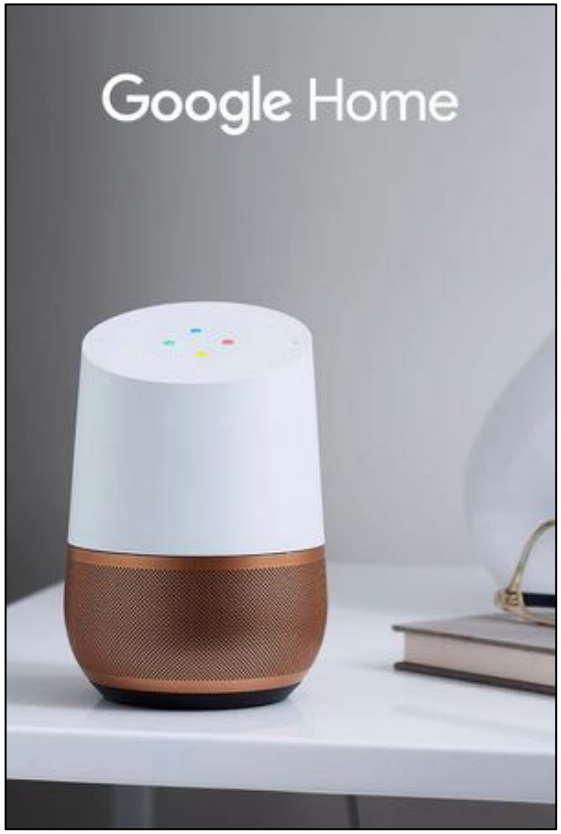
BackDoor: Sensing Out-of-band Sounds through Channel Nonlinearity

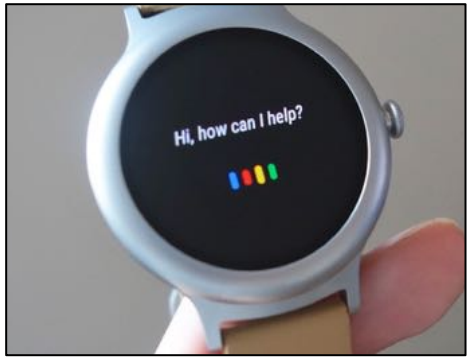
Nirupam Roy

ECE-420 Guest Lecture - 30th October 2017

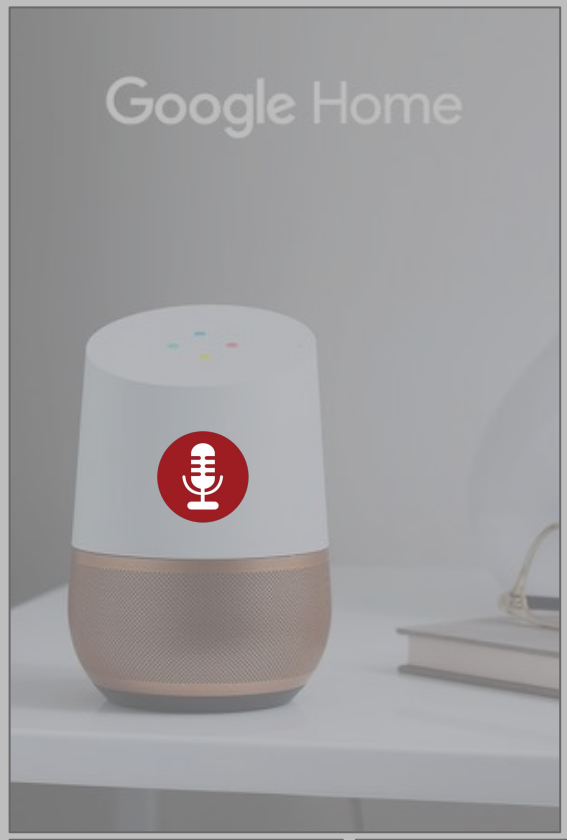
University of Illinois at Urbana-Champaign

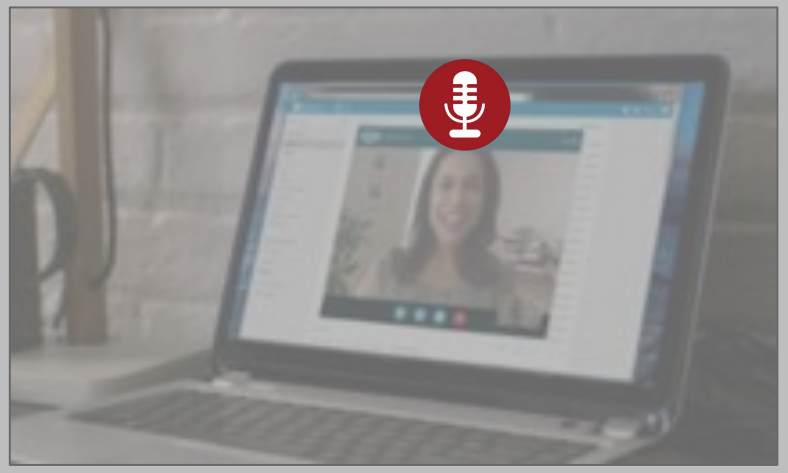
Microphones are everywhere

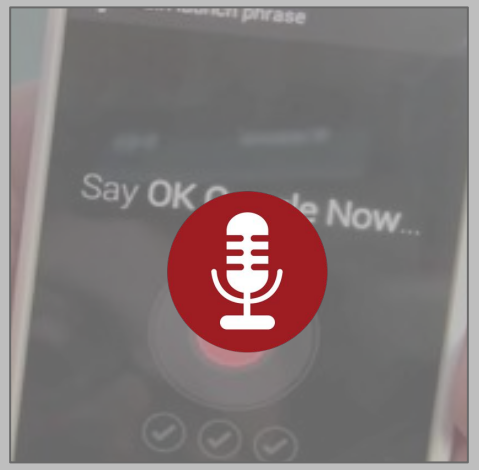


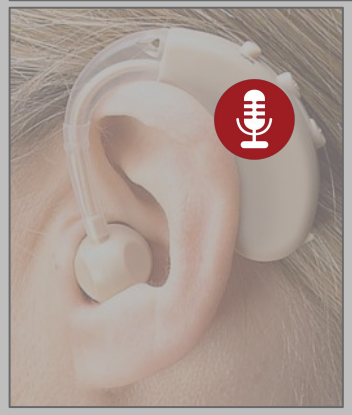


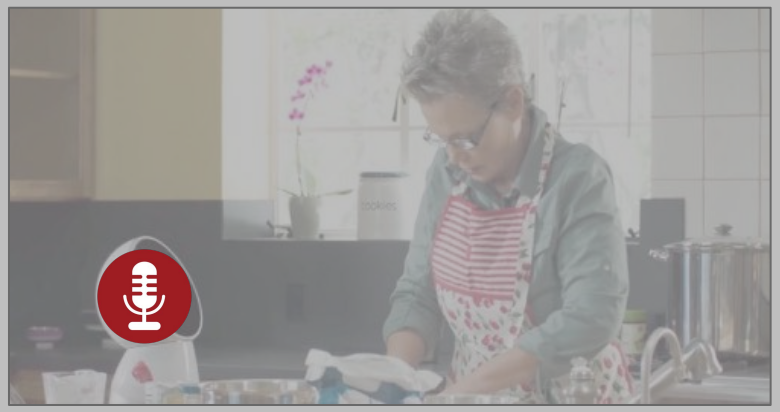
Microphones are everywhere



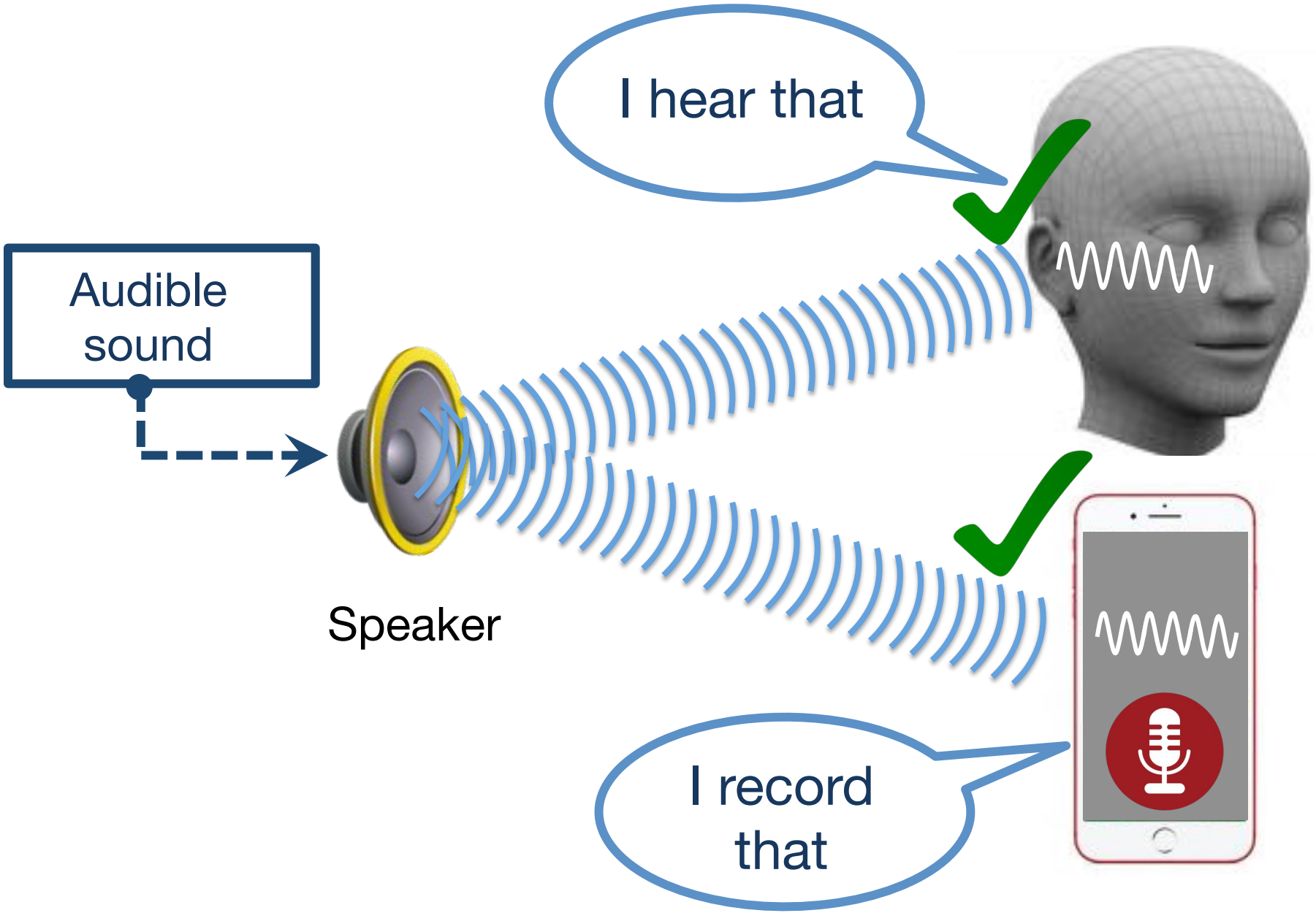




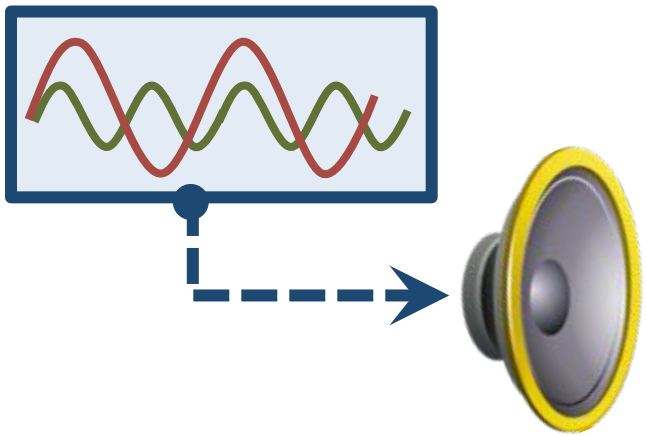




Microphones record audible sounds

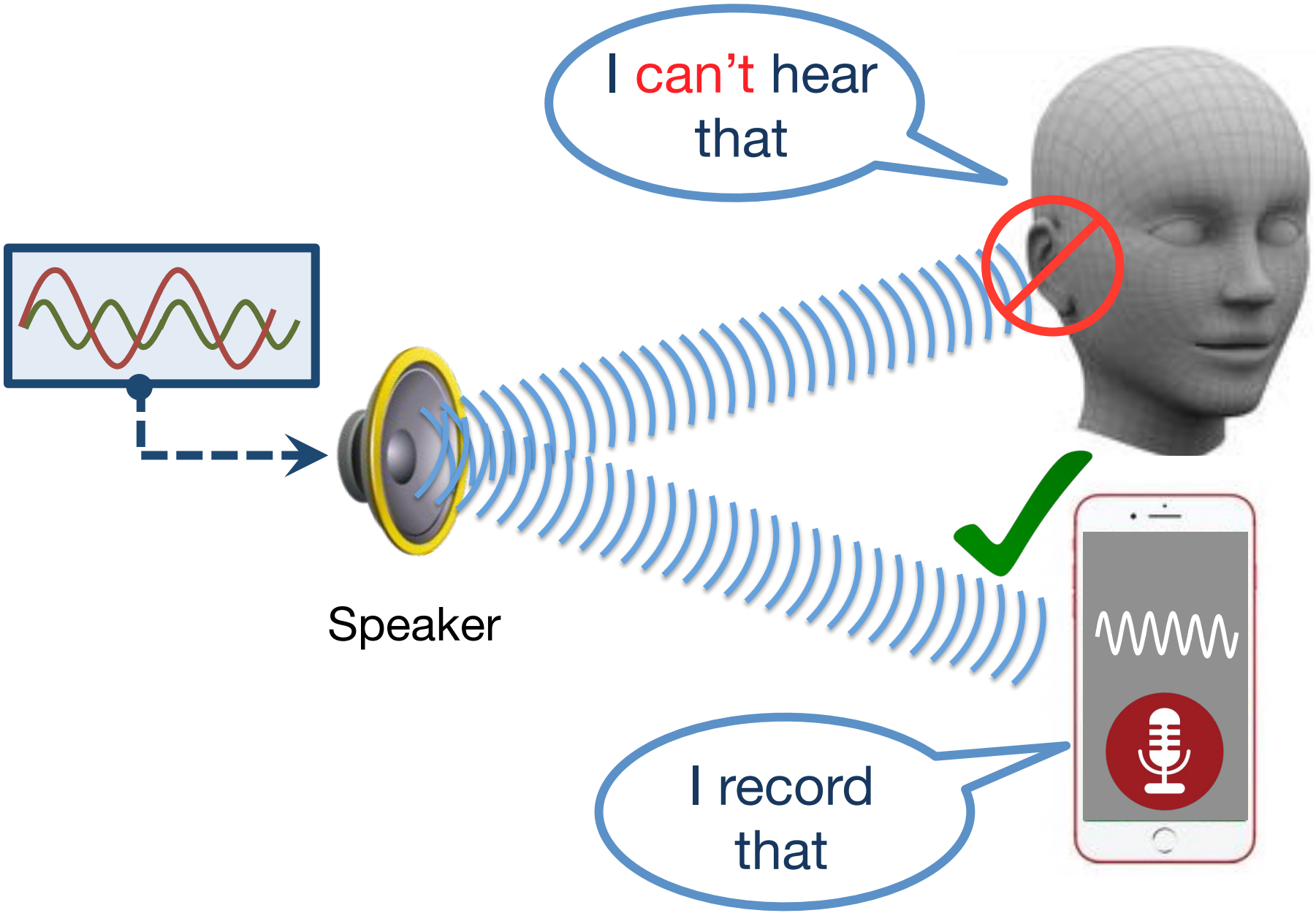


Inaudible, but recordable !

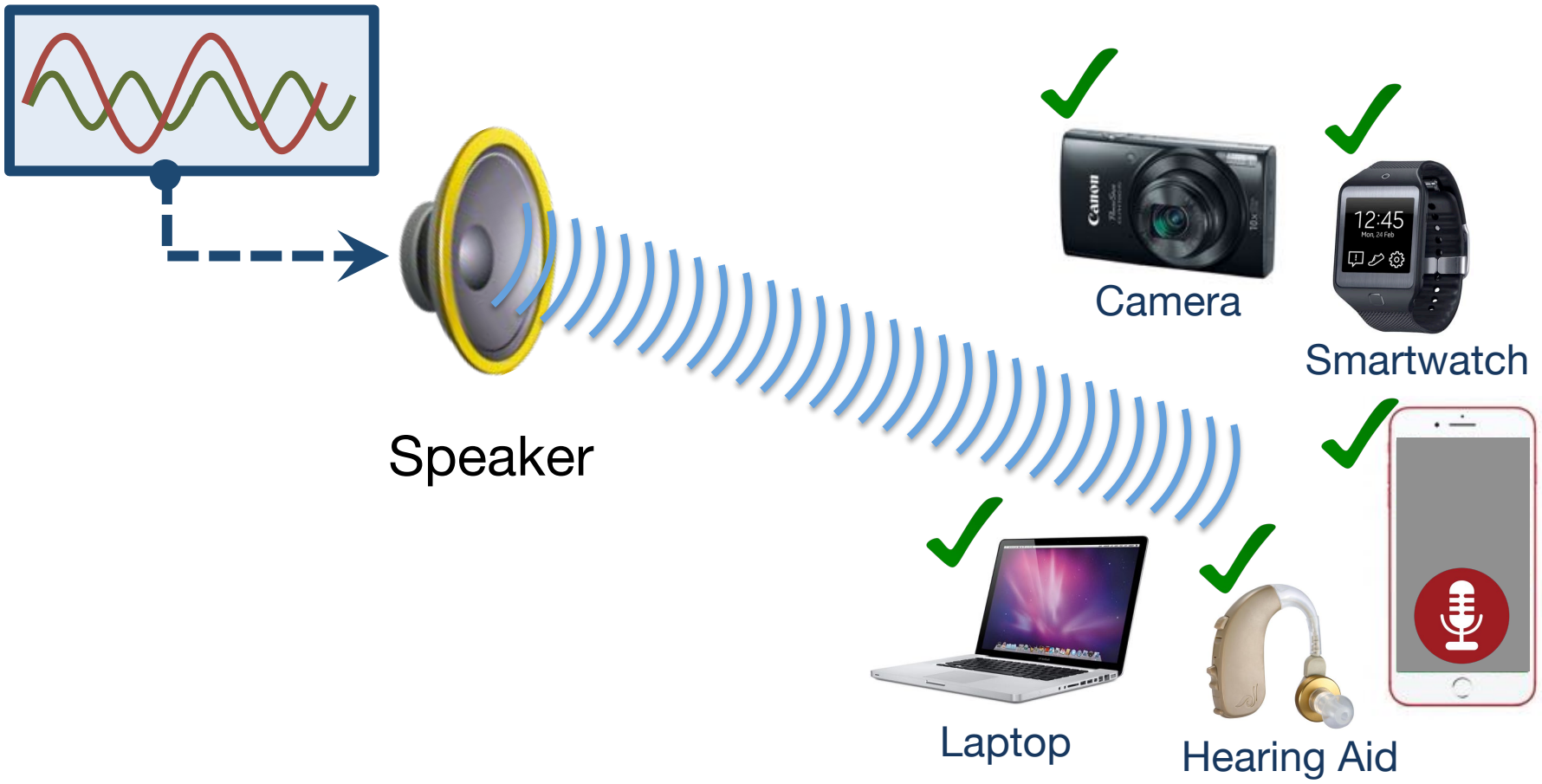


Speaker

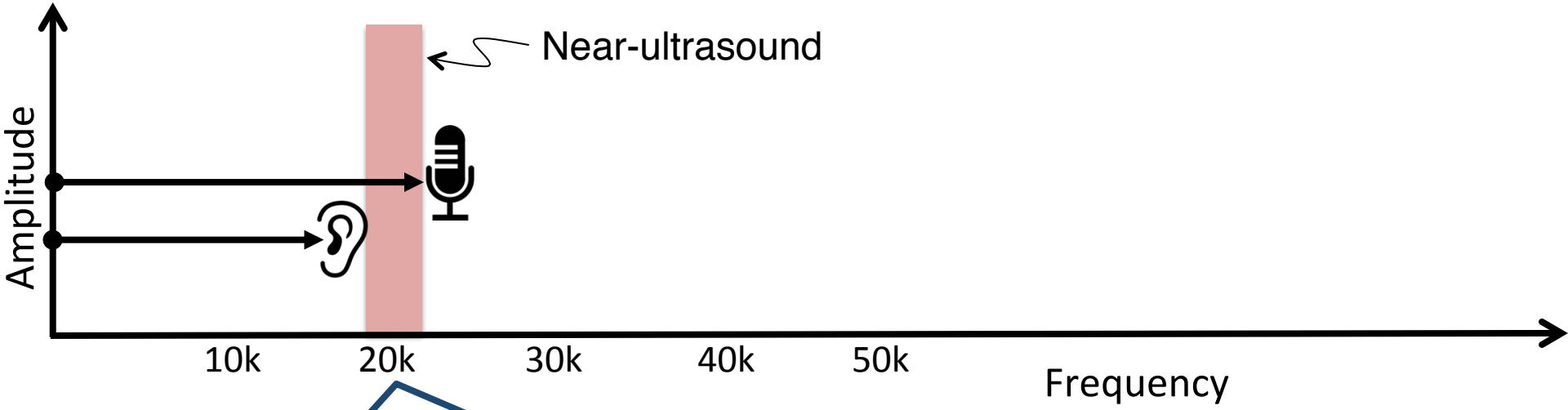
Inaudible, but recordable !



Works with unmodified devices



It's not "near-ultrasound"



chirp.io

Pseudo-ranging
SenSys'12

ApneaApp
MobiSys'15

DopLink
UbiComp'13

SoundWave
CHI'12

lisnr.com

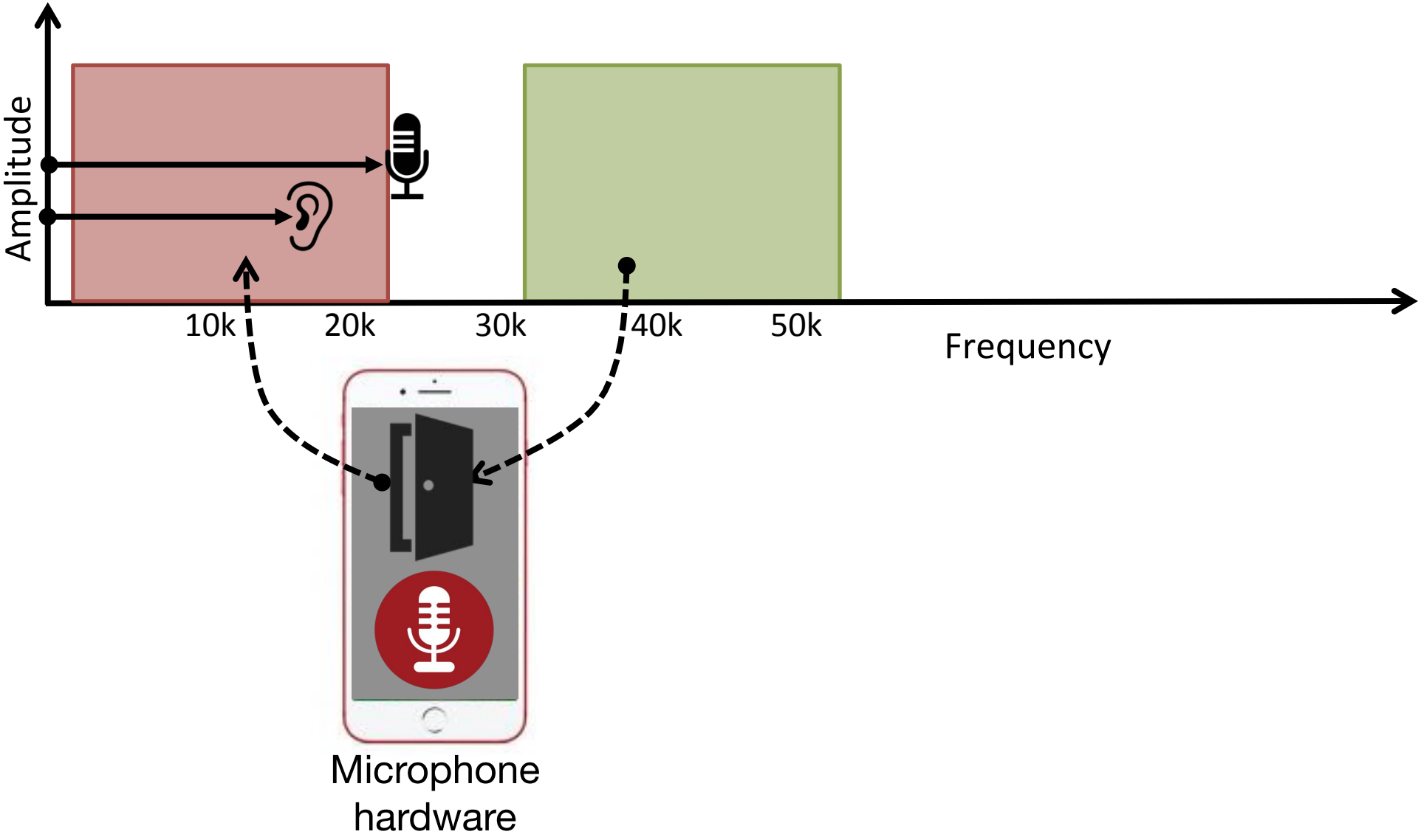
AAMouse
MobiSys'15

AirLink
UbiComp'14

Spartacus
MobiSys'13

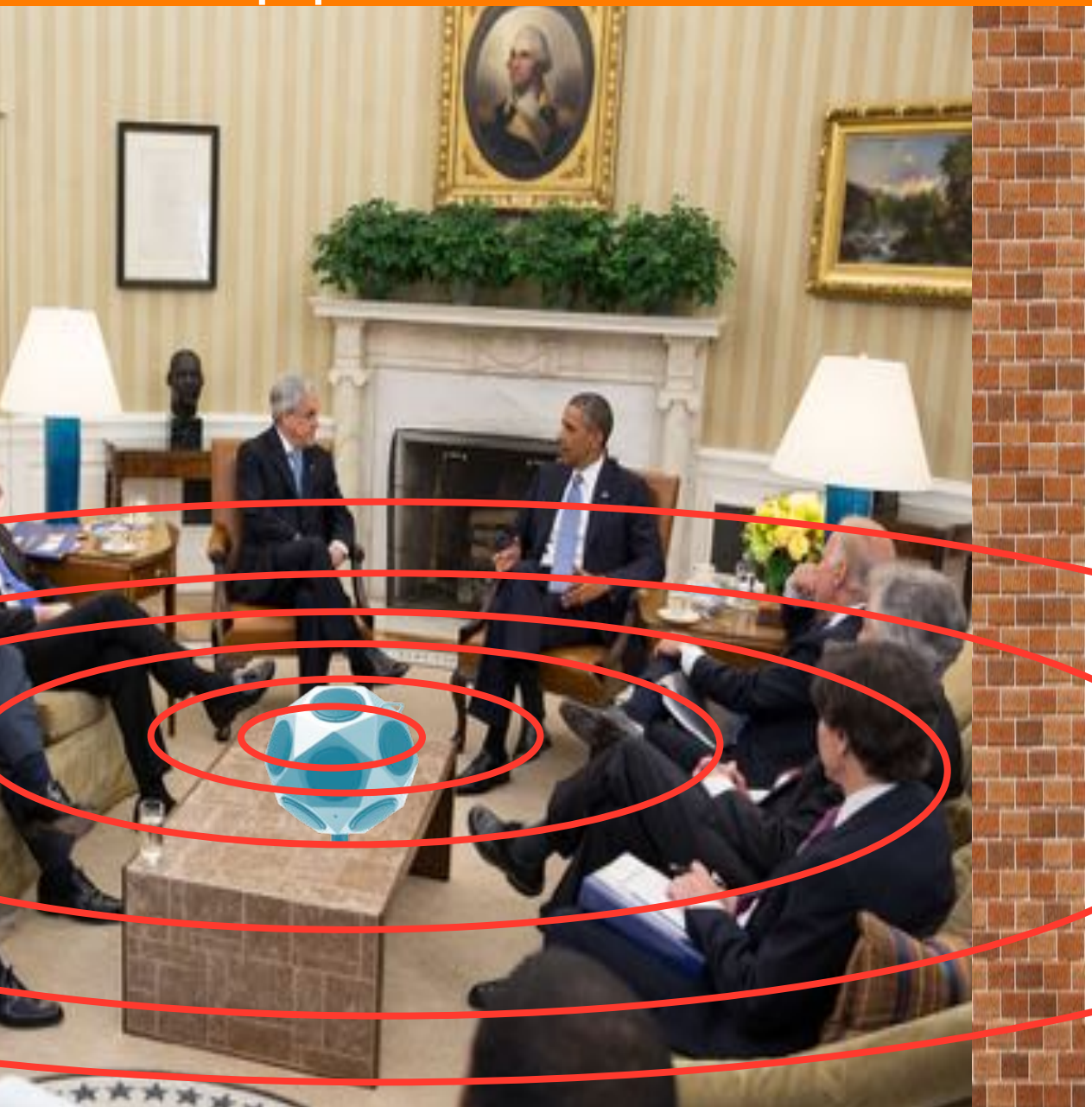
Crowd-counting
SenSys'12

Exploiting fundamental nonlinearity

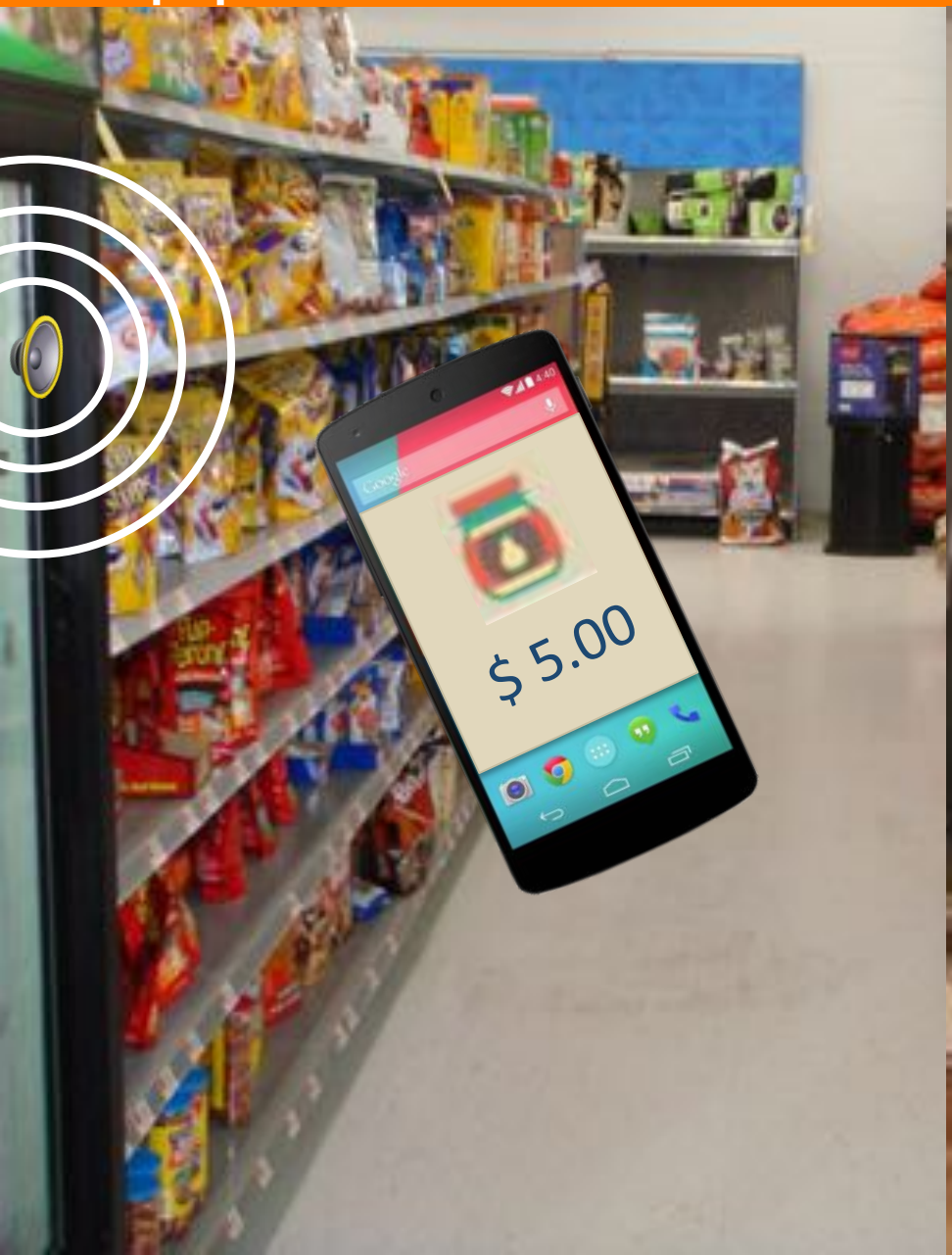


What can we do with it?

Opportunities: Acoustic jammer



Application: Acoustic communication



Threat: Acoustic DOS attack

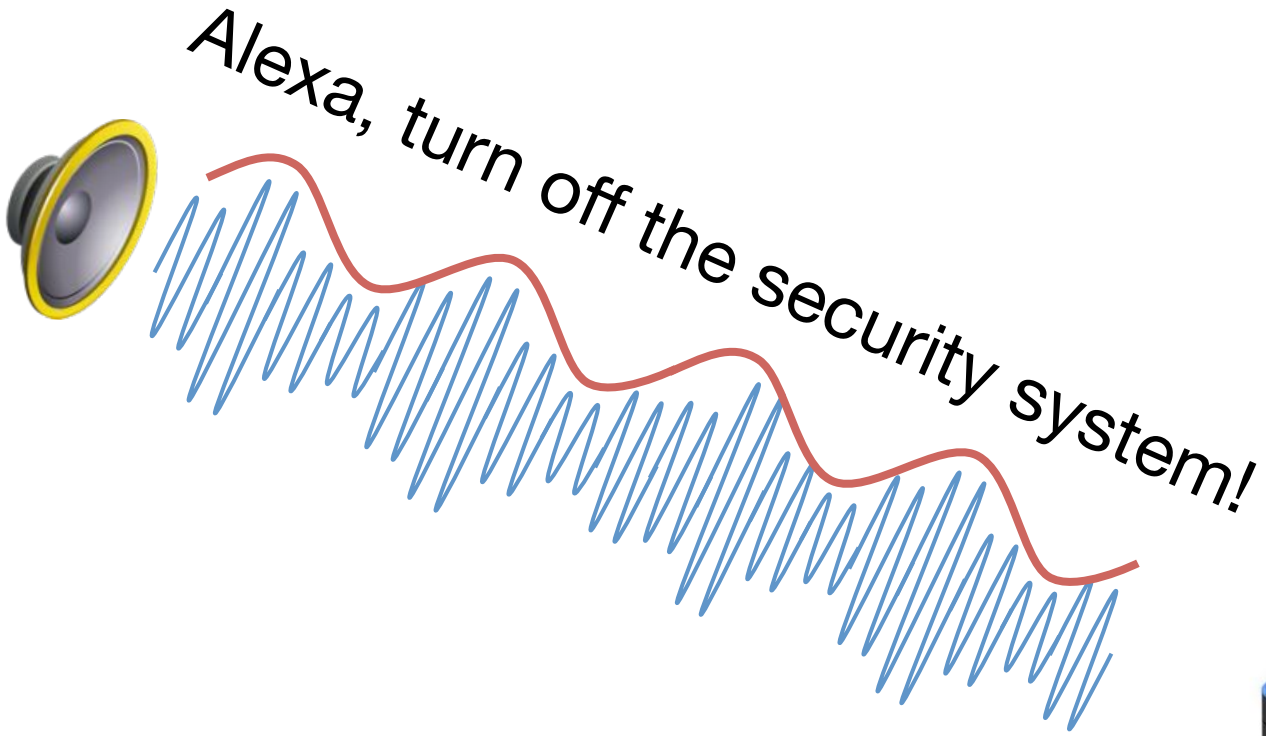
Jamming
hearing aids

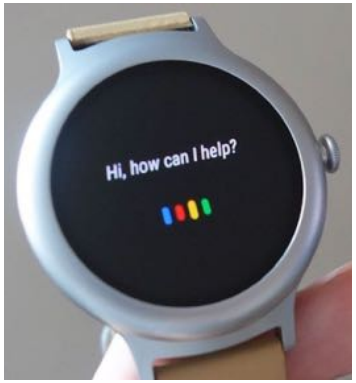
Threat: Acoustic DOS attack

Jamming
hearing aids

Blocking
911 calls

Threats: Inaudible voice attack





Talk outline

① Microphone Overview

② System Design

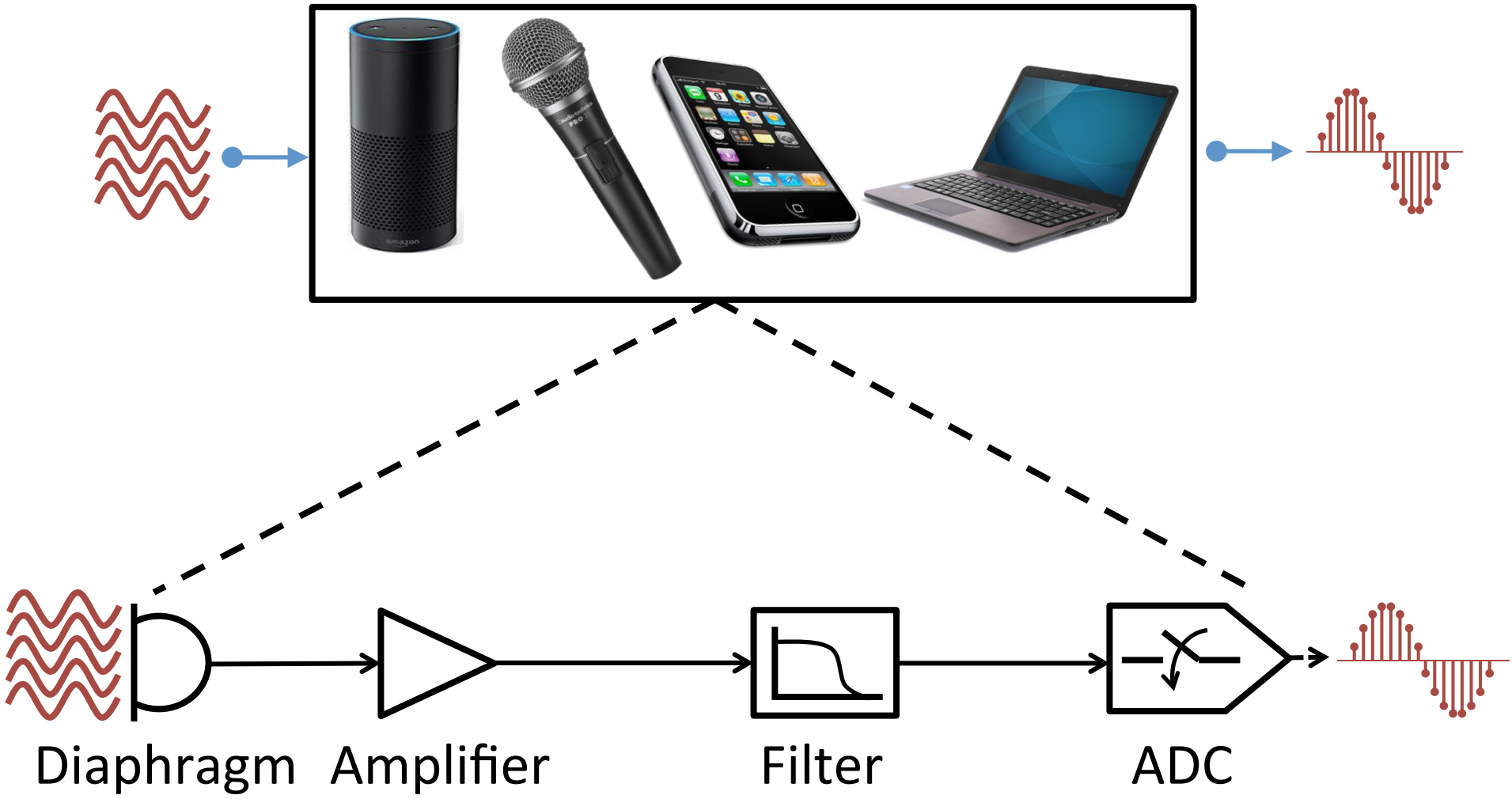
③ Challenges

④ Evaluation

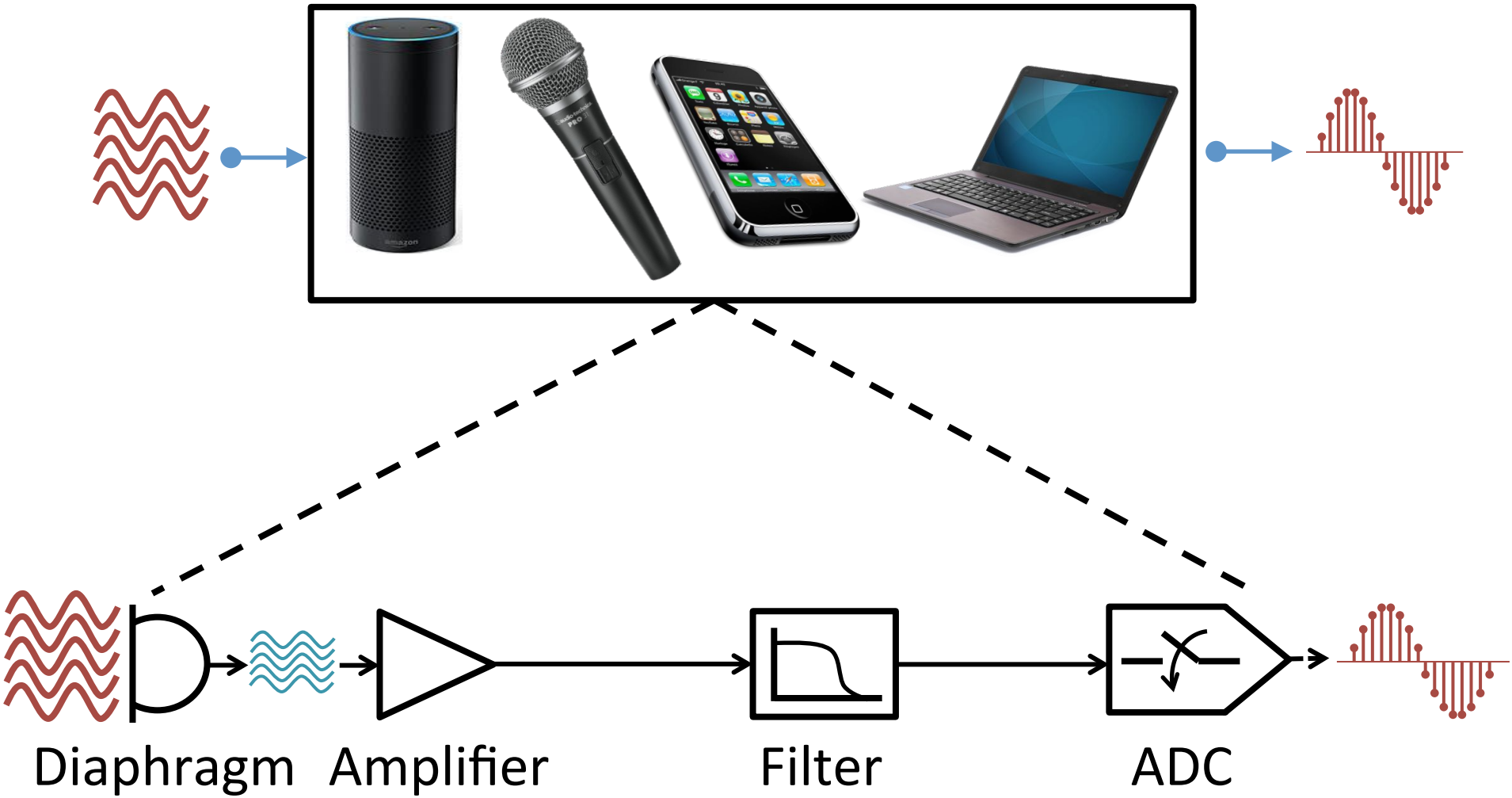
Talk outline

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

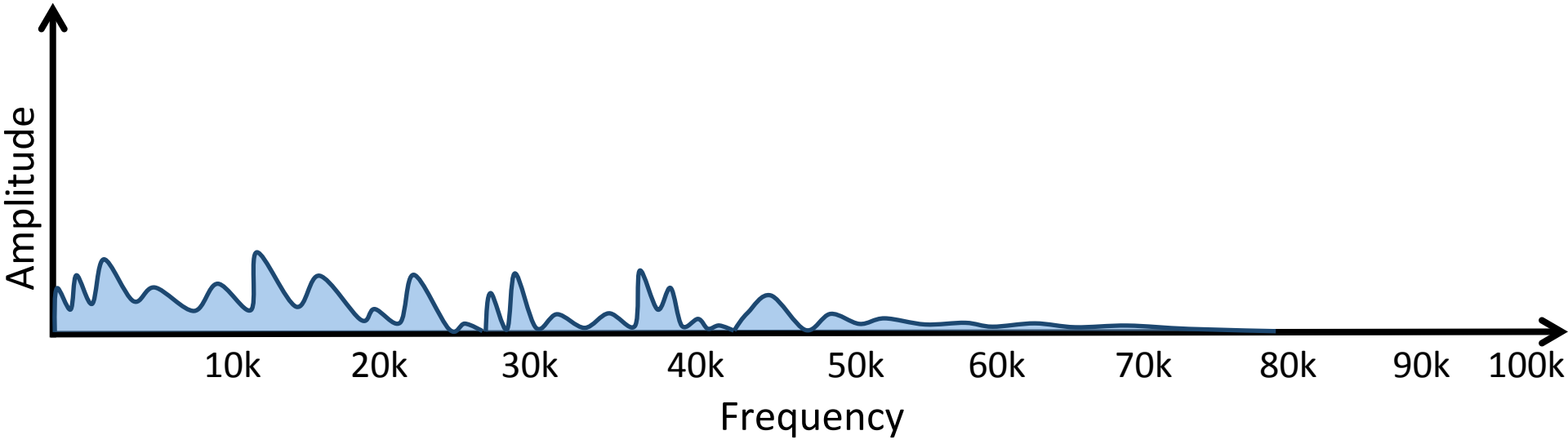
Microphone working principle

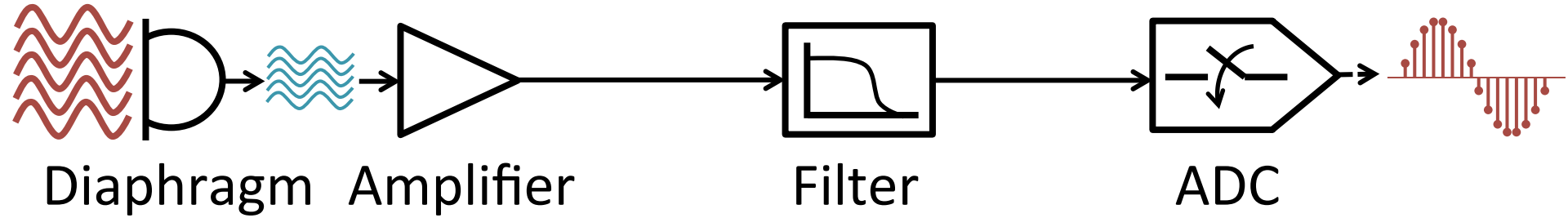


Microphone working principle

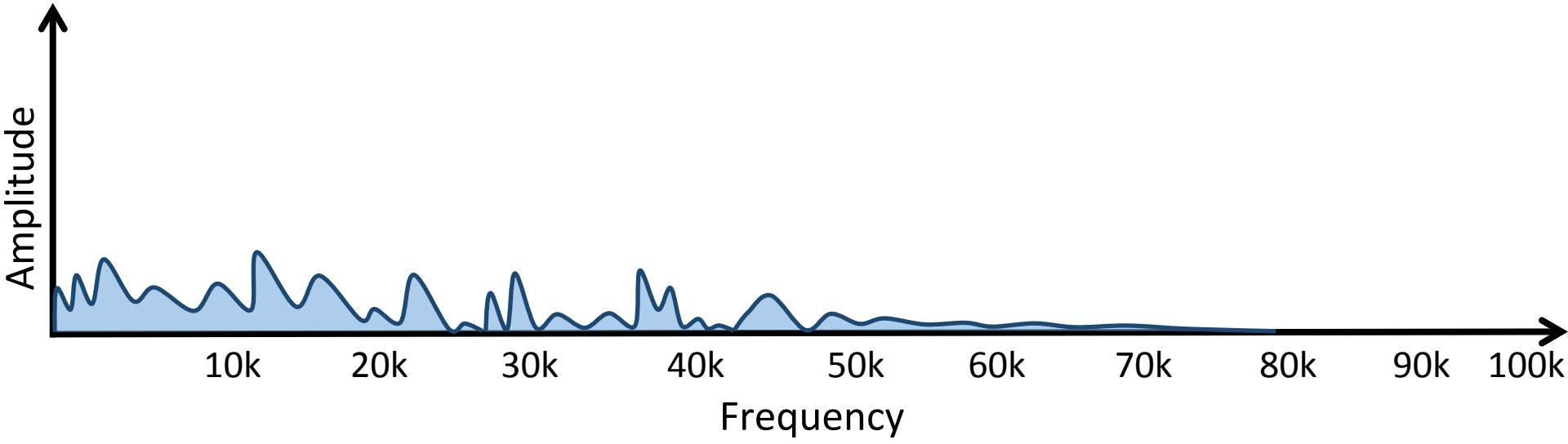


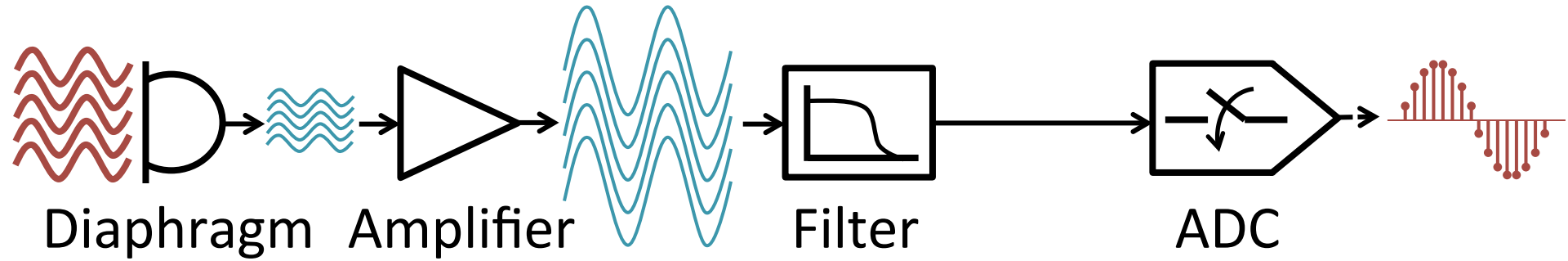
Microphone working principle



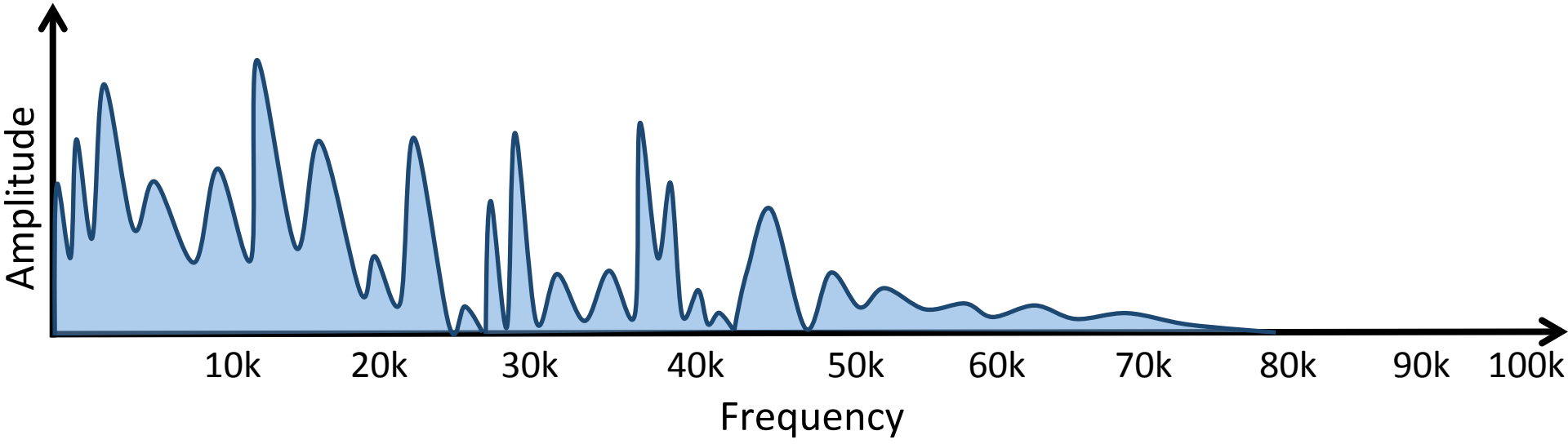


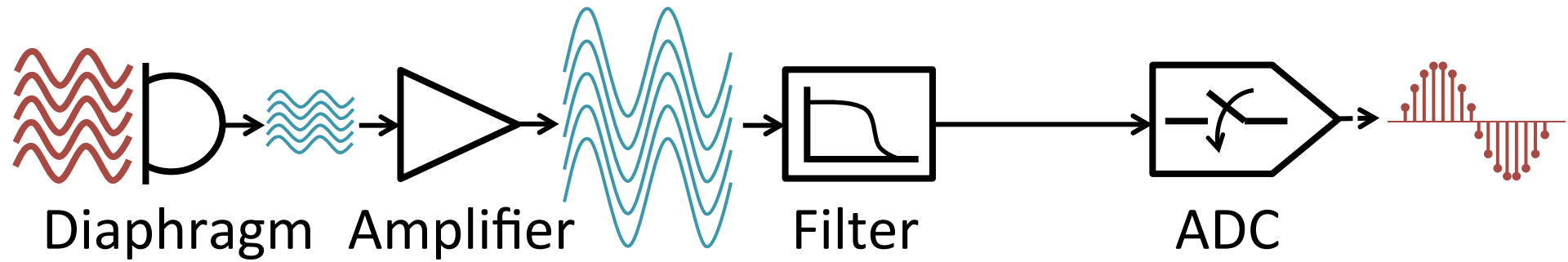
Microphone working principle



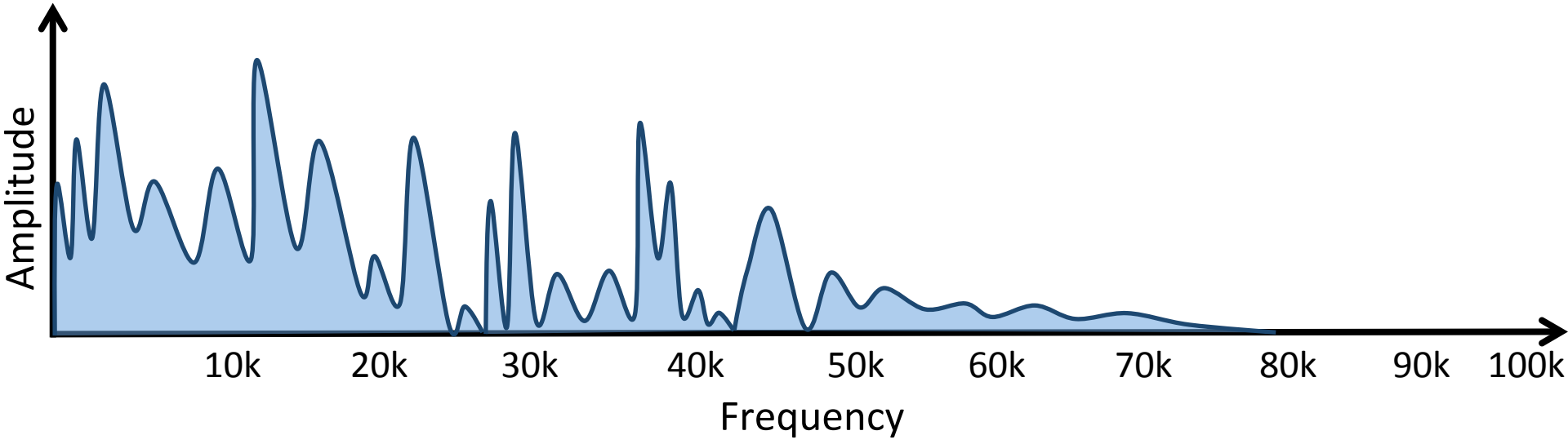


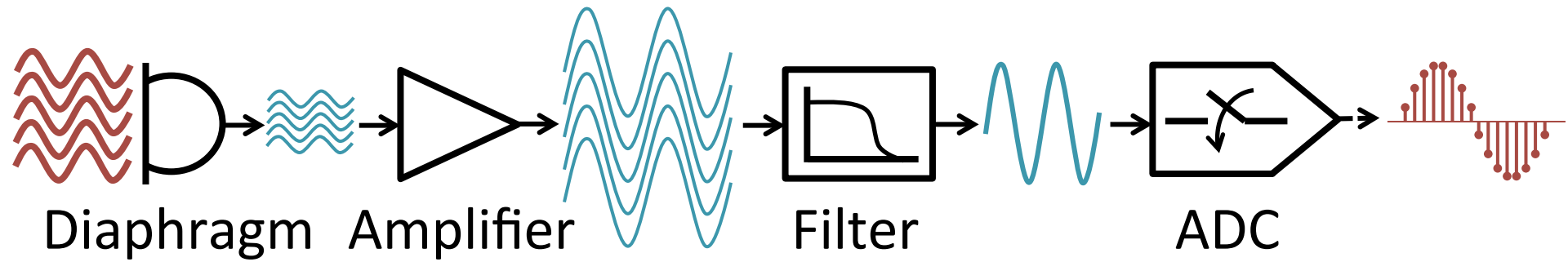
Microphone working principle



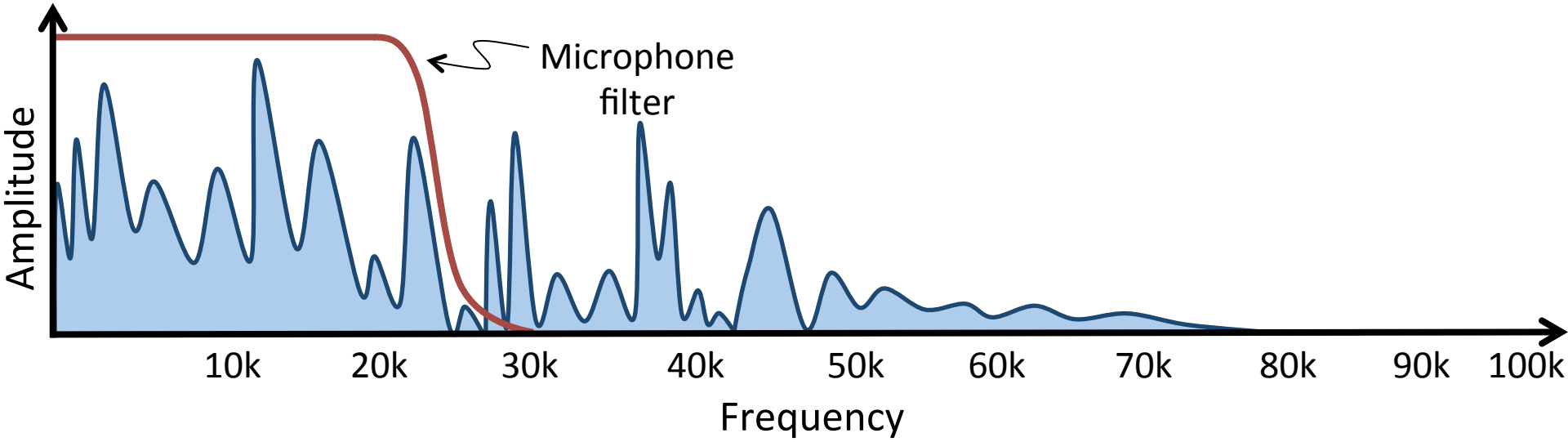


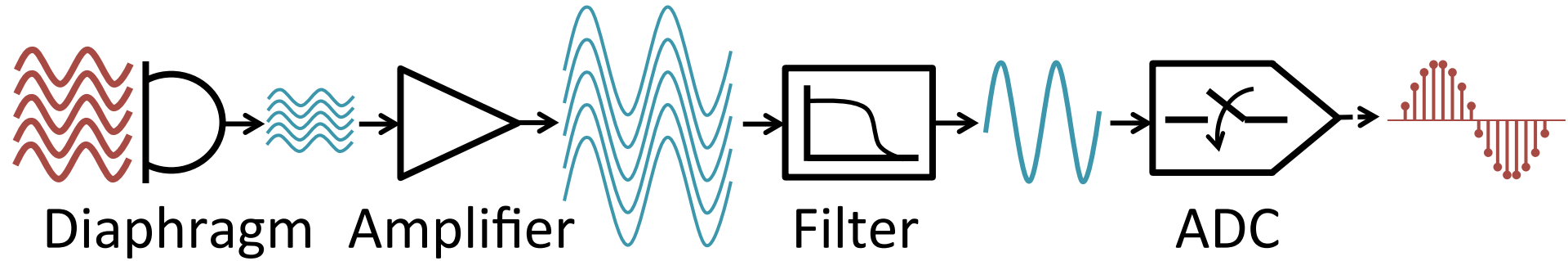
Microphone working principle



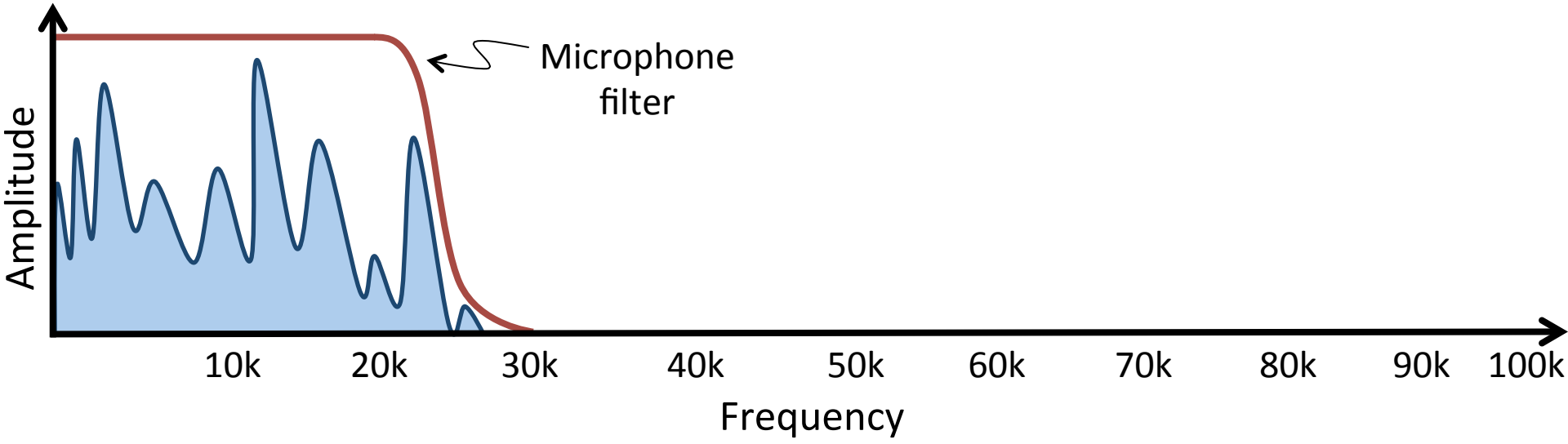


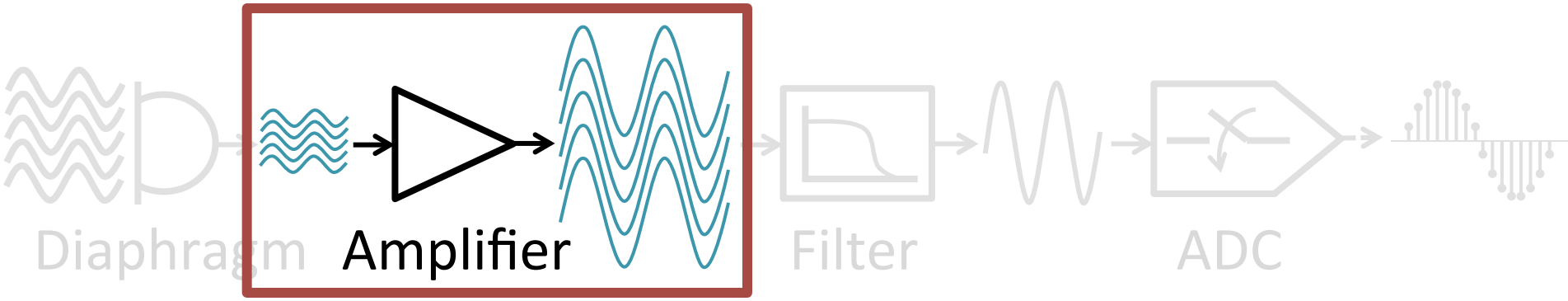
Microphone working principle



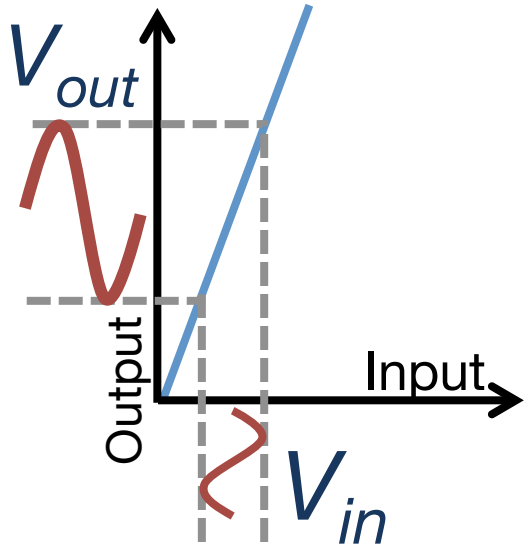


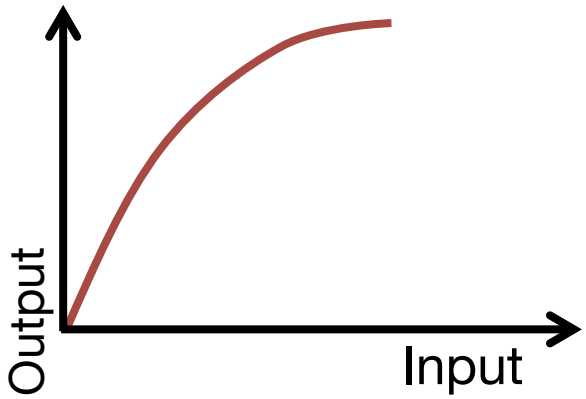
Microphone working principle





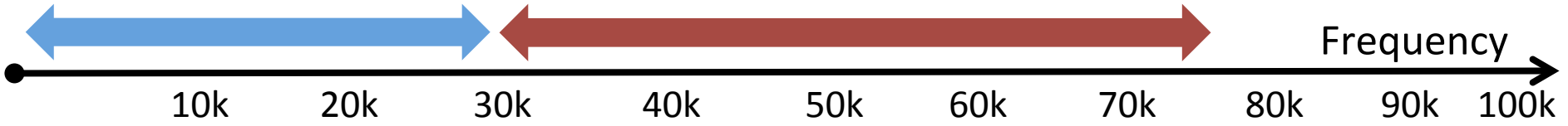
Microphone working principle

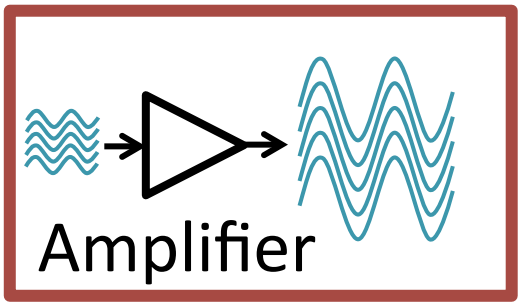




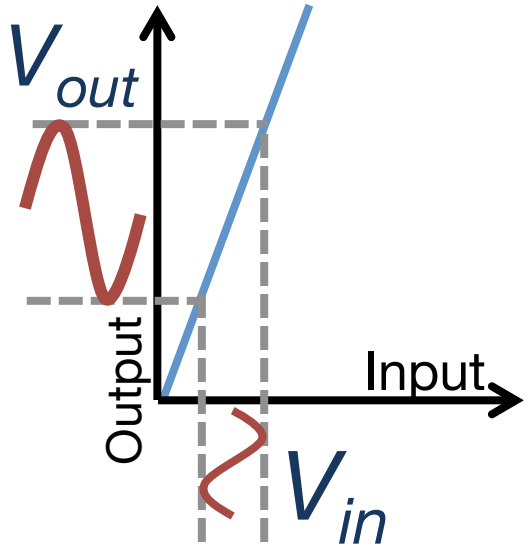
$V_{out} = a_1 V_{in}$

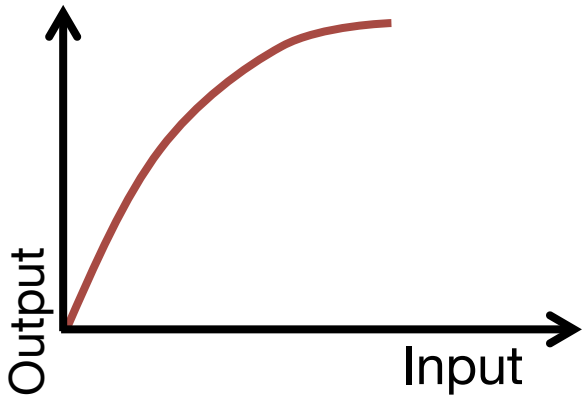
$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$





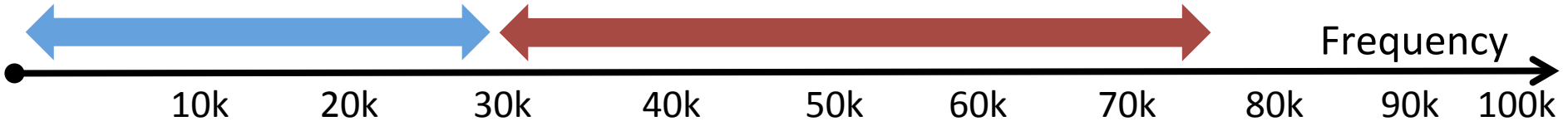
Microphone working principle

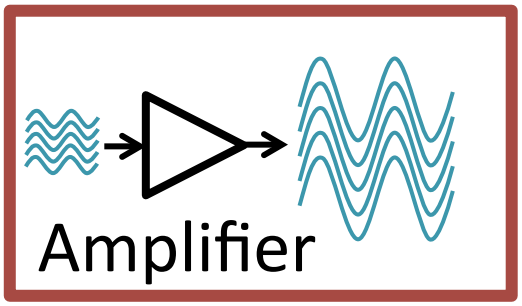




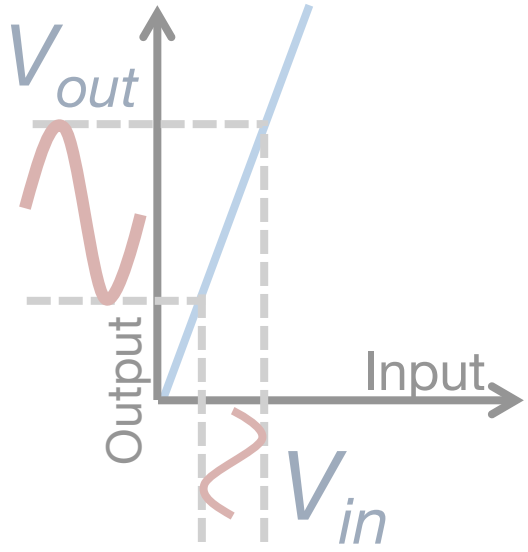
$V_{out} = a_1 V_{in}$

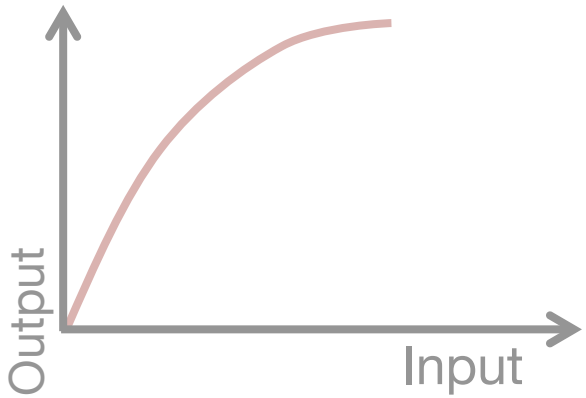
$V_{out} = a_1 V_{in} + a_2 V_{in}^2$





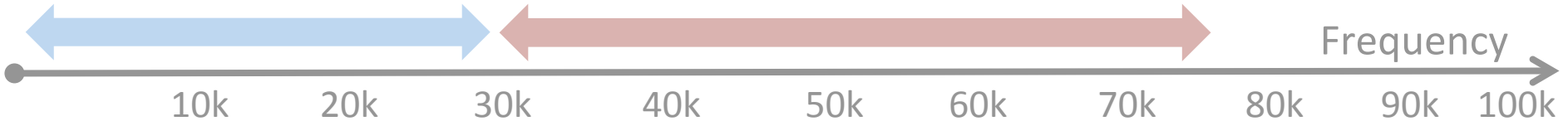
Microphone working principle

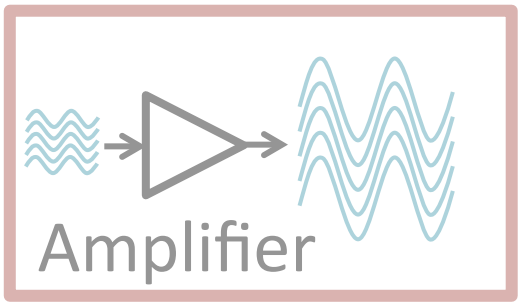




$V_{out} = a_1 V_{in}$

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





Talk outline

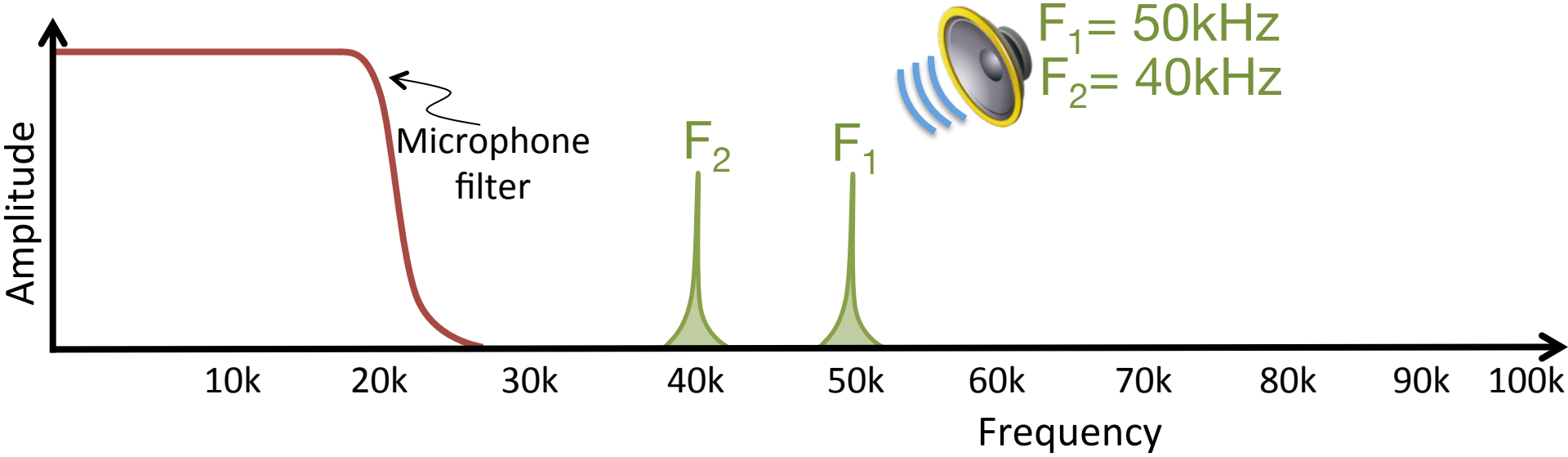
① Microphone Overview

② System Design

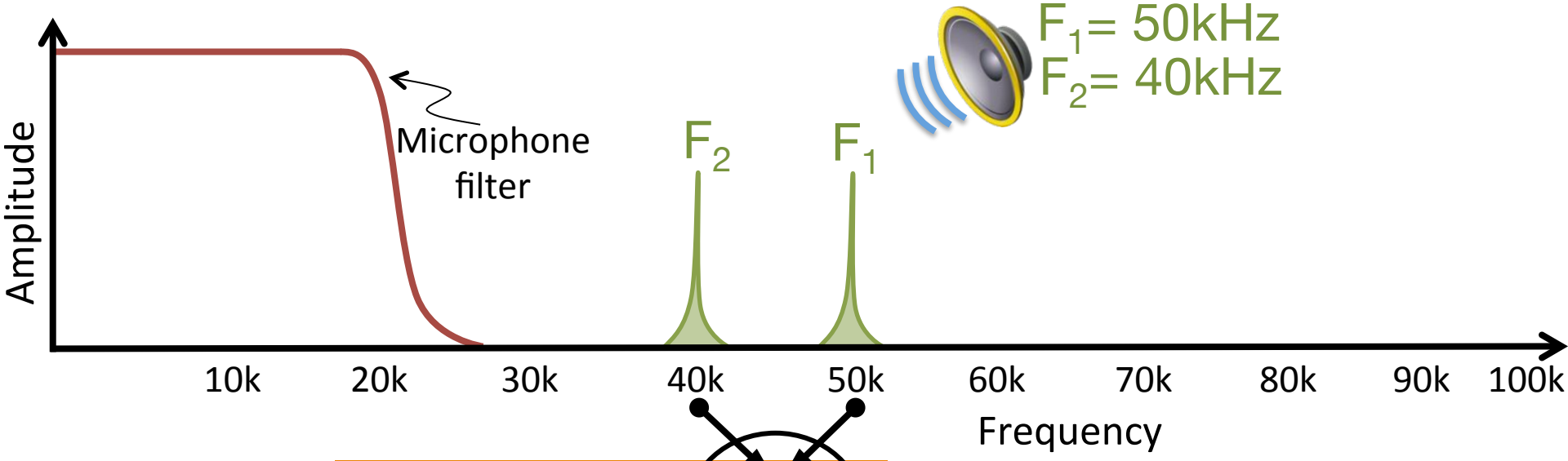
③ Challenges

④ Evaluation

Exploiting amplifier non-linearity



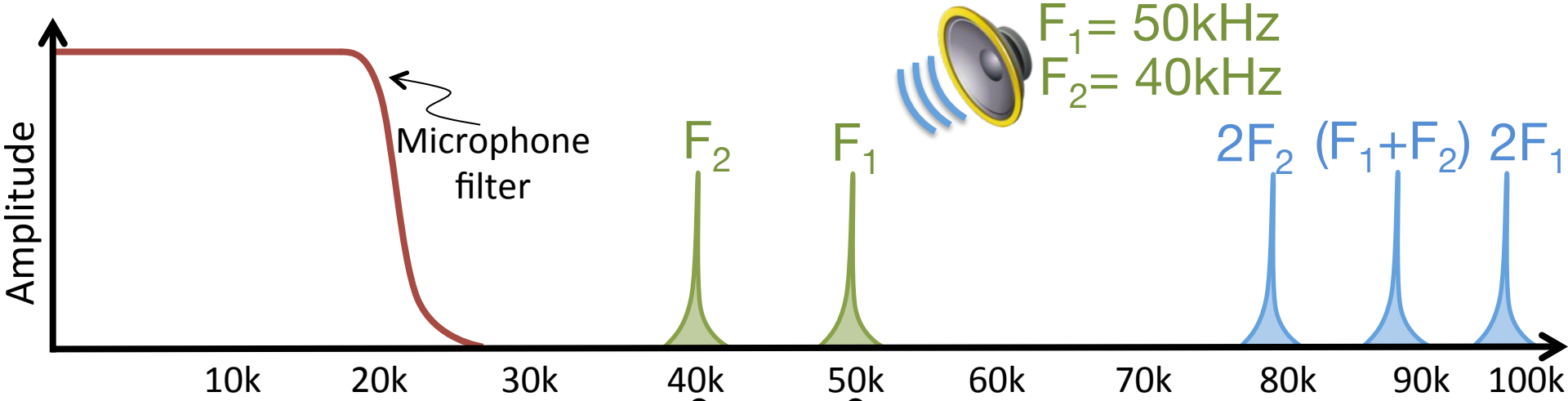
Exploiting amplifier non-linearity



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

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

Exploiting amplifier non-linearity

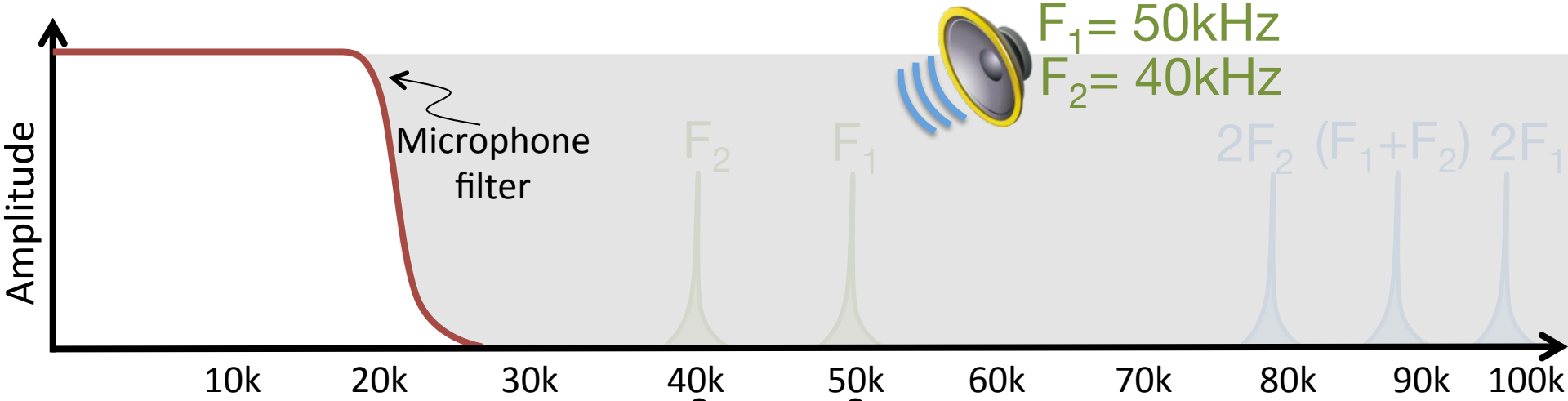


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

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

Exploiting amplifier non-linearity



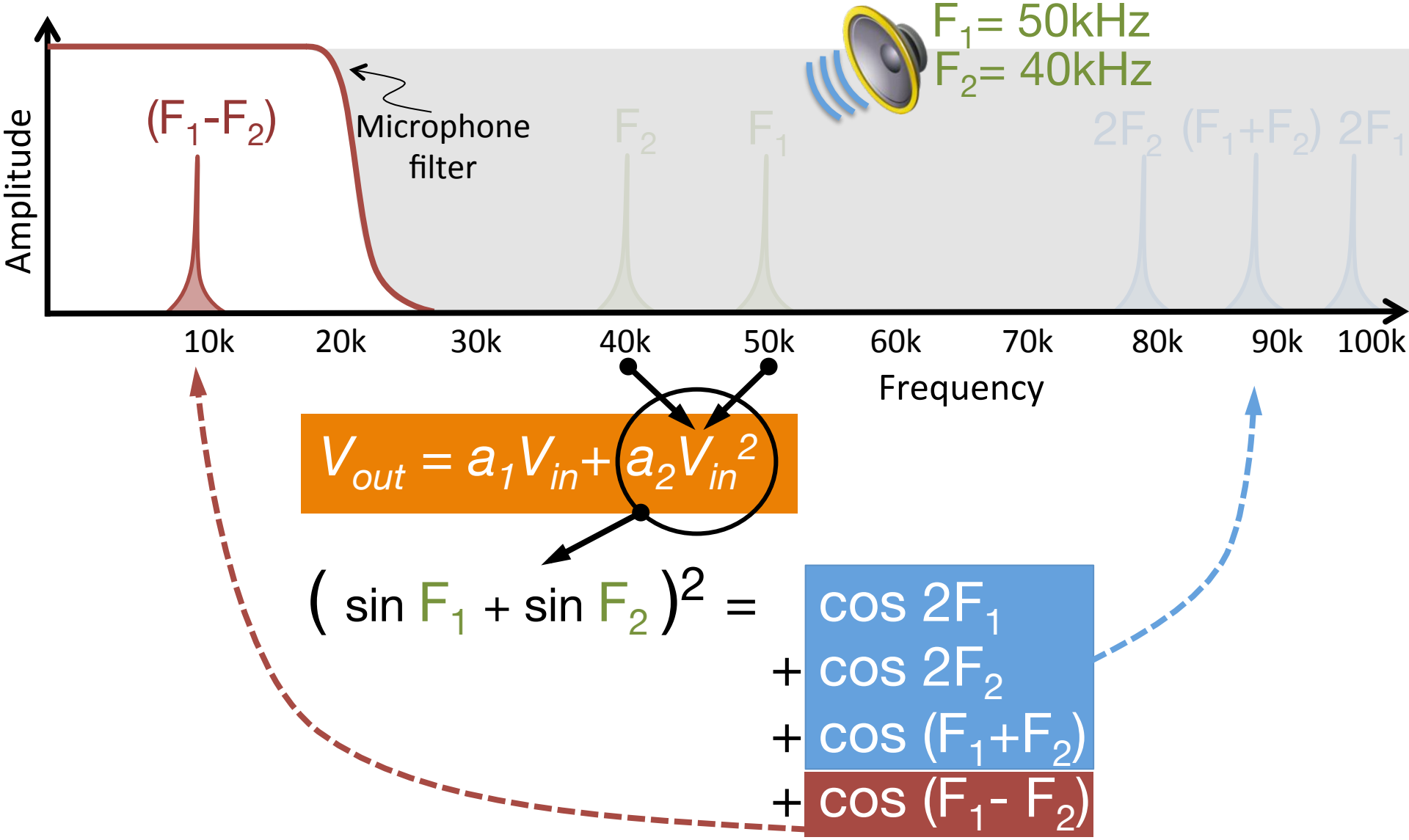
F_1= 50kHz
F_2= 40kHz

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

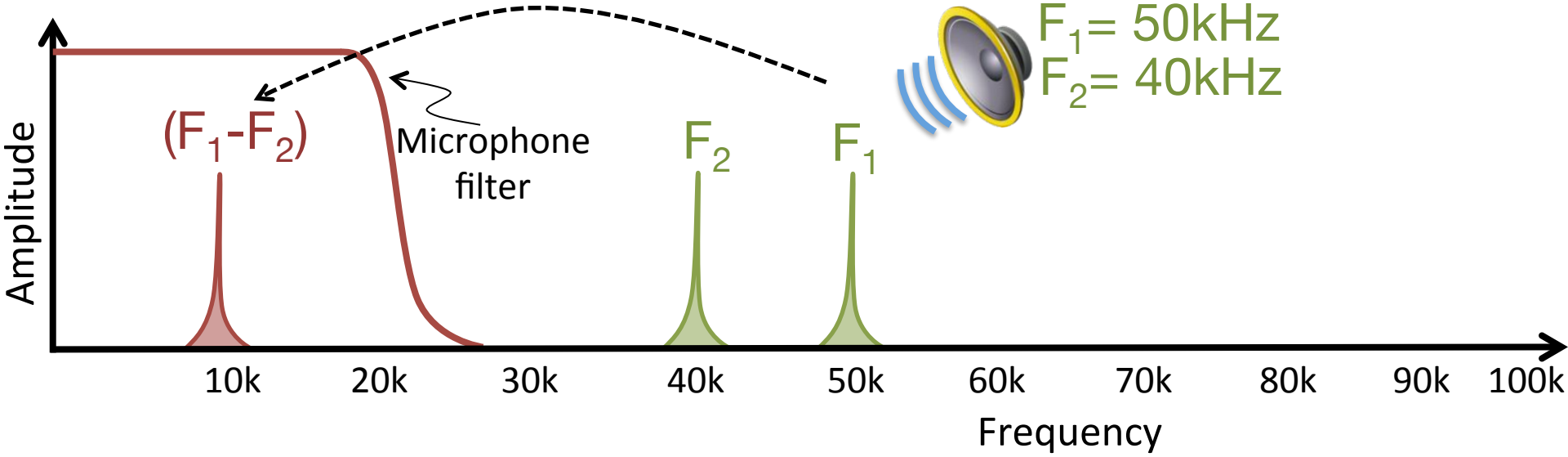
$$(\sin F_1 + \sin F_2)^2 =$$

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

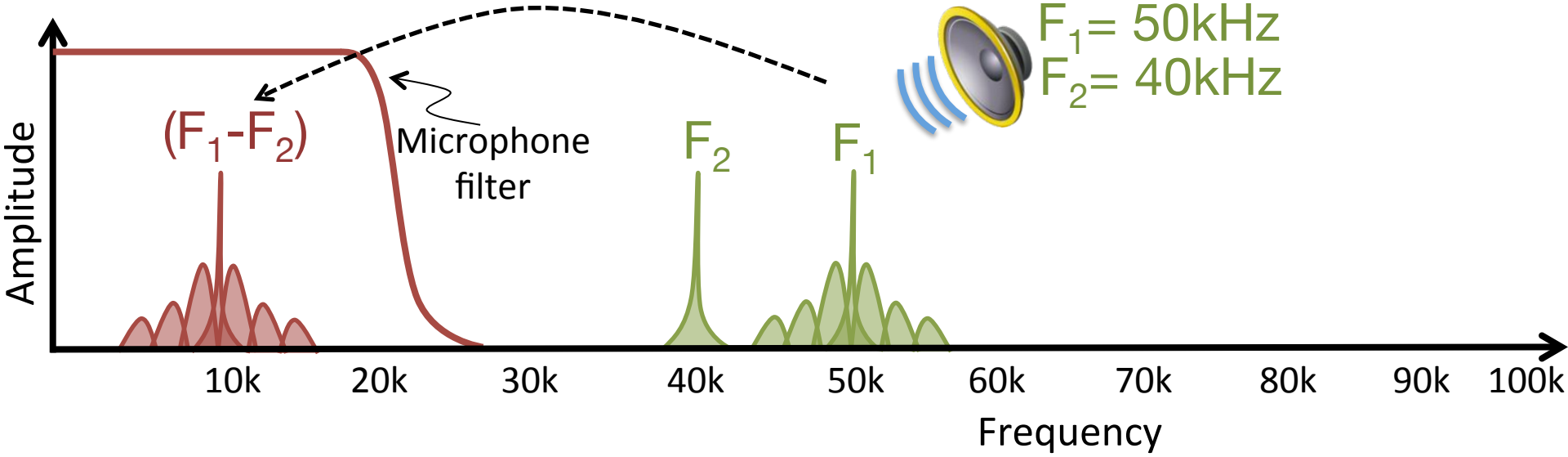
Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Exploiting amplifier non-linearity



Talk outline

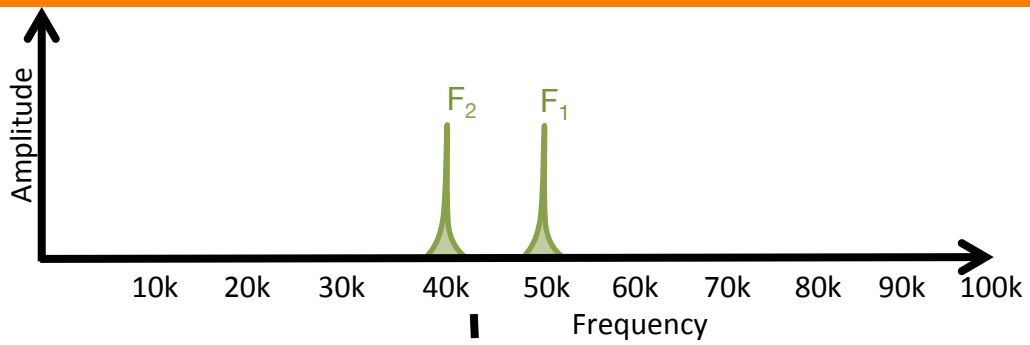
① Microphone Overview

② System Design

③ Challenges

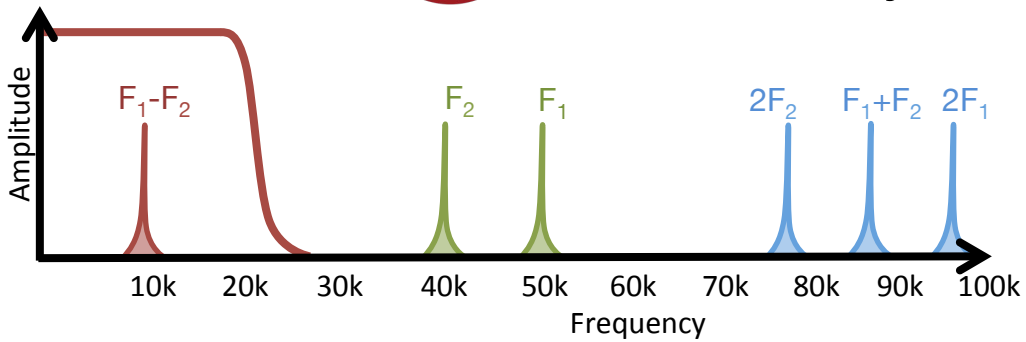
④ Evaluation

Challenges

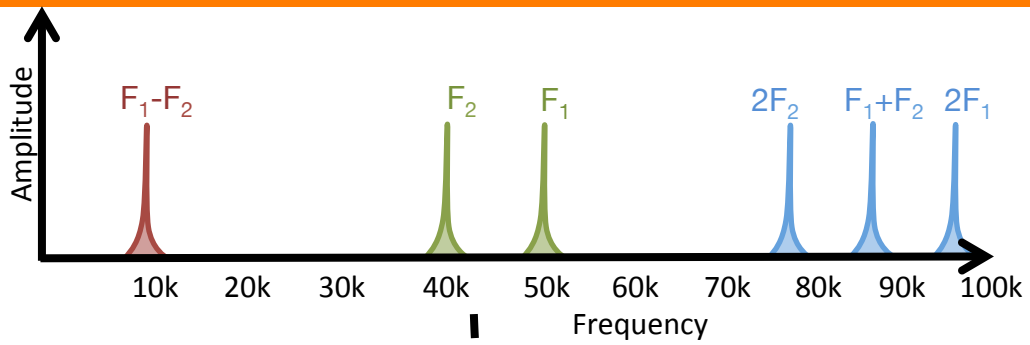


Speaker's nonlinearity

Microphone's nonlinearity

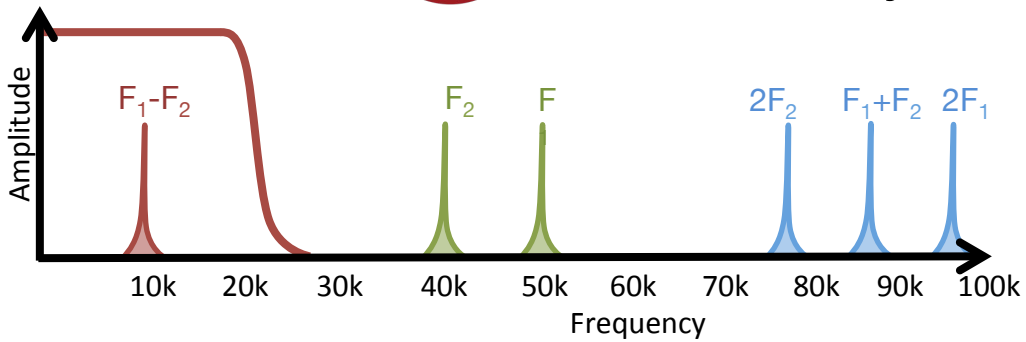


Challenges

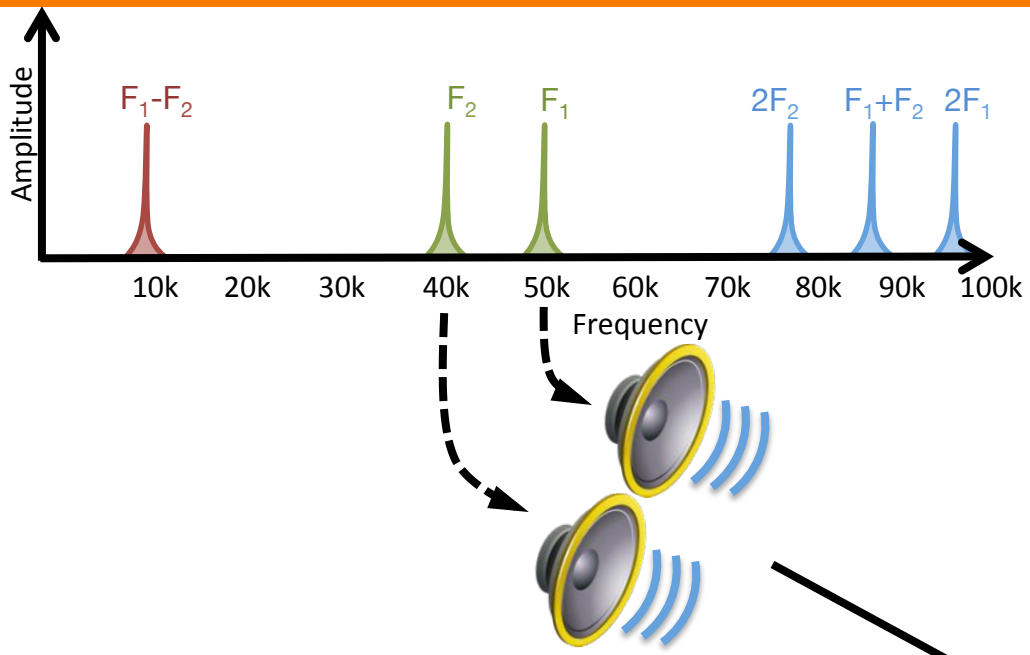


Speaker's nonlinearity

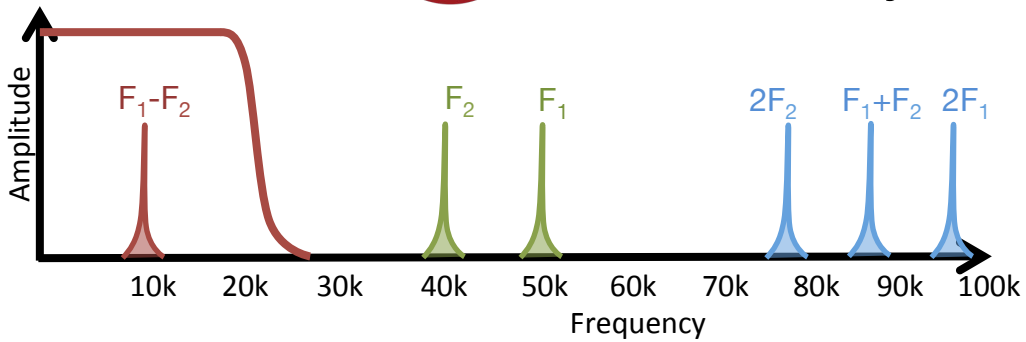
Microphone's nonlinearity



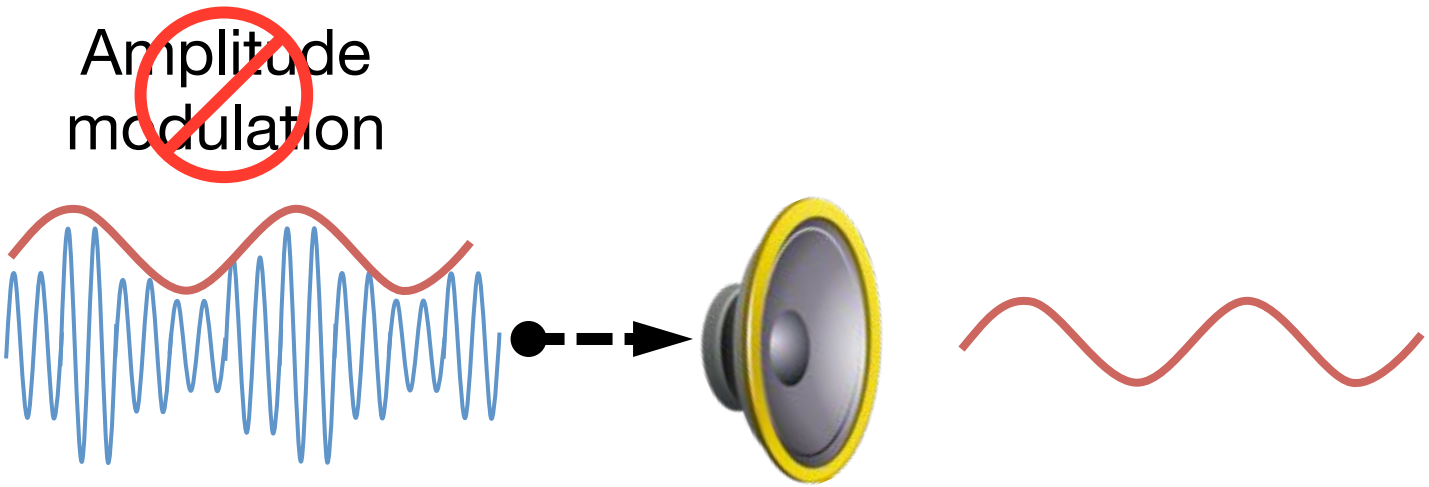
Challenges



Microphone's nonlinearity

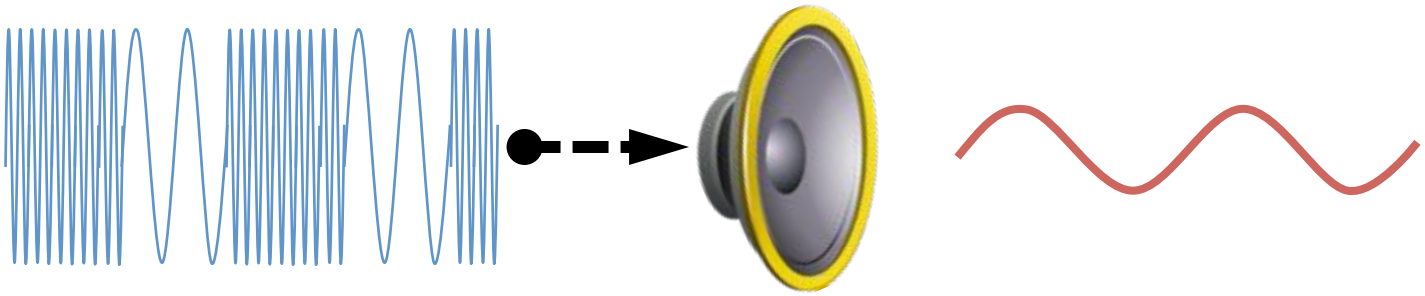


Challenges



Challenges

Frequency modulation



Ultrasonic speaker

Challenges

- Signal self-demodulation
- Piezoelectric ringing effect
- Carrier intermixing
- Spectrum inversion
- Carrier power allocation

Talk outline

① Microphone Overview

② System Design

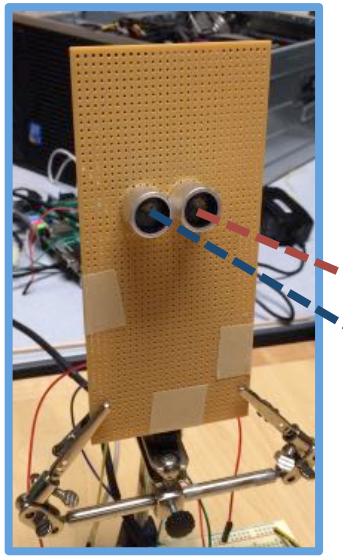
③ Challenges

④ Evaluation

Threats: Inaudible voice attack

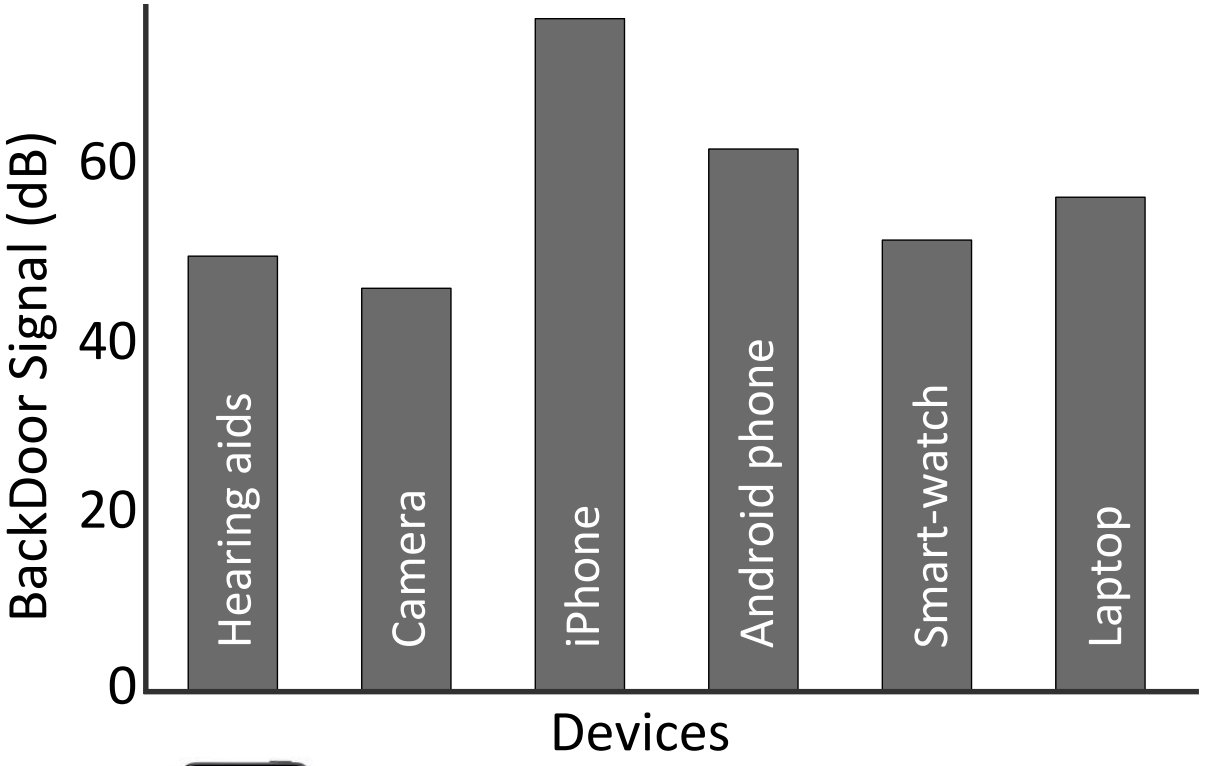
Live Demo: Attacking Amazon Echo though inaudible sound

Hardware generalizability



40 kHz

50 kHz



Hearing Aid

Camera

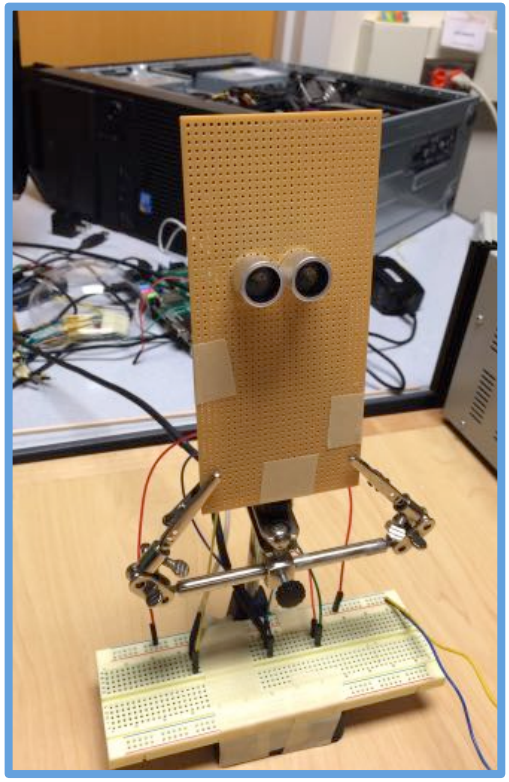
iPhone

Android phone

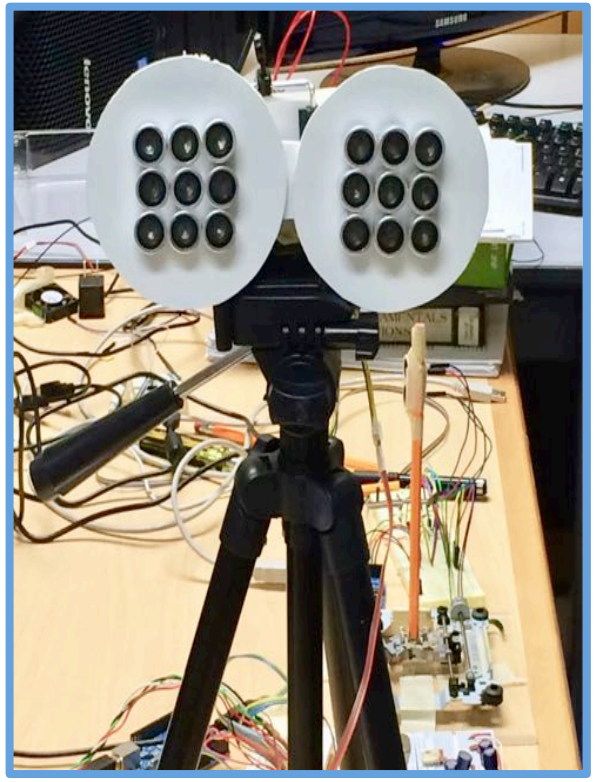
Smartwatch

Laptop

Implementation

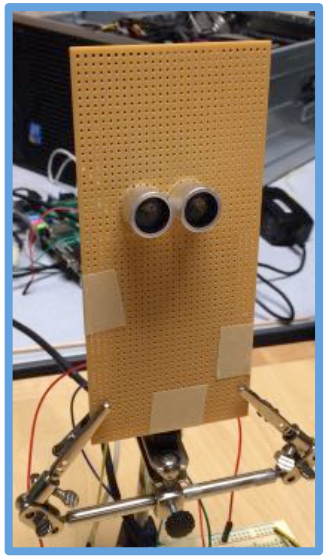


Communication prototype



Jammer prototype

Communication performance

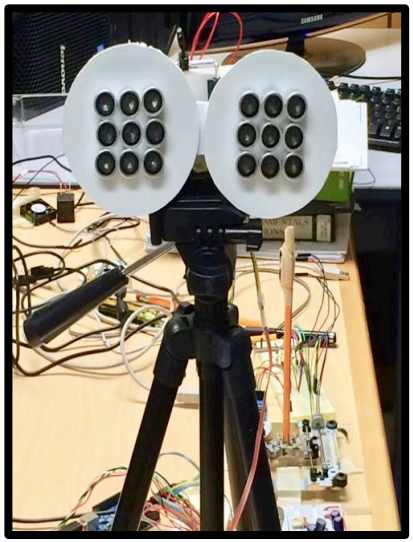


FM data packets

4kbps
up to 1 meter

More power can increase the distance

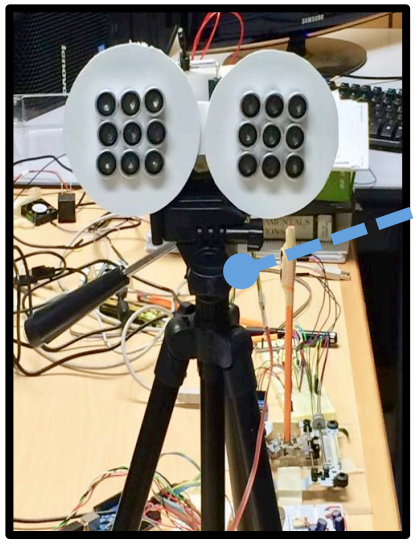
Jamming performance



BackDoor jammer

Spy microphone

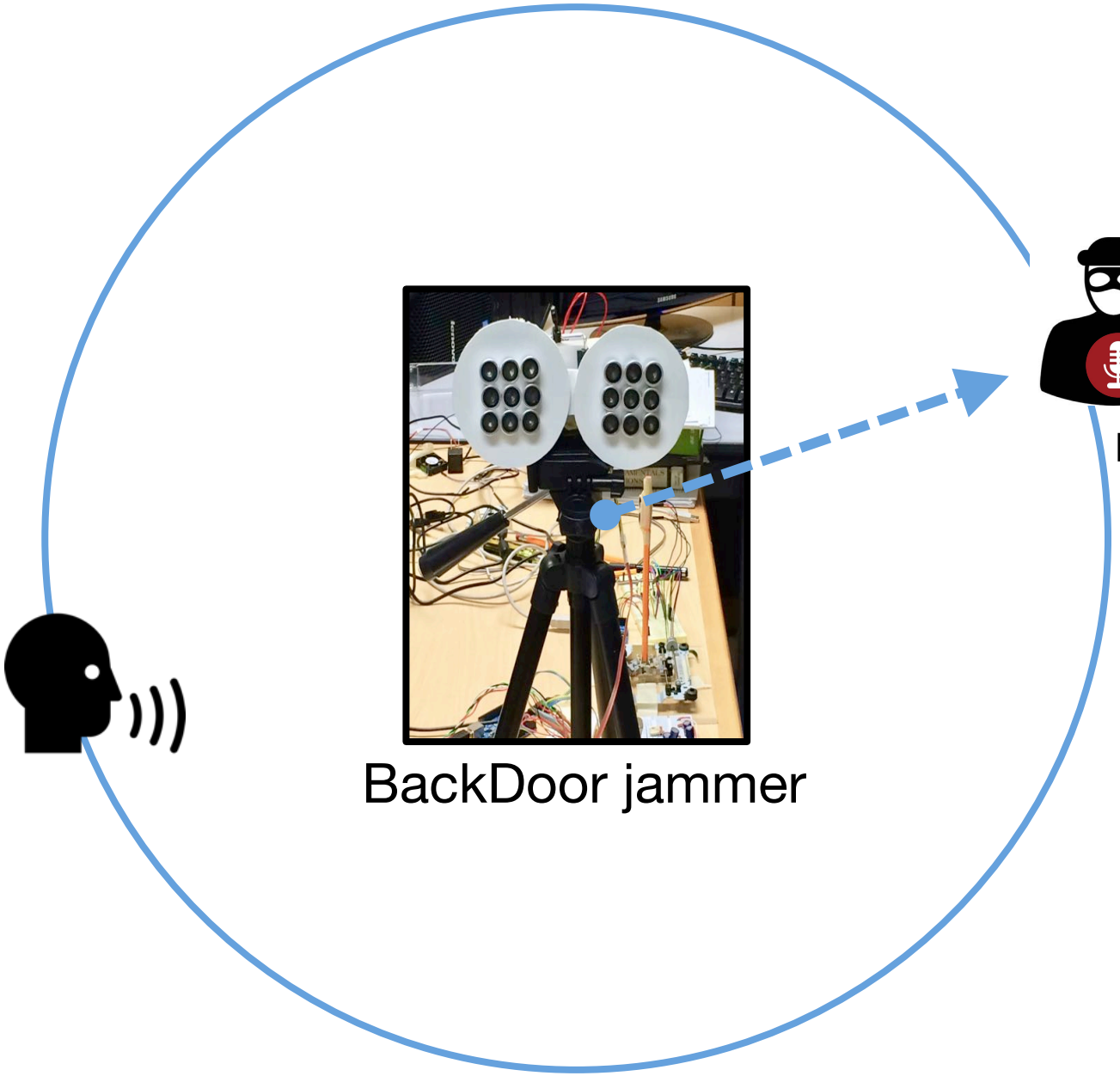
Jamming performance



BackDoor jammer

Spy microphone

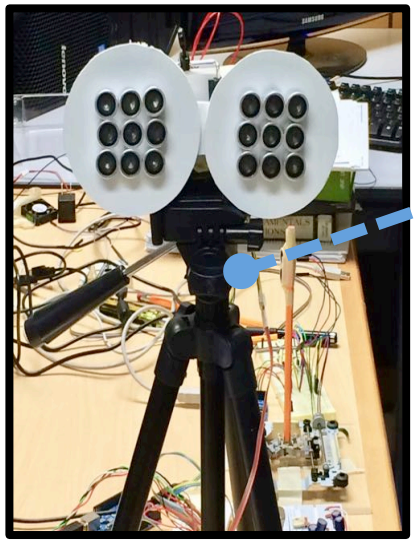
Jamming performance



BackDoor jammer

Spy microphone

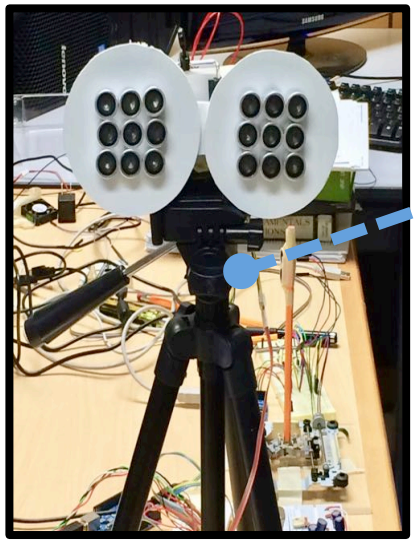
Jamming performance



BackDoor jammer

Spy microphone

Jamming performance

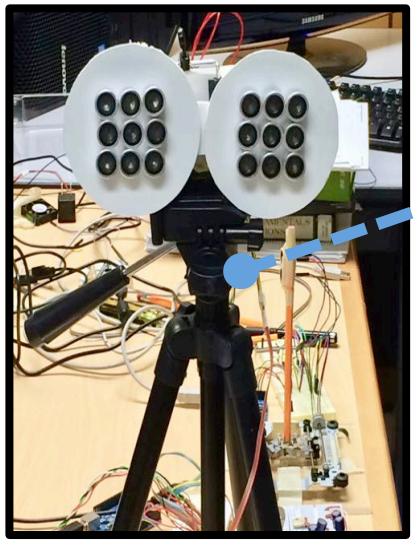


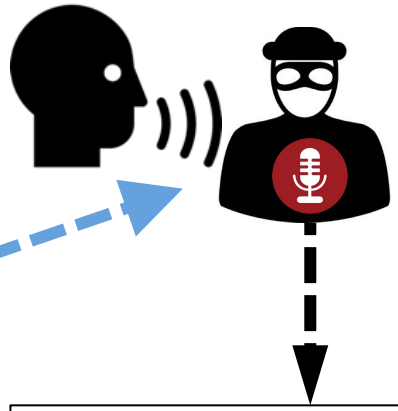
BackDoor jammer

Spy microphone

Jamming performance

2000 spoken words

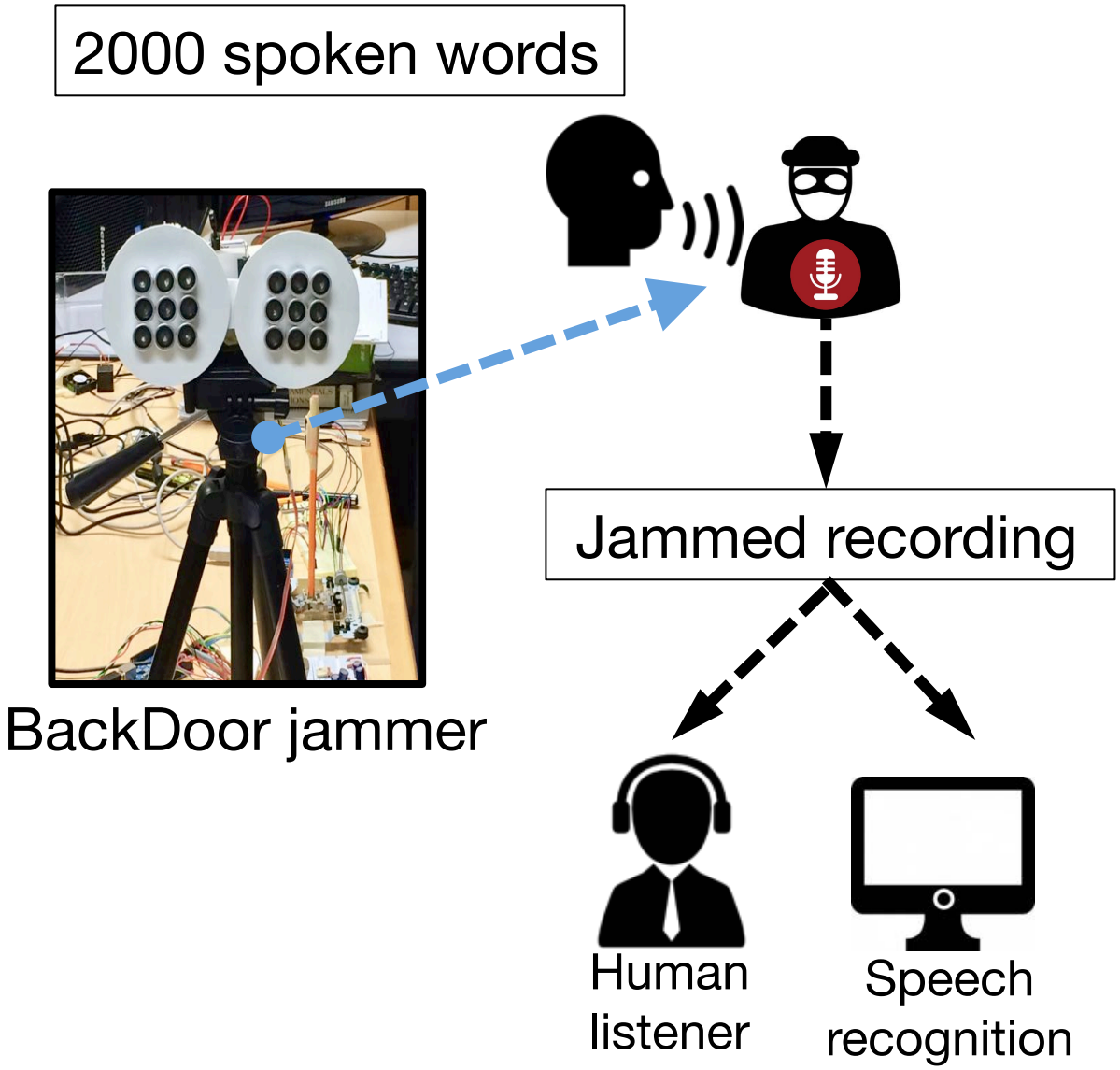




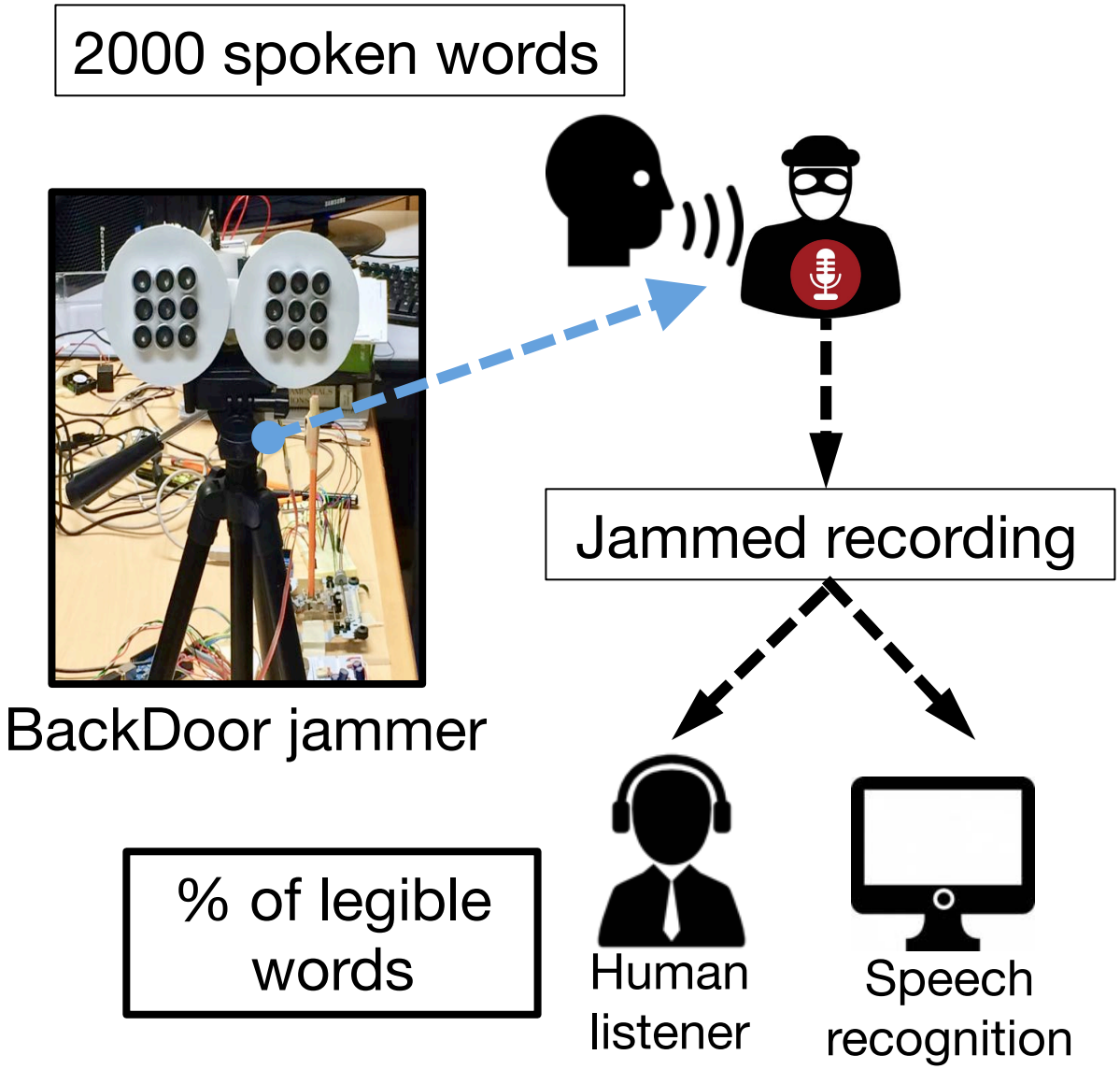
Jammed recording

BackDoor jammer

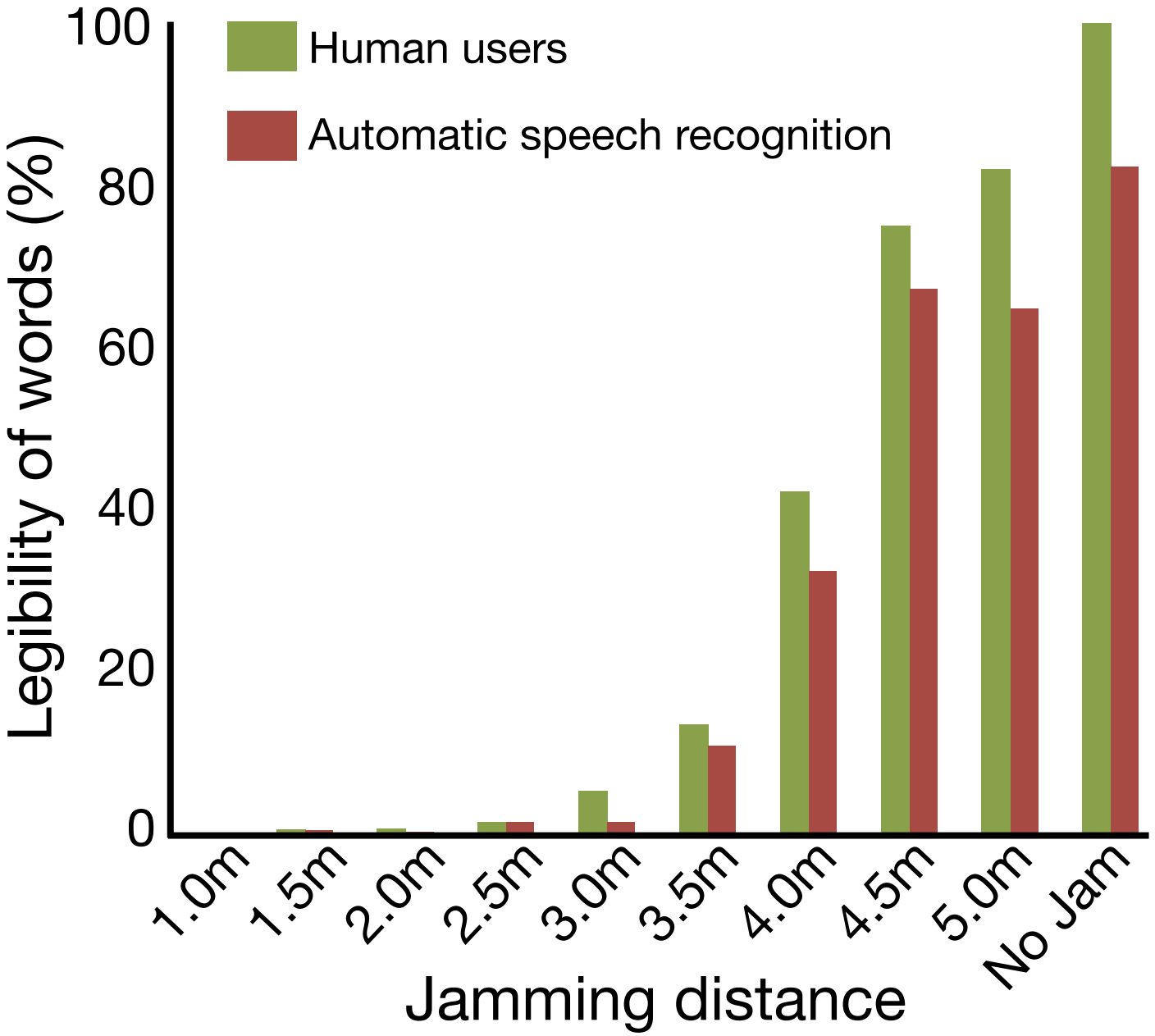
Jamming performance



Jamming performance



Jamming performance



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

Ripple: Communication through Physical Vibration

Short range communication:
a new need of this decade

Short range communication:
a new need of this decade


Security and Alarm
HVAC Control
Light Control
Motion Sensor
Thermostat
Environmental Monitoring
Door Control
Internet Gateway
Energy Management
Window Control
Home Control Box
Remote Control

Emerging technologies for short range

Driving forces of short range communication research

Emerging technologies for short range

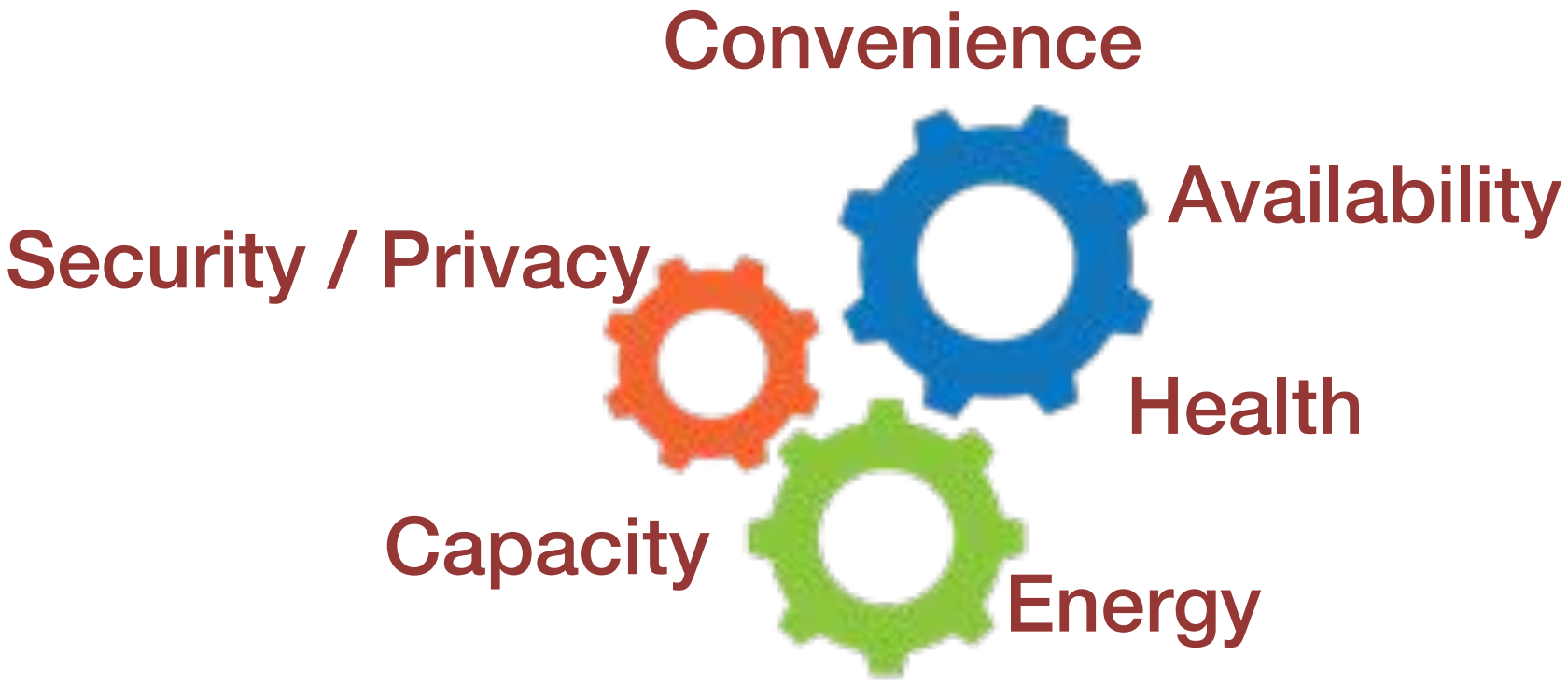
Emerging technologies for short range

Security / Privacy

Capacity

Driving forces of short range communication research

Emerging technologies for short range



Driving forces of short range communication research

Emerging technologies for short range

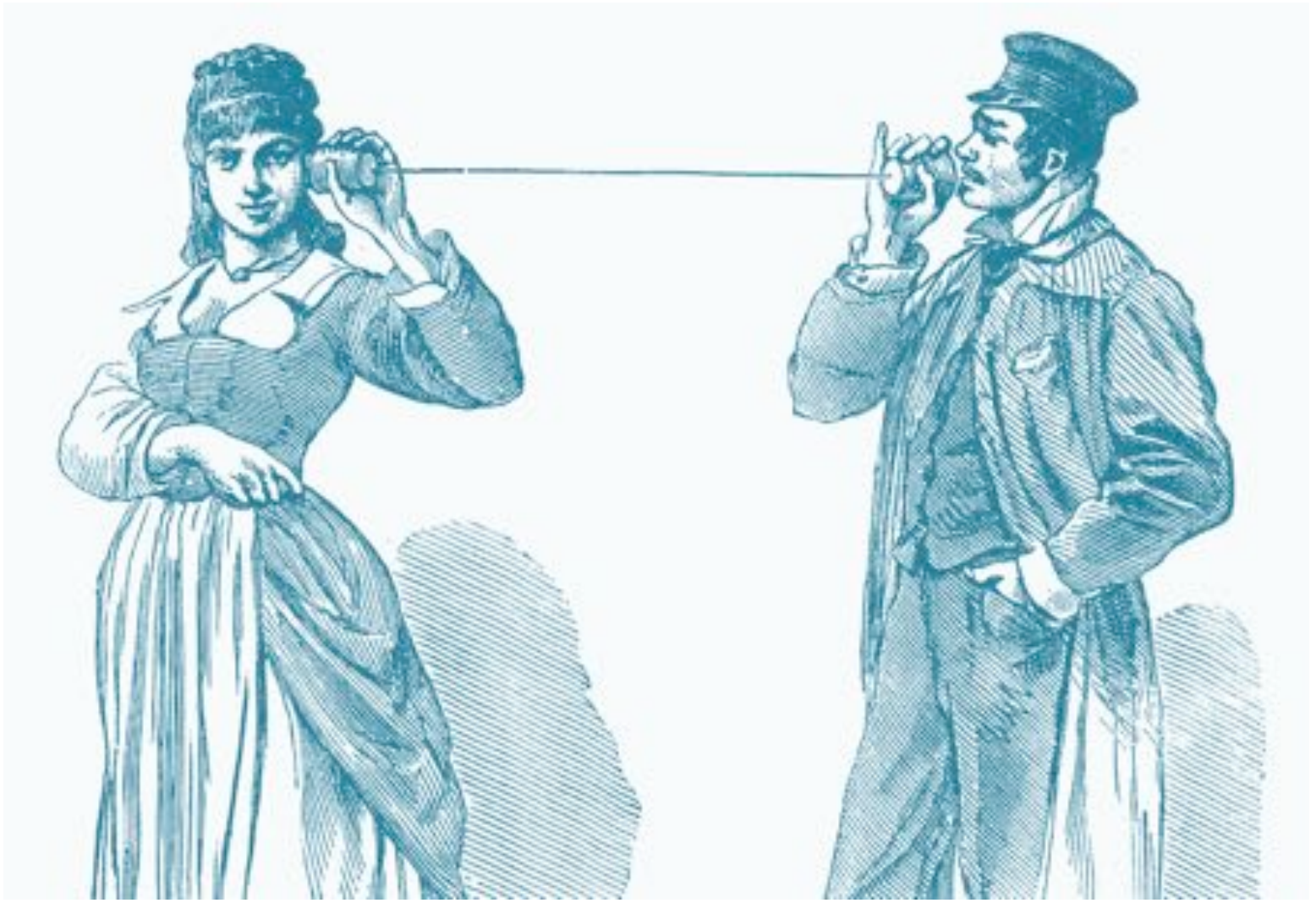
Visible Light Communication

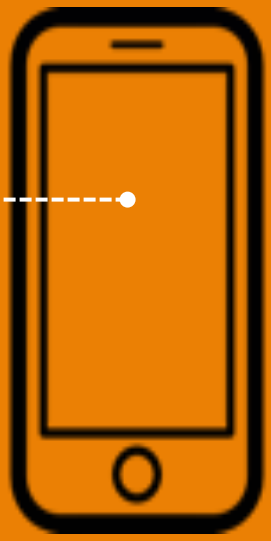
bytelight

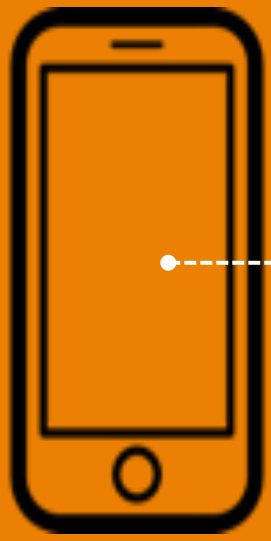
Acoustic NFC

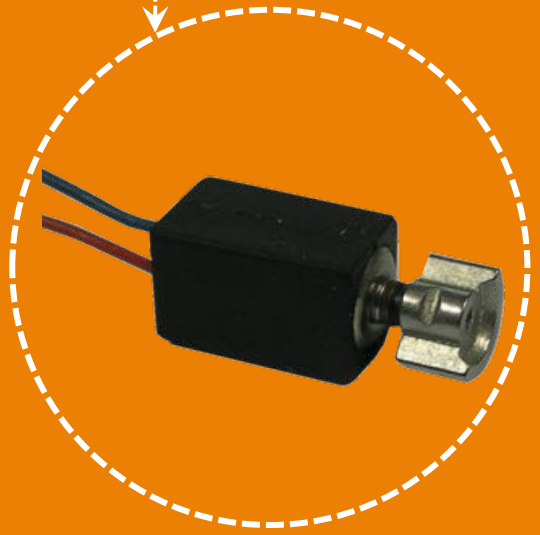
Zoosh
Powered by Norotte

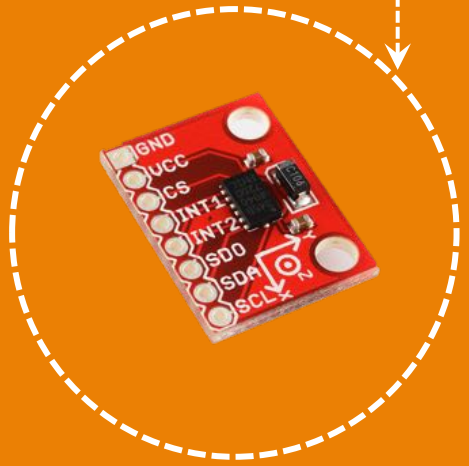
Physical vibration:
a new mode of communication





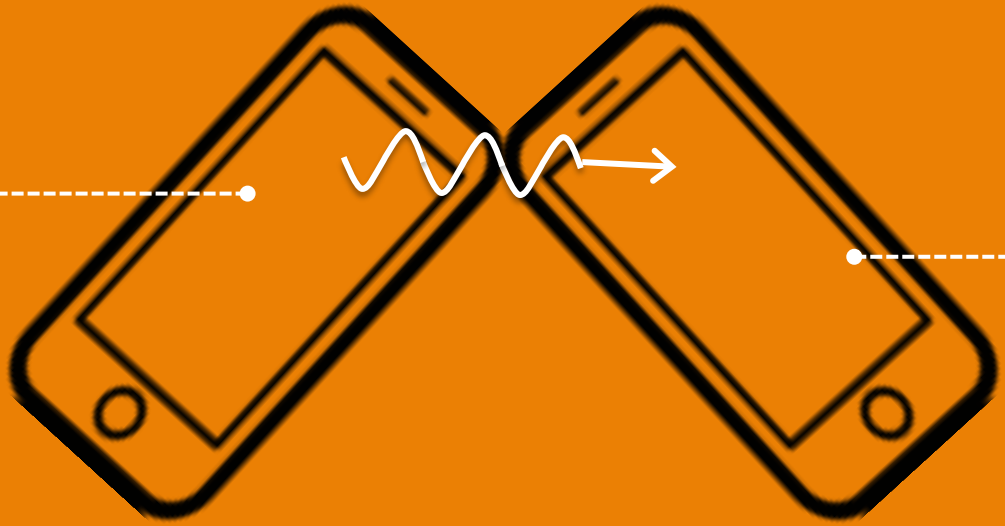


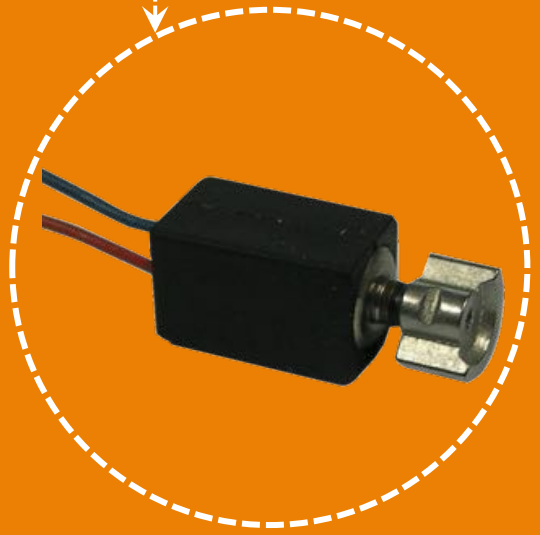




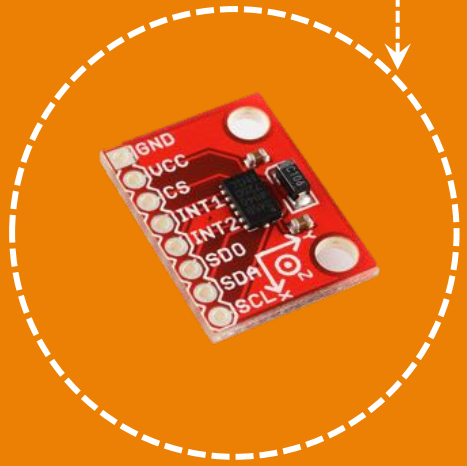
Vibration Motor

Accelerometer

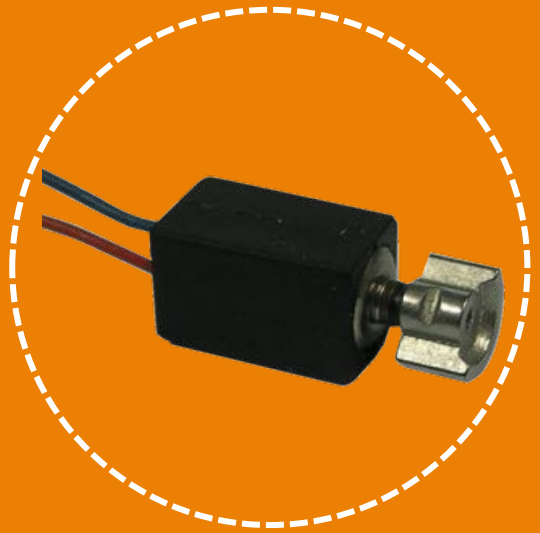




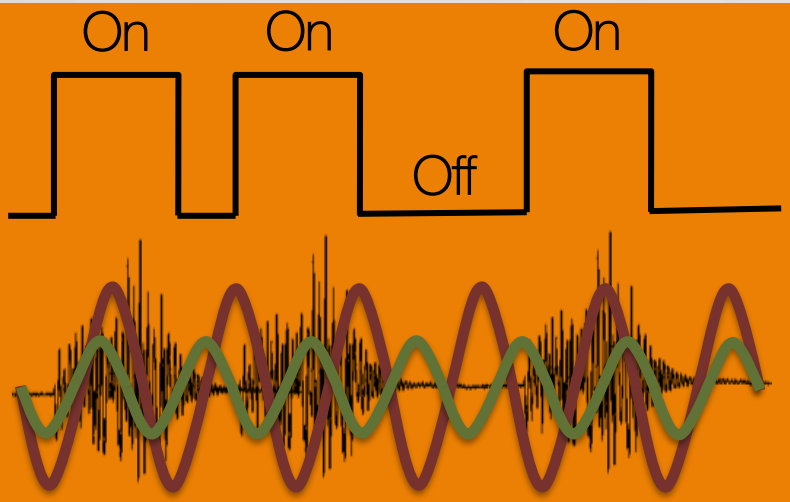
Vibration Motor



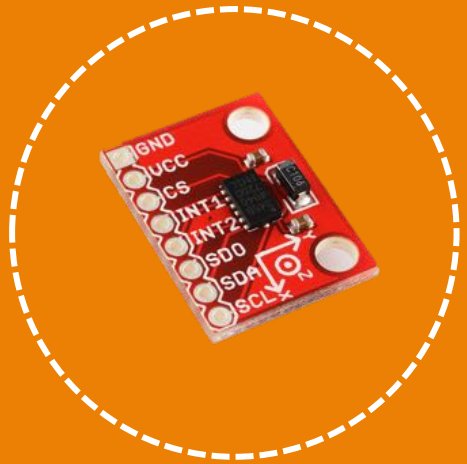
Accelerometer



Vibration Motor



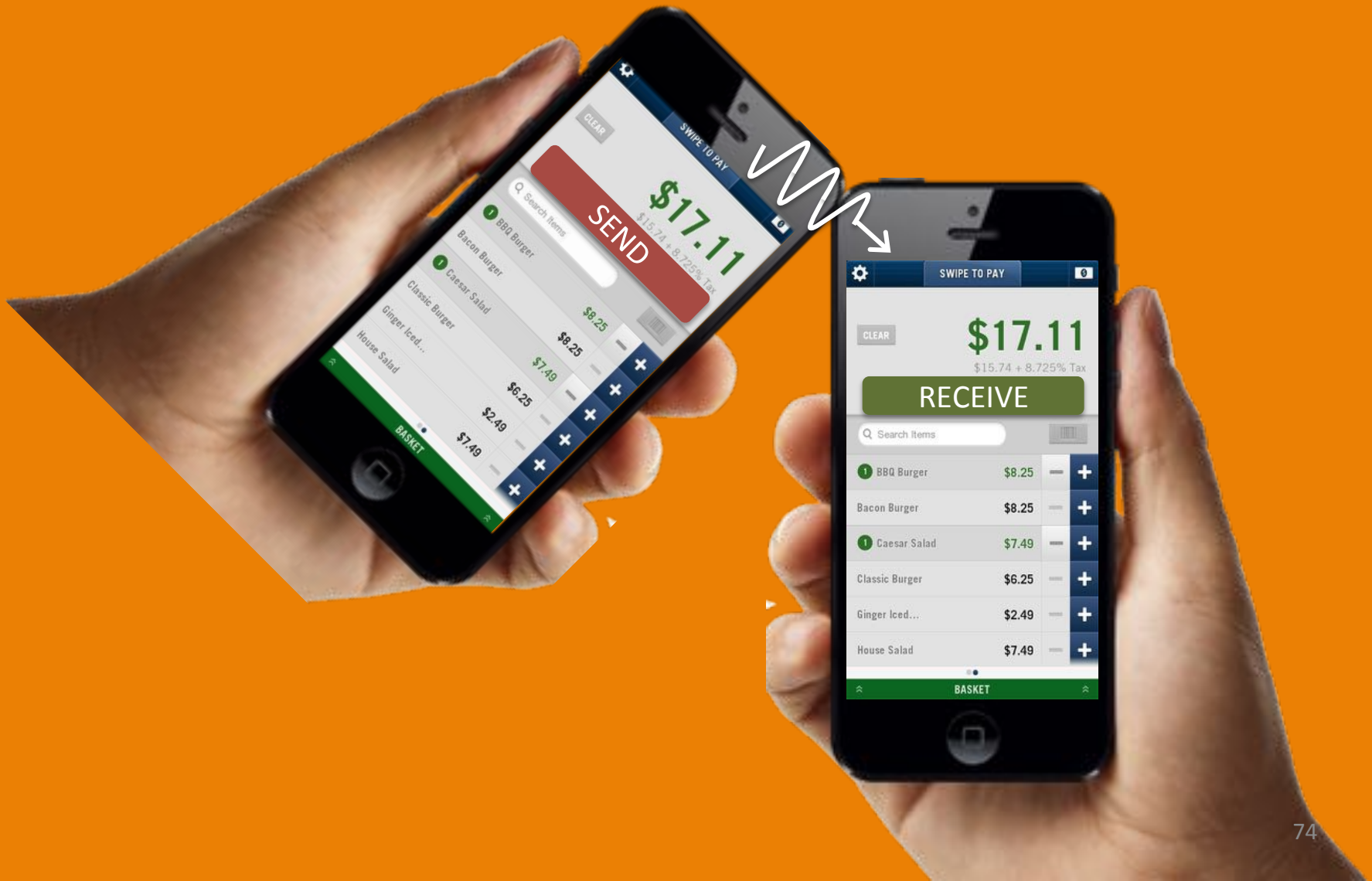
Modulated vibration



Accelerometer

Applications: Mobile Money Transfer

Applications: Mobile Money Transfer



Applications: Authentication with Ring

Applications: Authentication with Ring

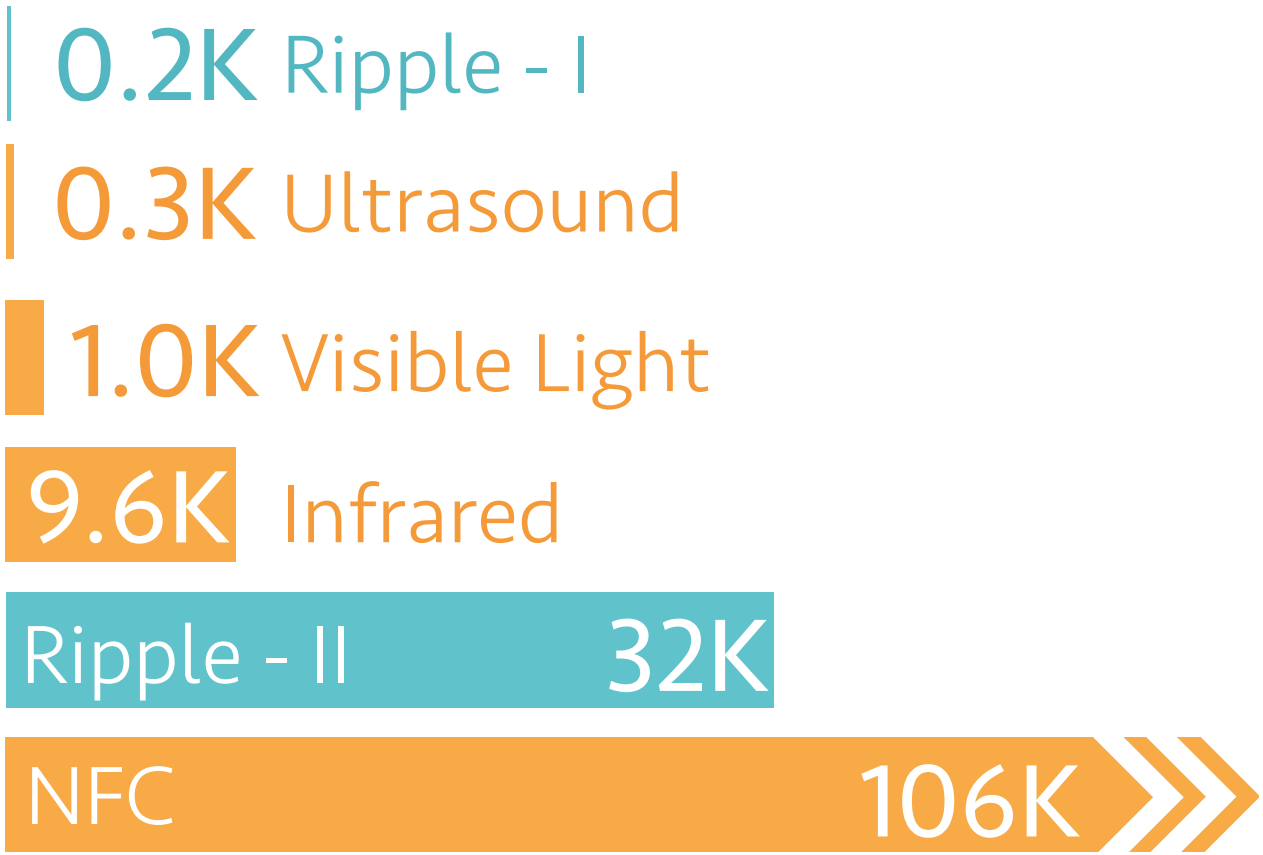
Applications: Authentication with Ring

Applications: Body-Area Network

Or…may be you can come up with a better one

Ripple: Communicating through Physical Vibrations

Ripple data-rate



(bits-per-second, entry level versions)

Ripple-II: Faster Communication through Physical Vibration

Thank You

Website: http://nroy8.web.engr.illinois.edu

SyNRG group website: http://synrg.csl.illinois.edu