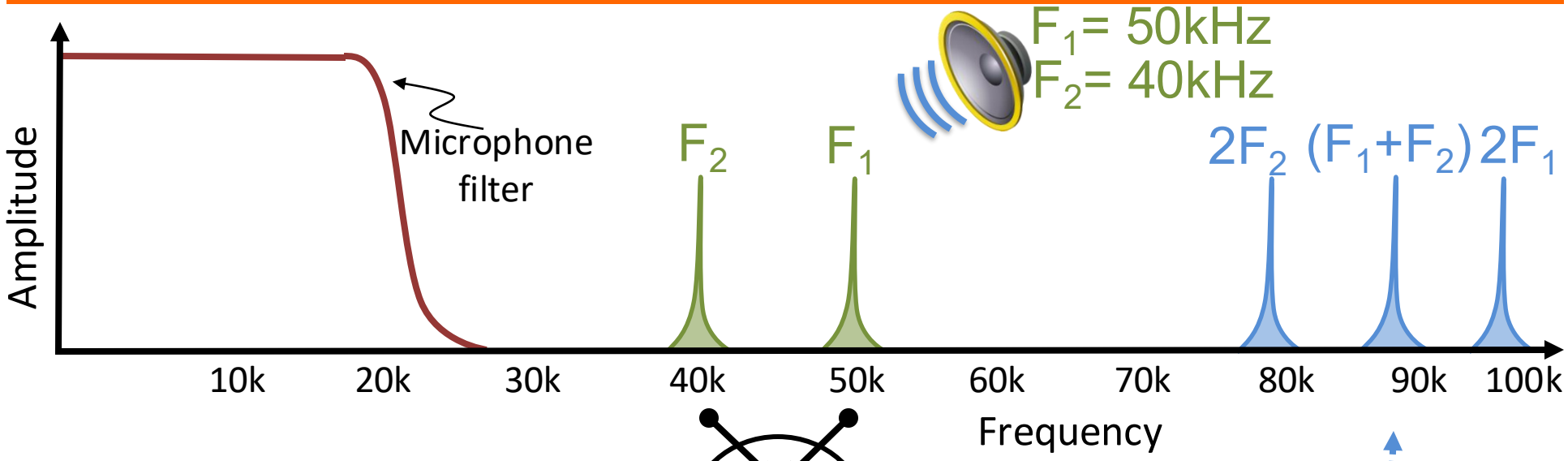
Exploiting amplifier non-linearity



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

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

Exploiting amplifier non-linearity

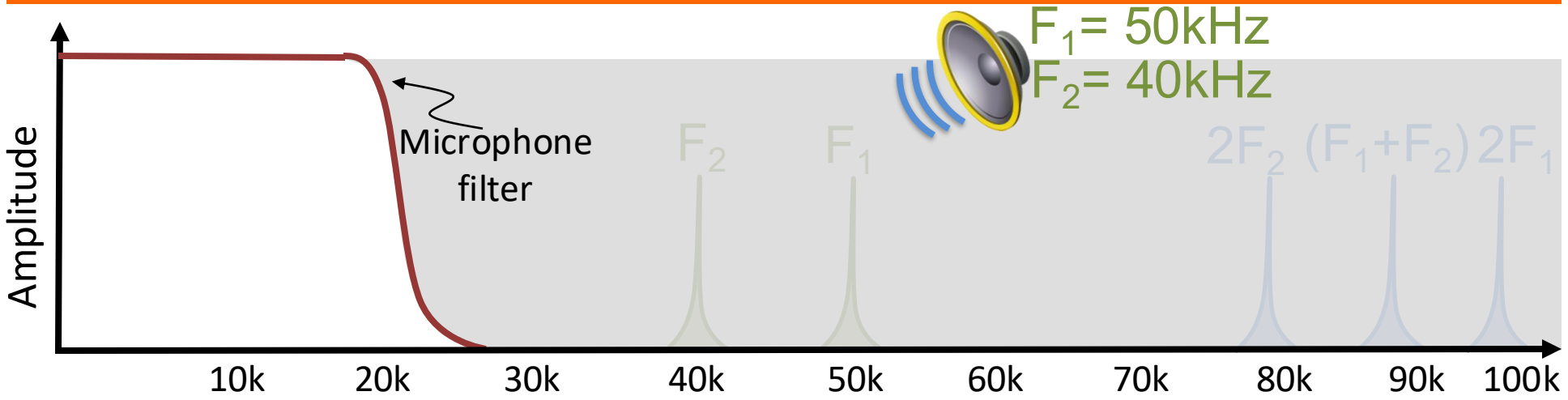


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

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

Exploiting amplifier non-linearity

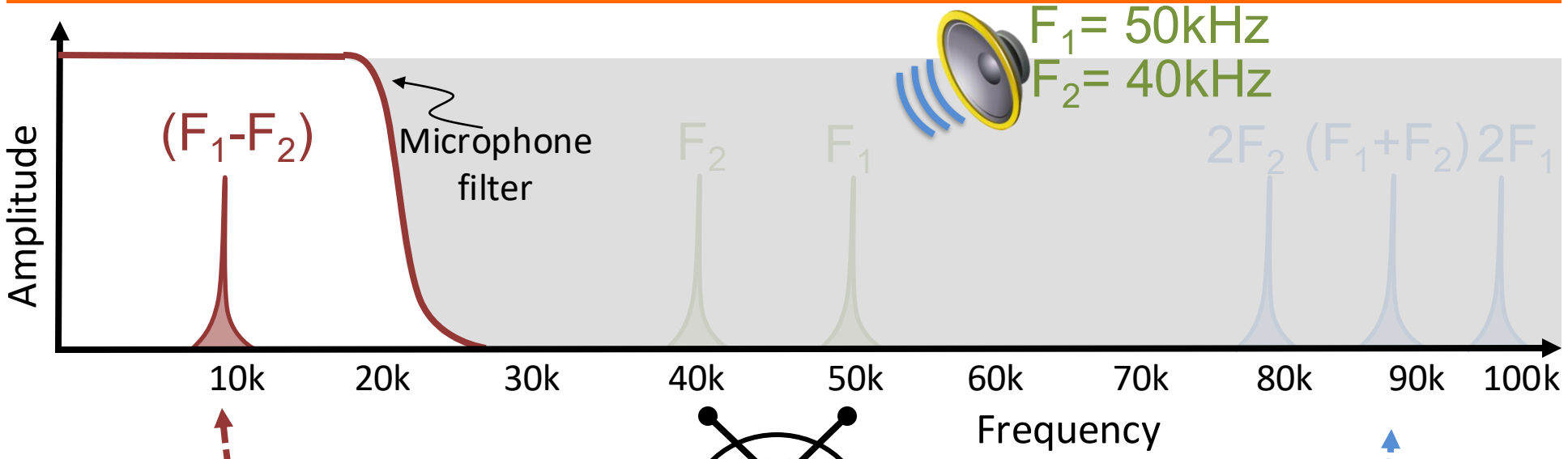


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

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

Exploiting amplifier non-linearity

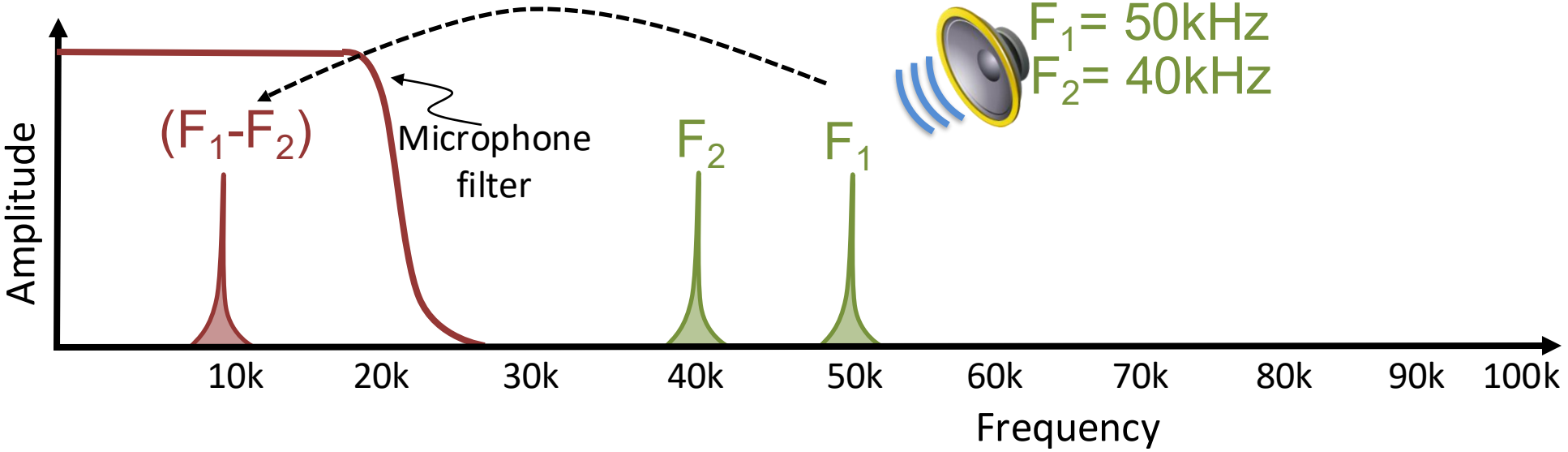


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

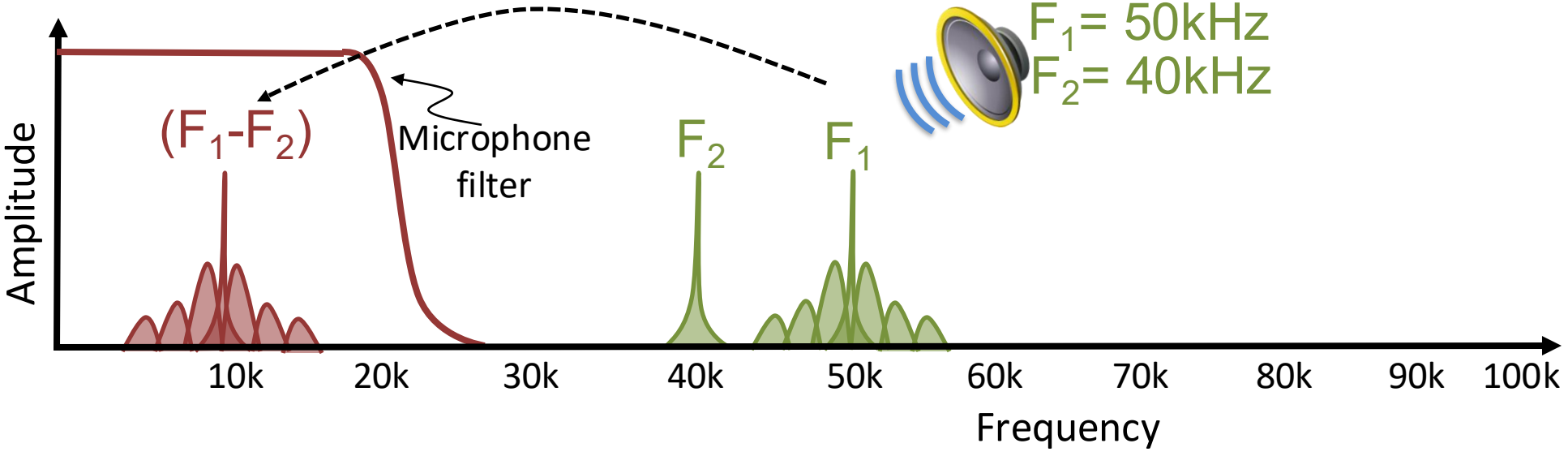
$$(\sin F_1 + \sin F_2)^2 =$$

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

Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Talk outline

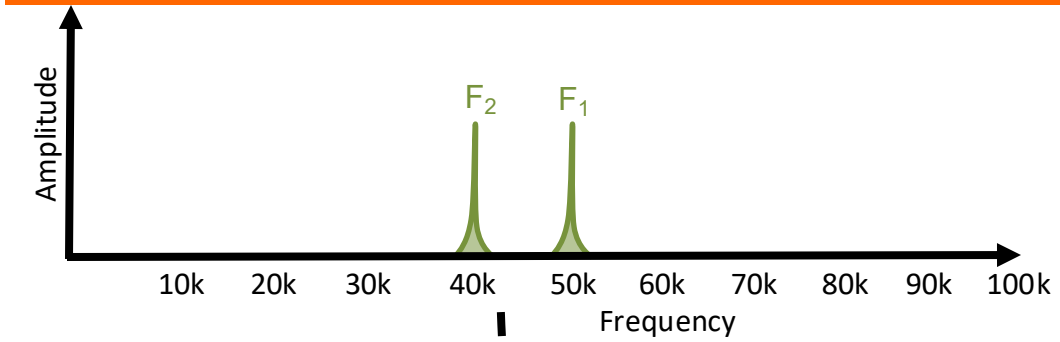
① Microphone Overview

② System Design

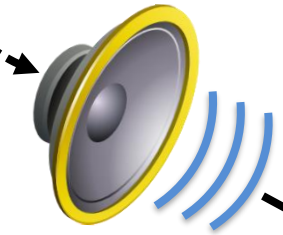
③ Challenges

④ Evaluation

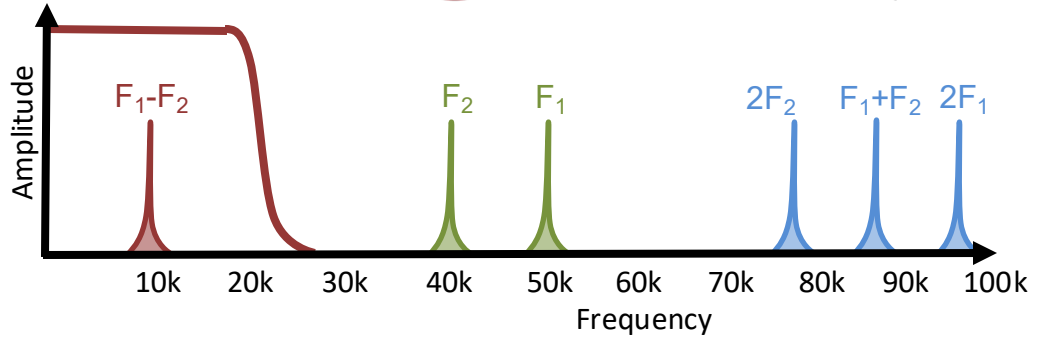
Challenges



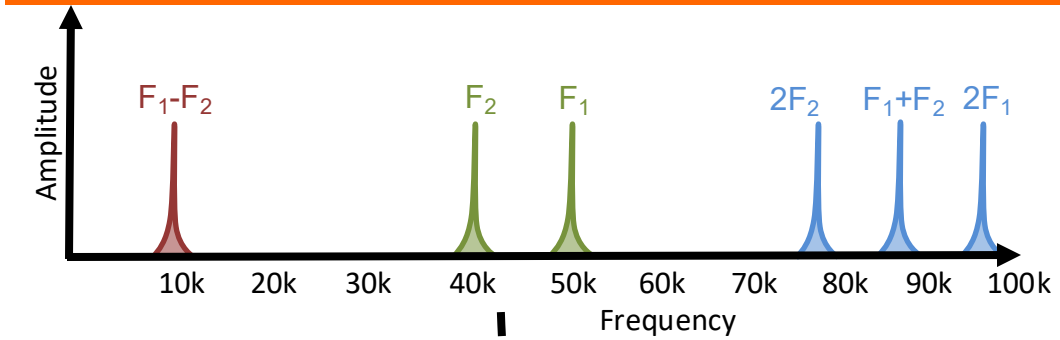
Speaker's nonlinearity



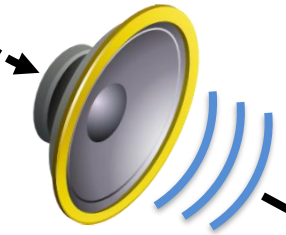
Microphone's nonlinearity



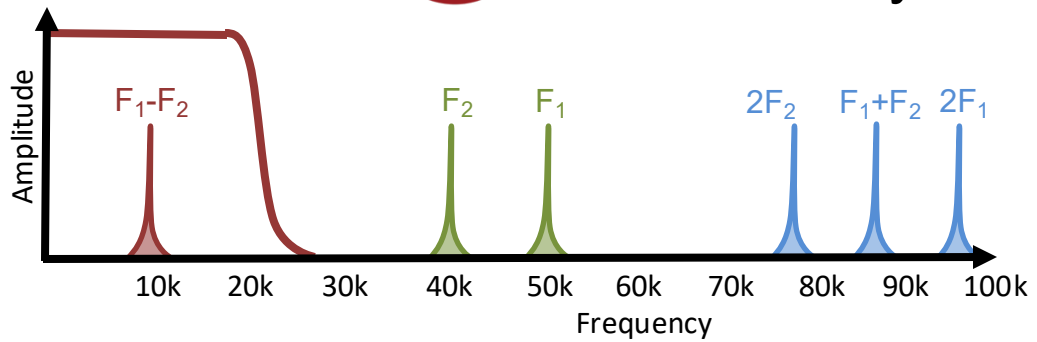
Challenges



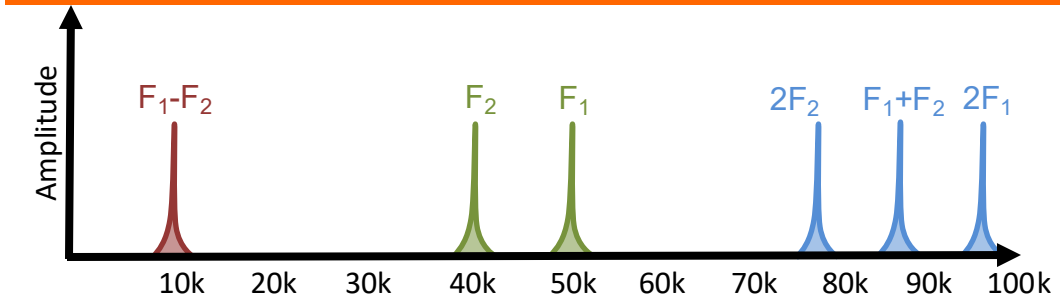
Speaker's nonlinearity



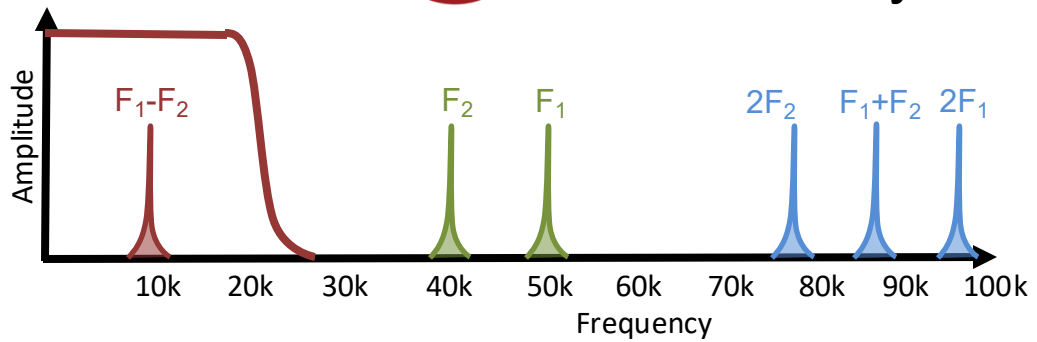
Microphone's nonlinearity



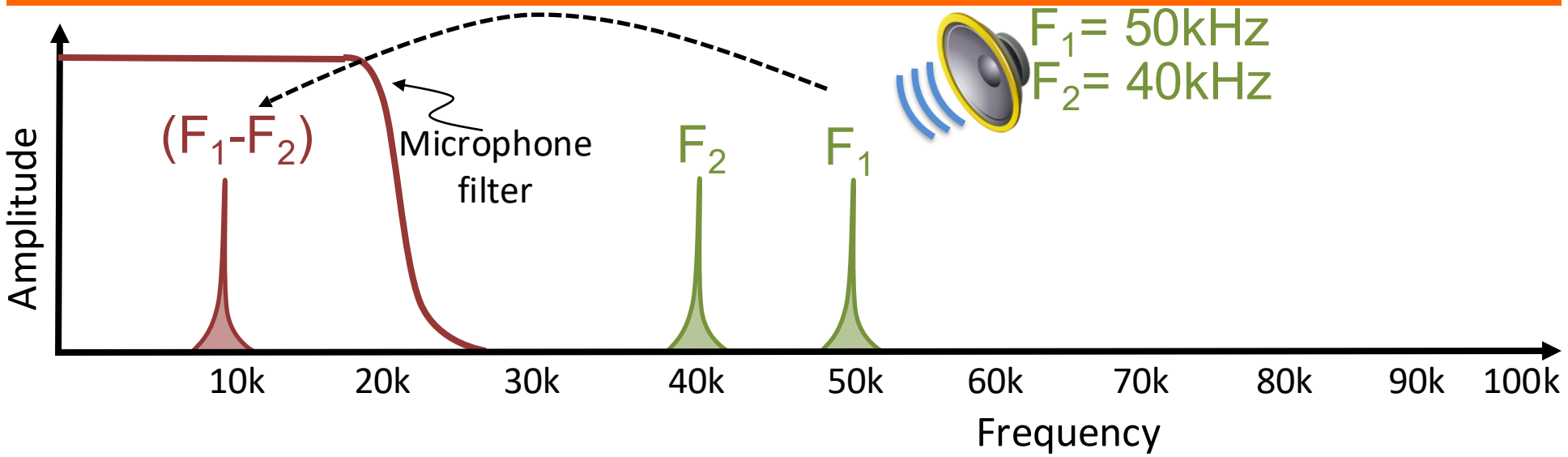
Challenges



Microphone's nonlinearity



Exploiting amplifier non-linearity



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

How can we send this command?

Talk outline

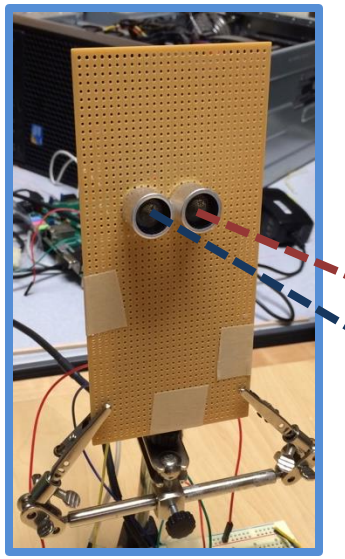
① Microphone Overview

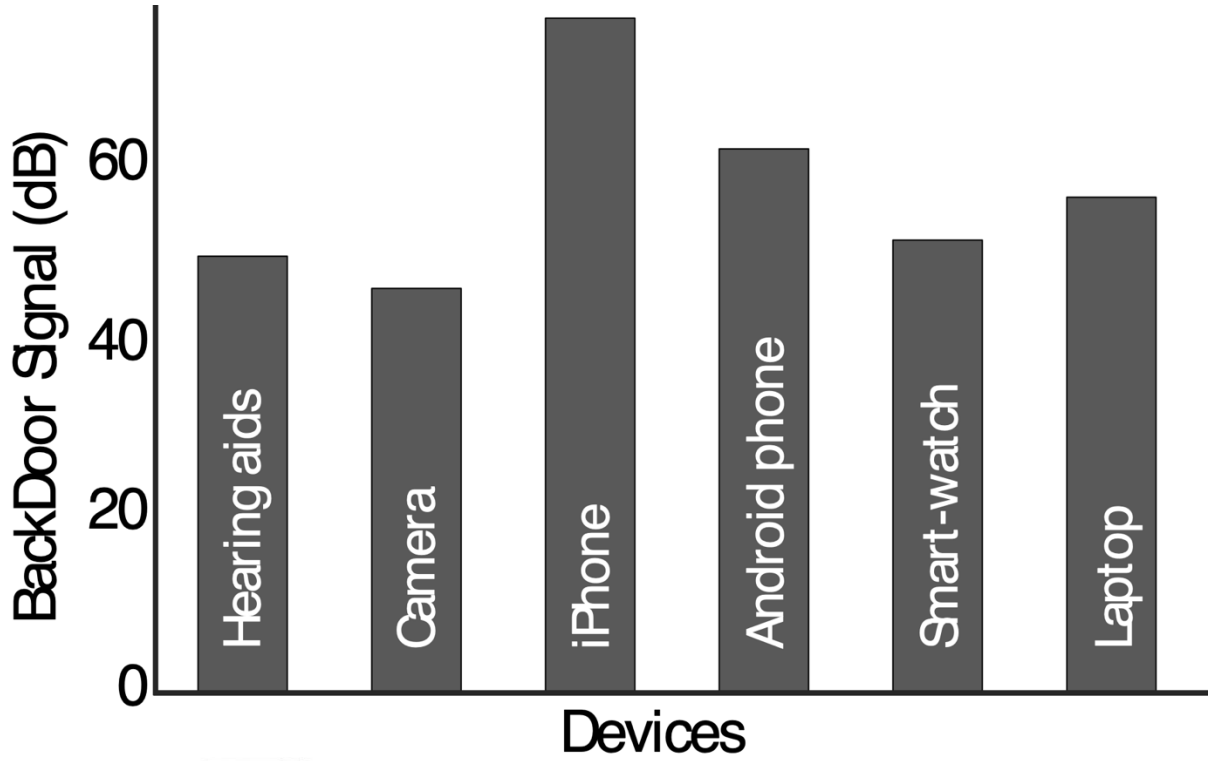
② System Design

③ Challenges

④ Evaluation

Hardware generalizability






Hearing Aid

Camera

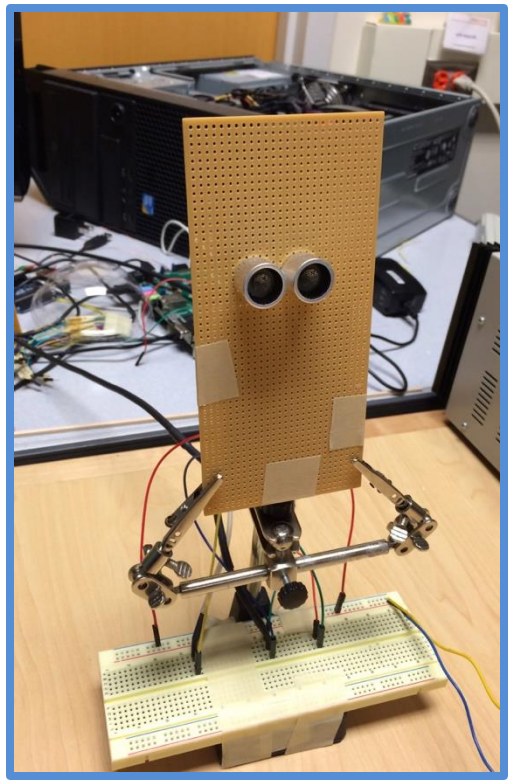

iPhone

Android phone

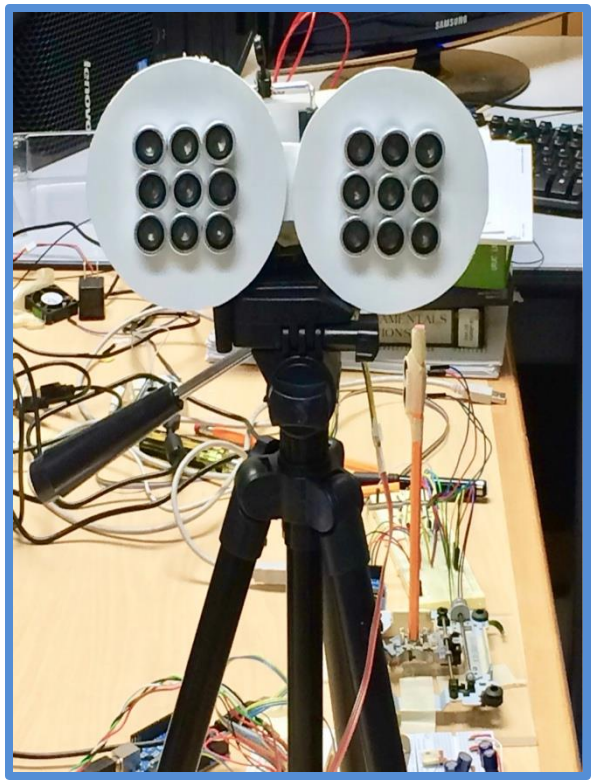
Smartwatch


Laptop

Implementation

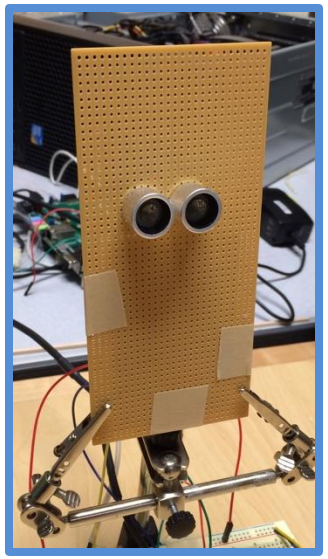


Communication prototype



Jammer prototype

Communication performance

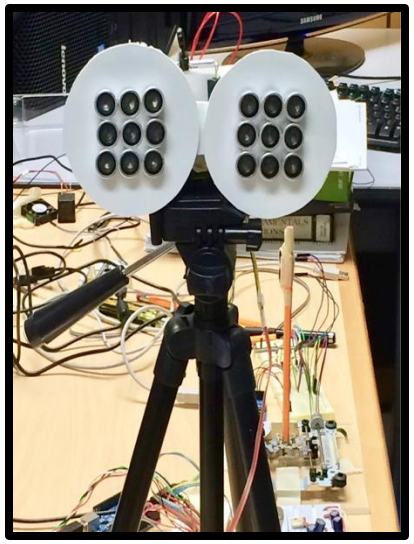


FM data packets

4kbps
up to 1 meter

More power can increase the distance

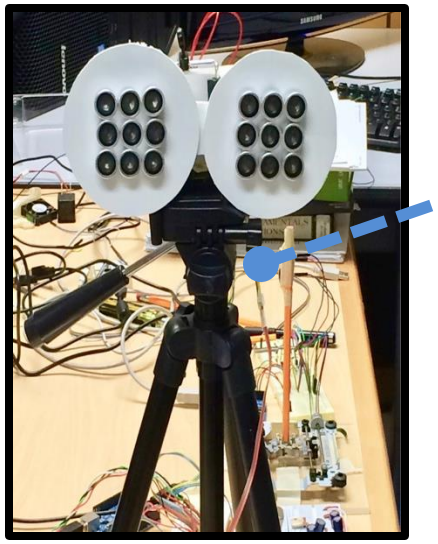
Jamming performance



BackDoor jammer

Spy microphone

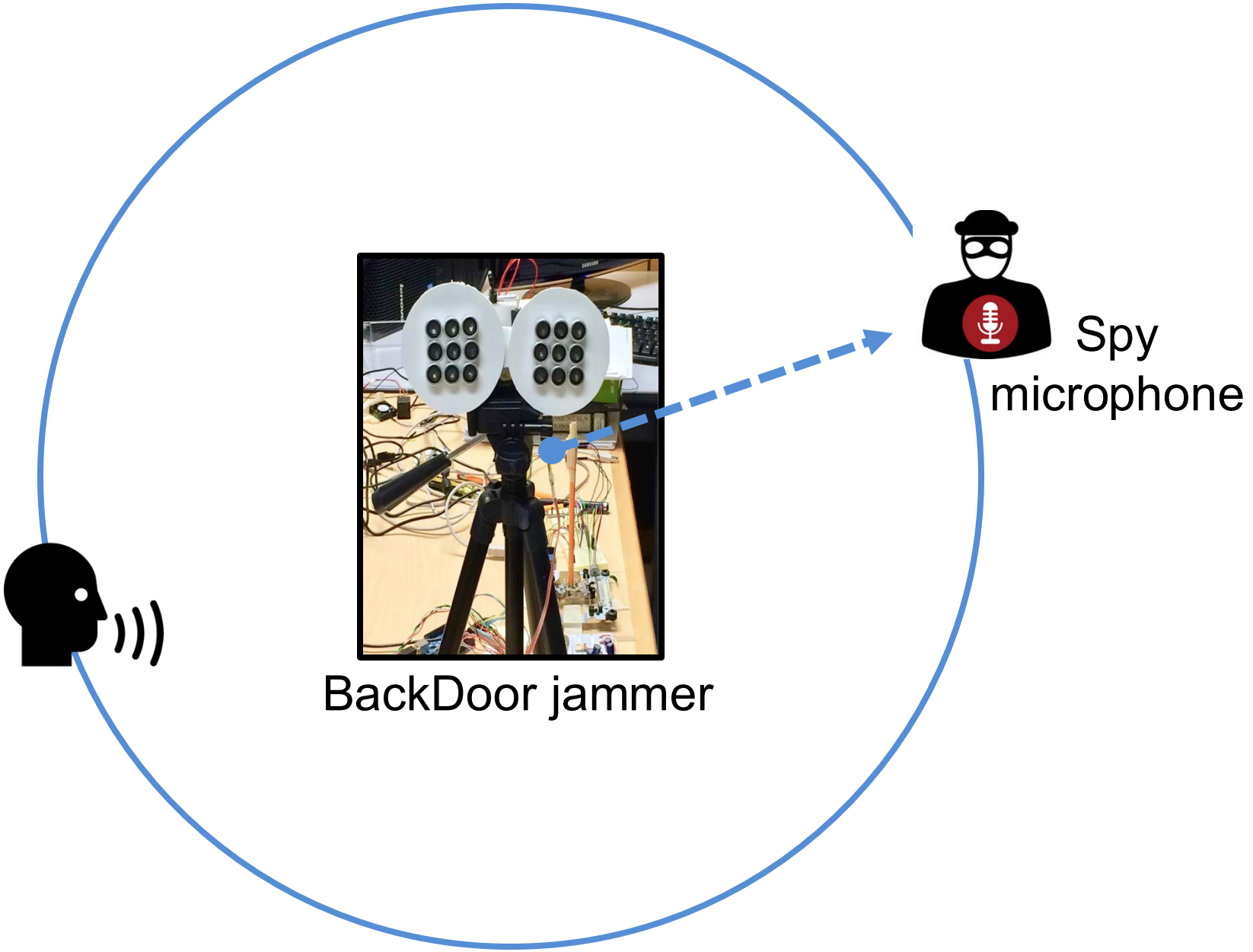
Jamming performance



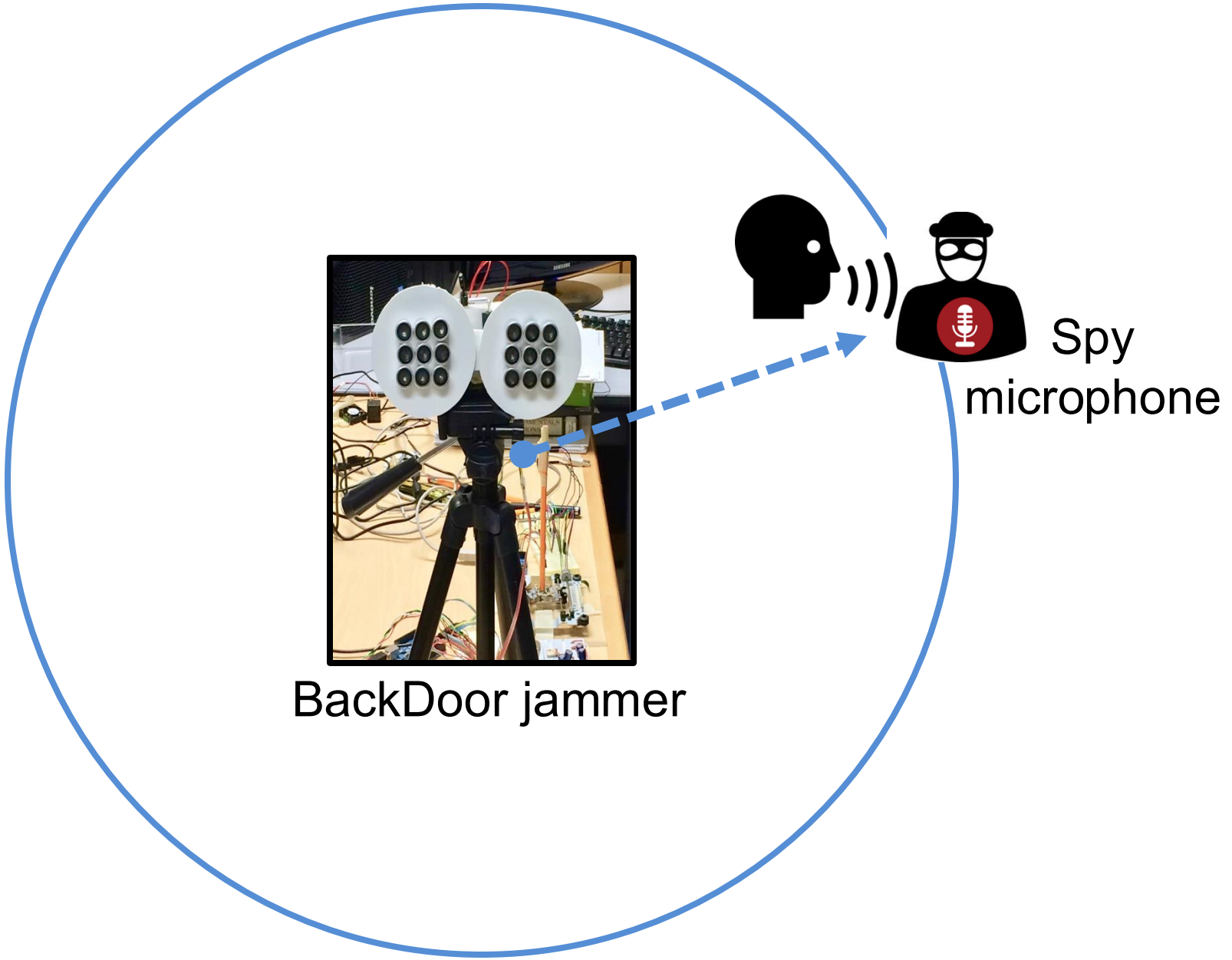
BackDoor jammer

Spy microphone

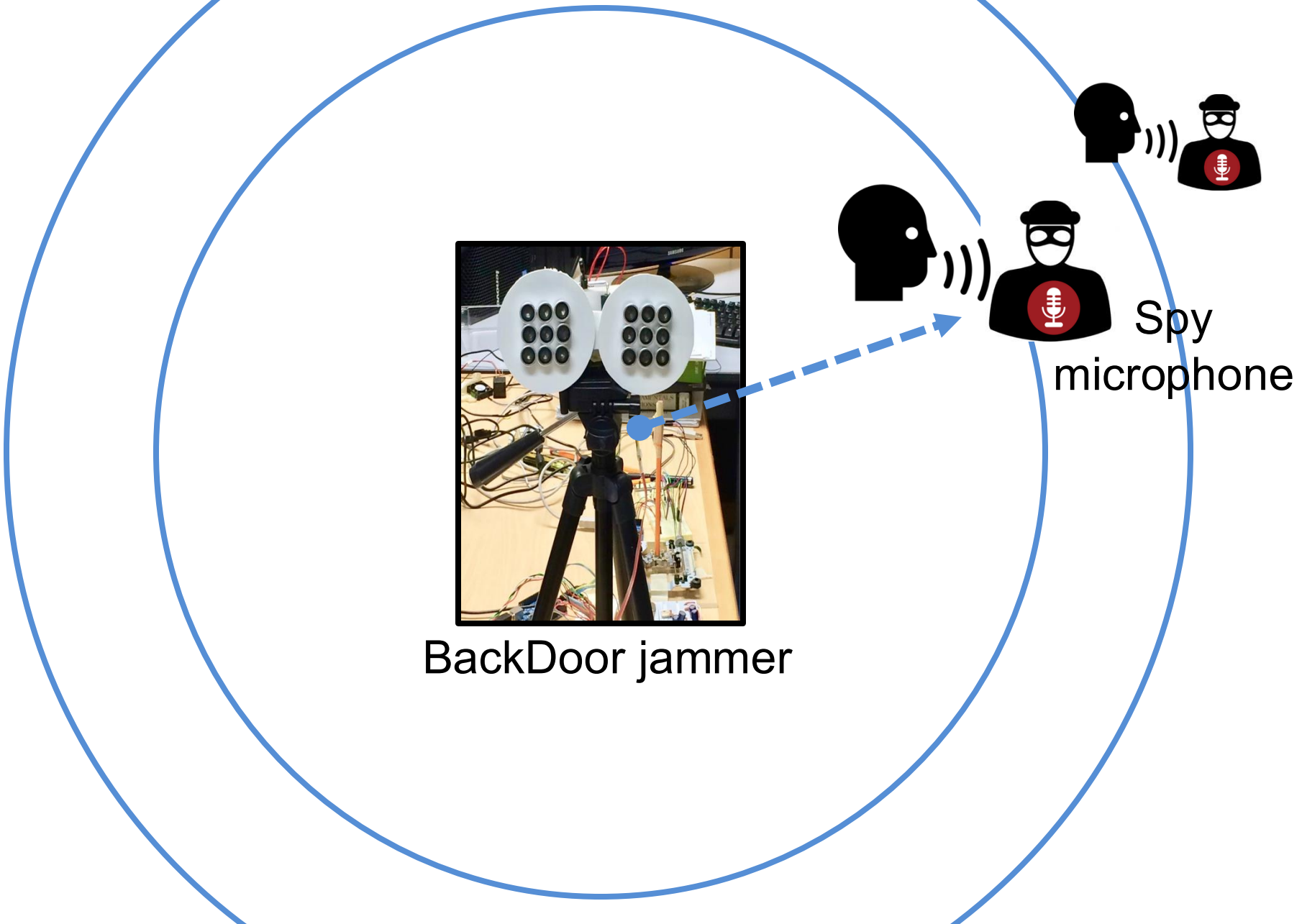
Jamming performance



Jamming performance

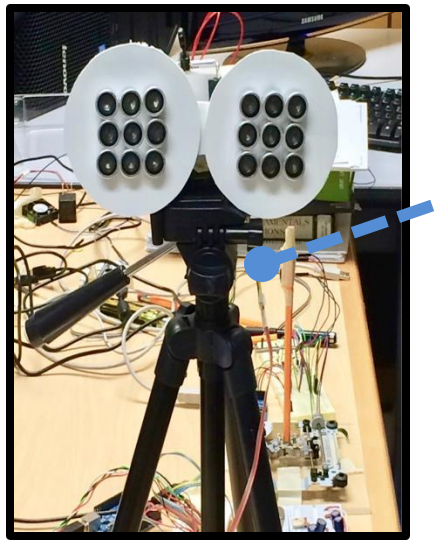


Jamming performance

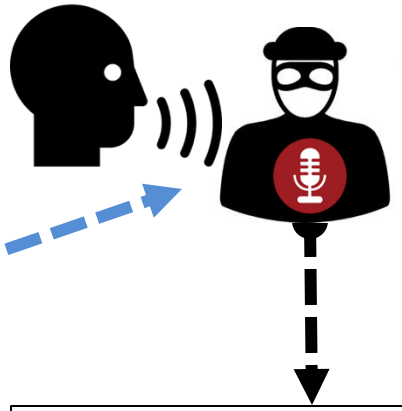


Jamming performance

2000 spoken words

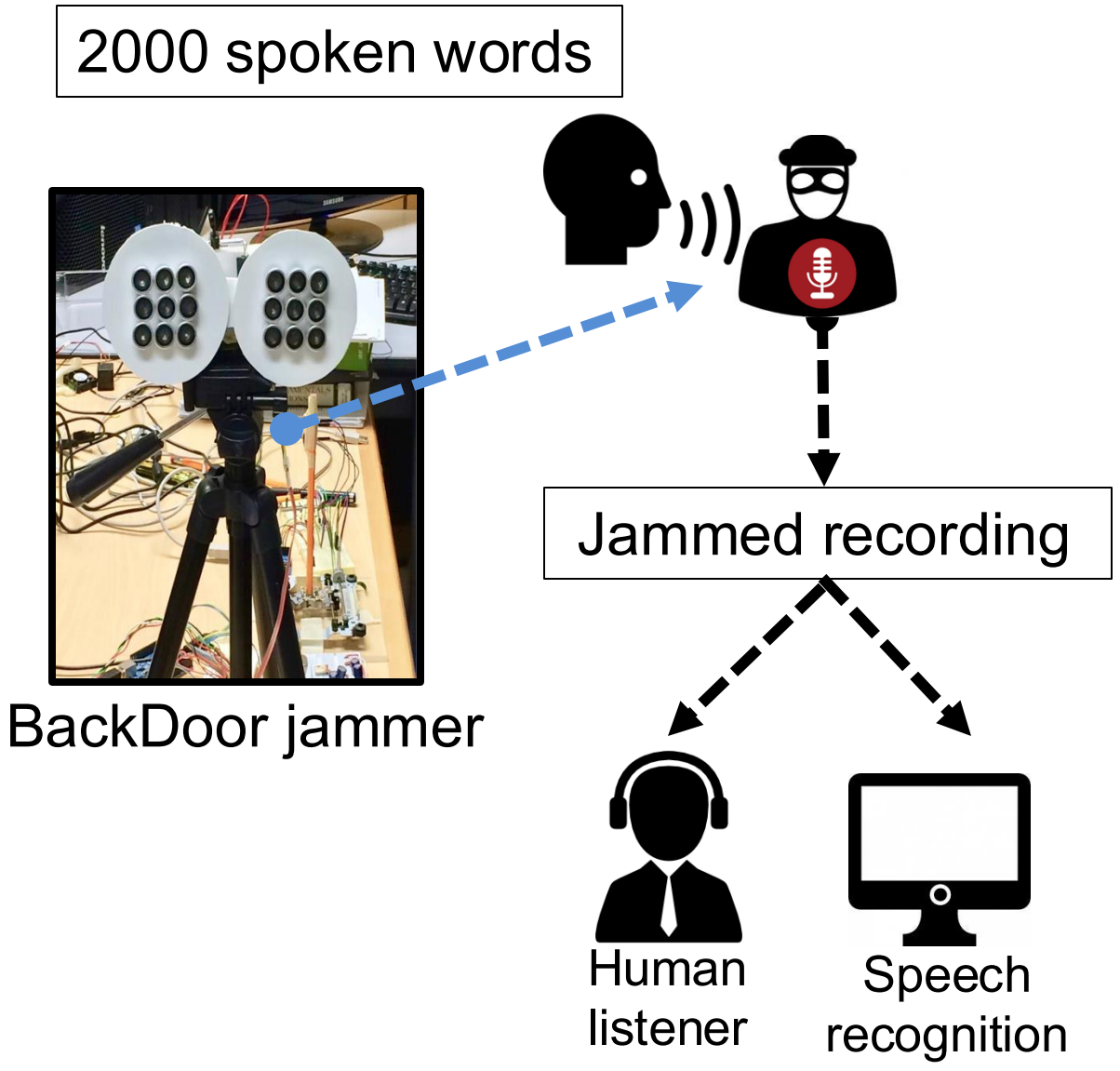


BackDoor jammer



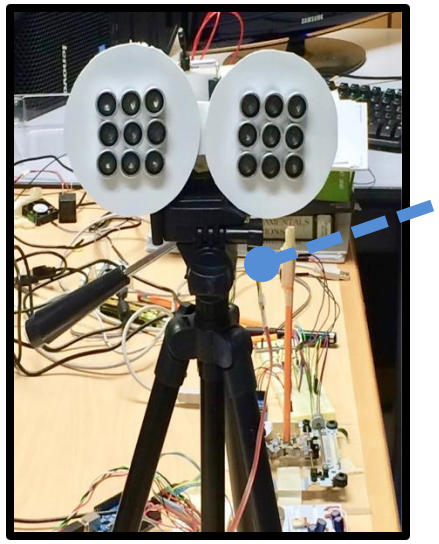
Jammed recording

Jamming performance



Jamming performance

2000 spoken words



BackDoor jammer

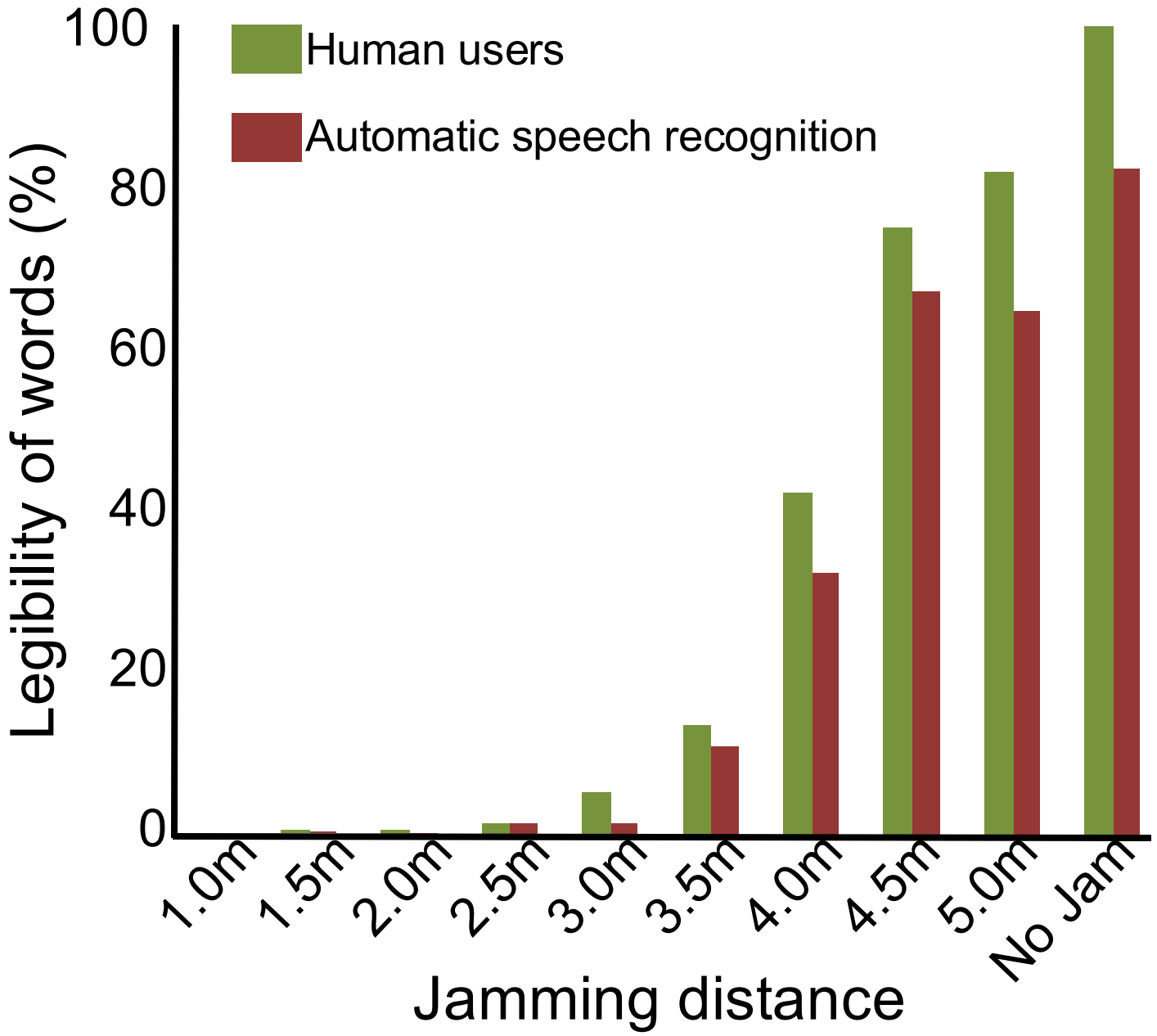
Jammed recording

% of legible words

Human listener

Speech recognition

Jamming performance

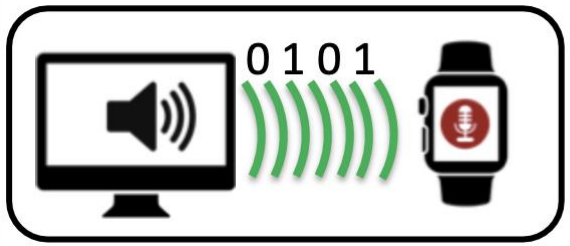


Takeaways

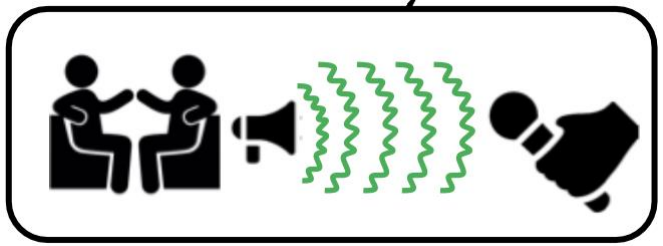
1. Specially designed inaudible sound can be recorded with unmodified microphone
2. It can make acoustic jammer possible and also can be a communication channel
3. It also uncovers threats like acoustic Denial-of-Service attacks

To summarize…

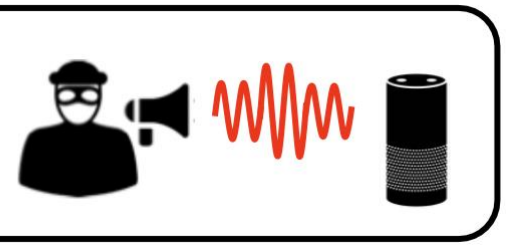
Communication

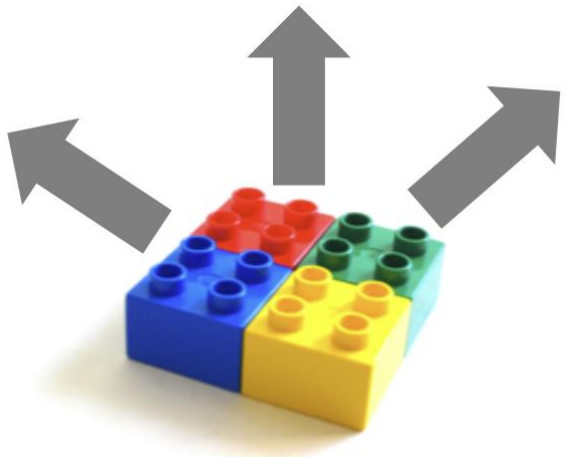


Privacy



Attack





Inaudible Acoustics is a new primitive …

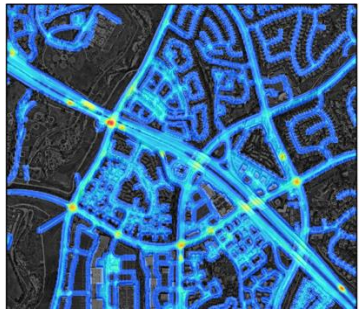
that makes **inaudible** ultrasound **audible** to microphones

Underpinning a wide range of IoAT applications …

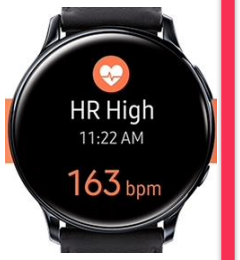
Remainder of the Class

Emerging Application Domains & Cross-Cutting Topics

1. Transportation

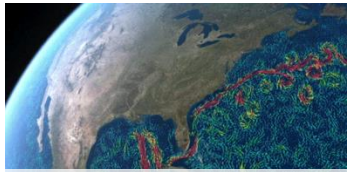


2. Health



3. Agriculture

4. Oceans/Climate



Upcoming lectures

5. Security/Privacy