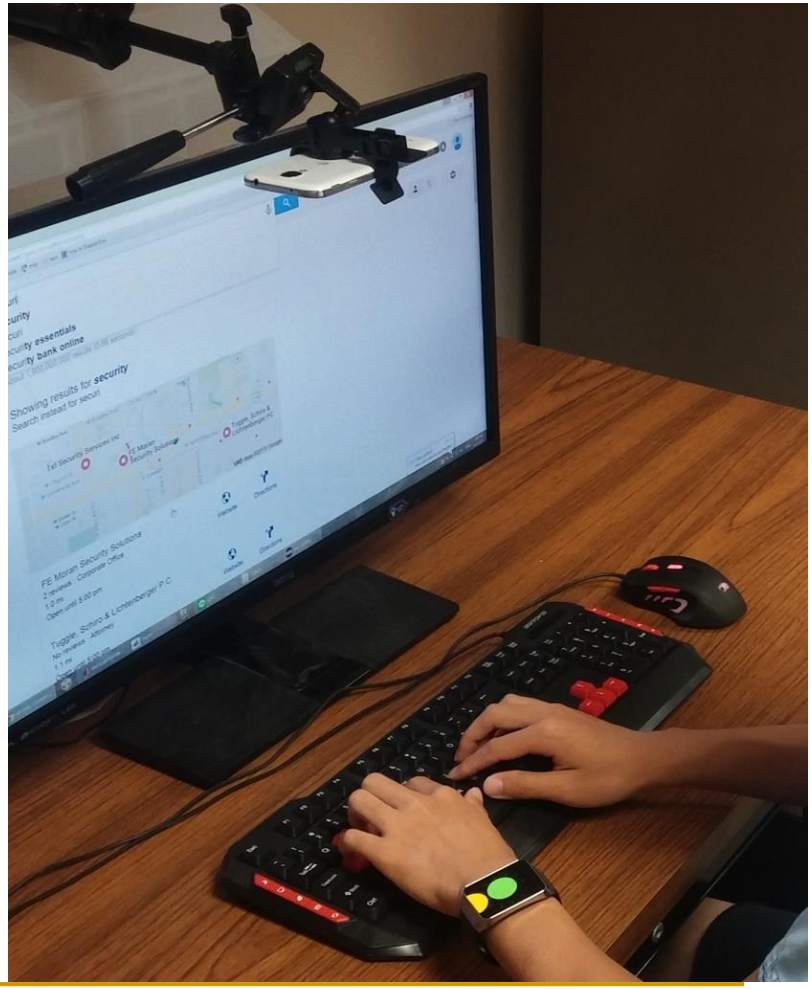
Privacy and Security of Smart Devices

Amitangshu Pal

Guessing the Typing Patterns through IMUs

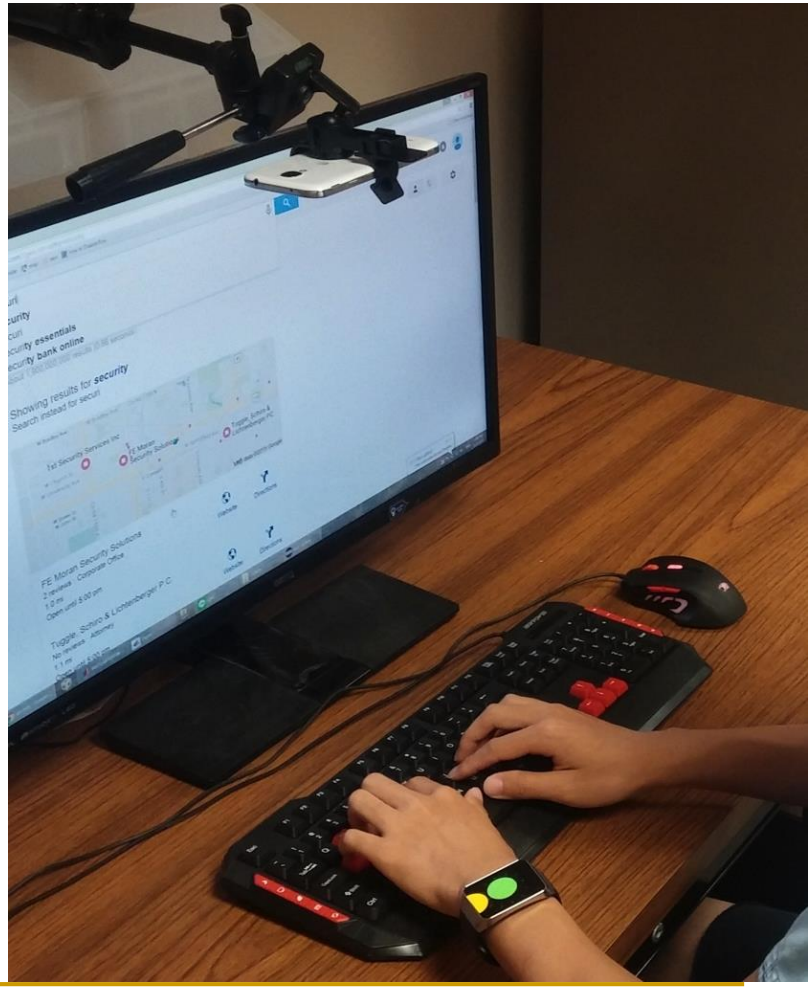
Can we Predict the Typing Behavior from IMU data?

- Offline phase and Online phase
  - In offline phase, the attacker collects the typing behavior from ground truth and IMU readings
  - In online phase, the attacker uses the IMU readings to guess the words



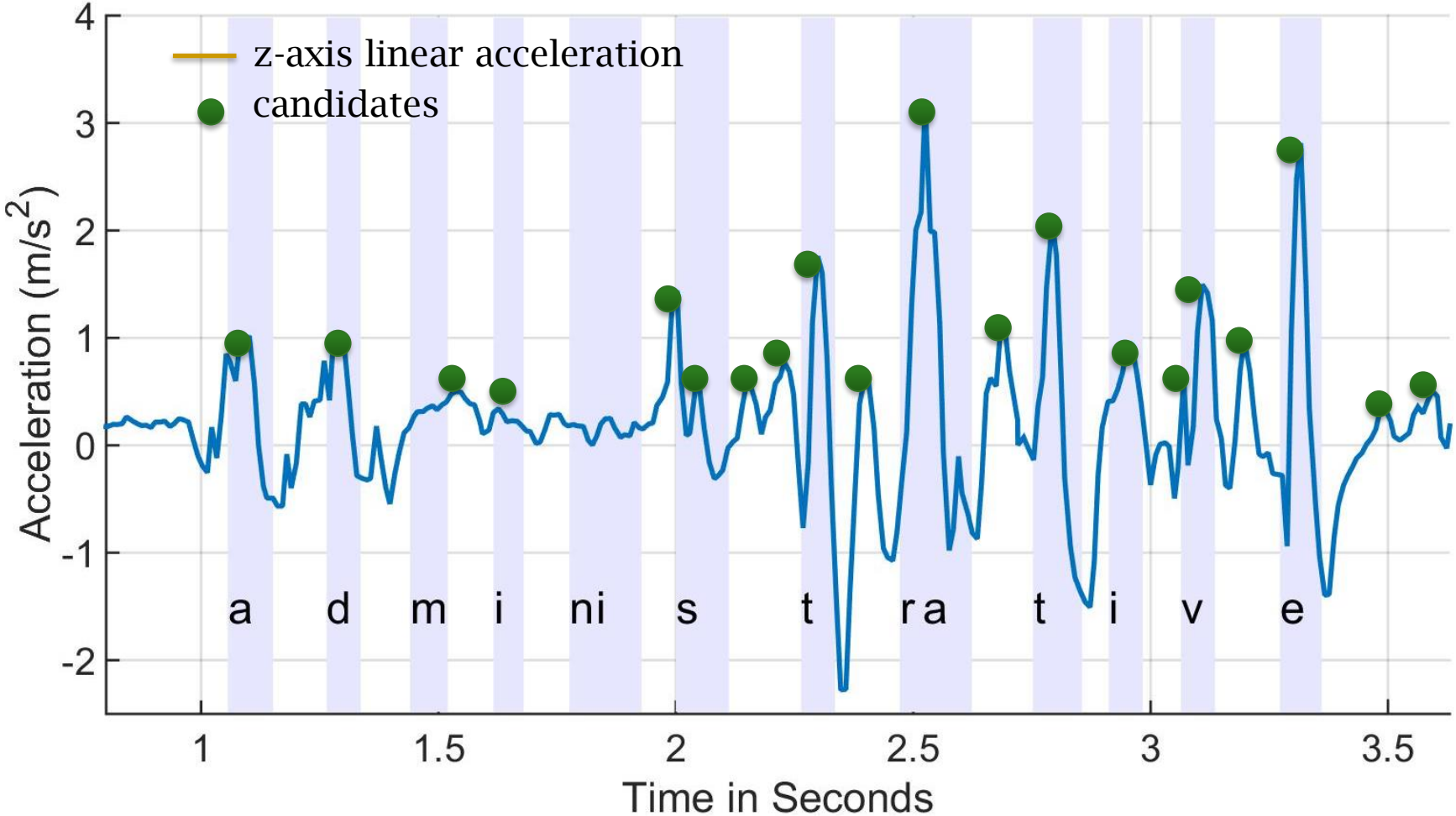
Can we Predict the Typing Behavior from IMU data?

- Let's discuss 3 steps:
  - Find the keystroke time
  - Predict keystroke to character
  - Find the likelihood of the word typed

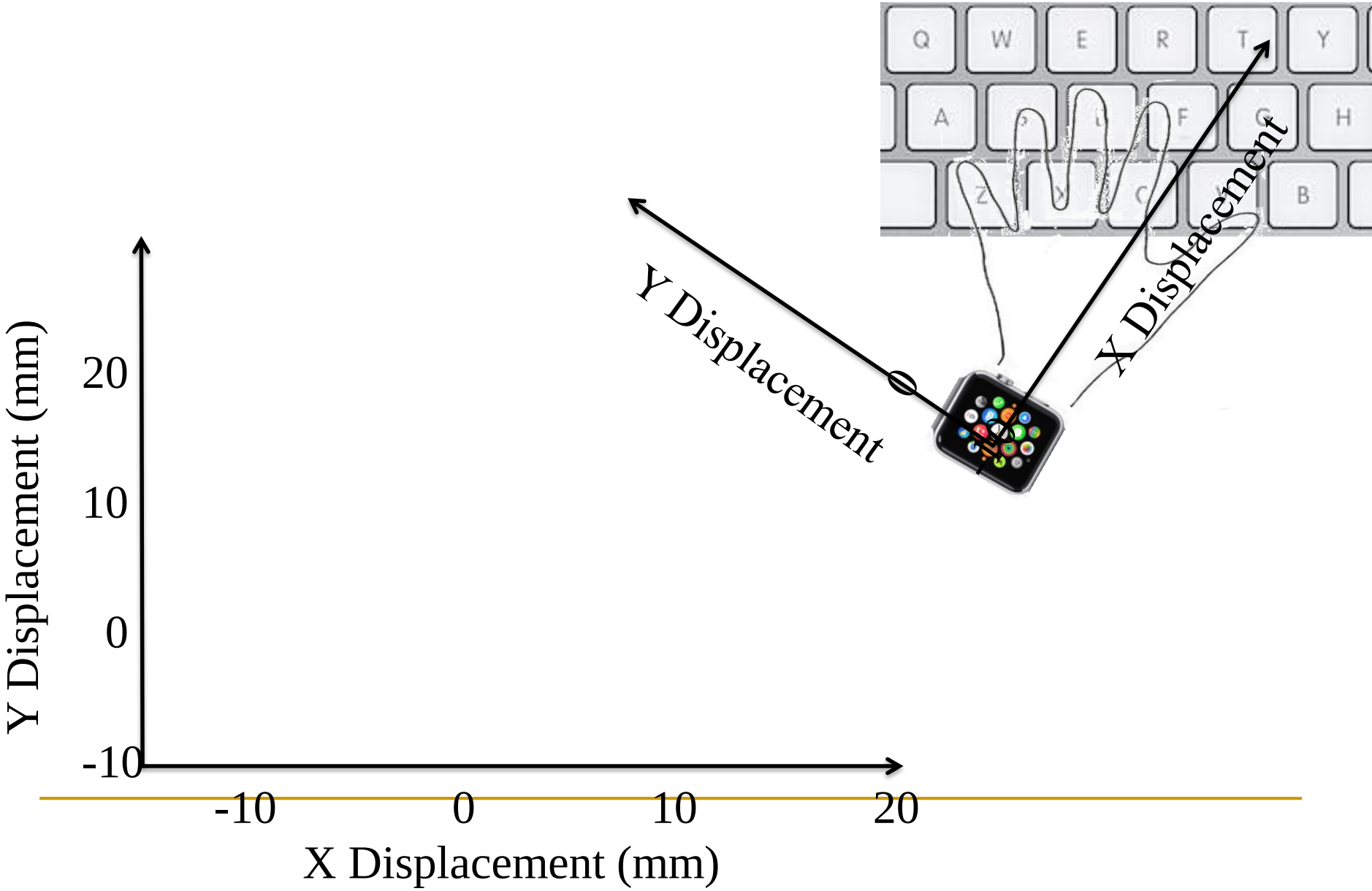


Step1: Detecting the Keystroke Time

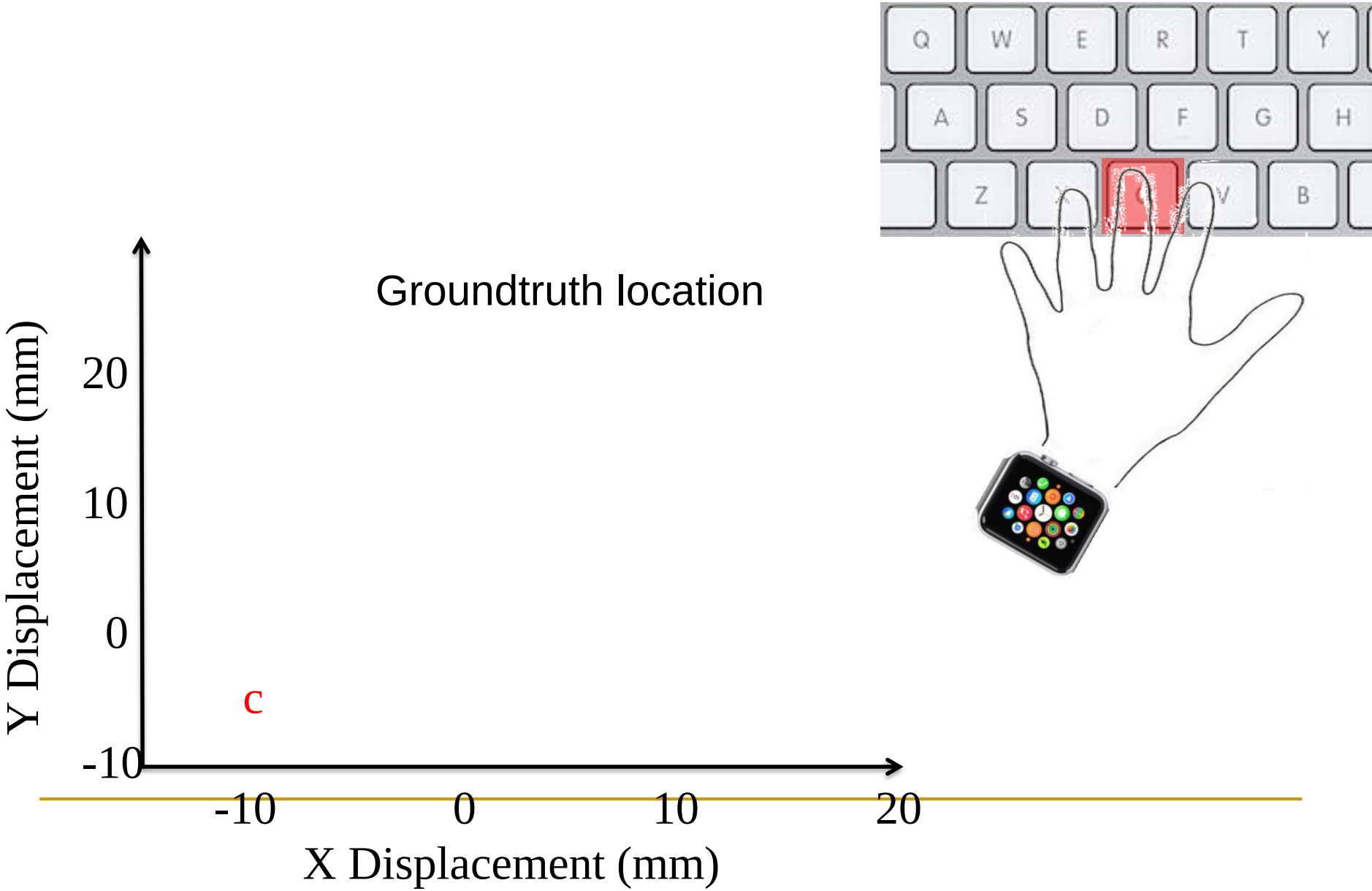
Use z-acceleration to infer keystroke time



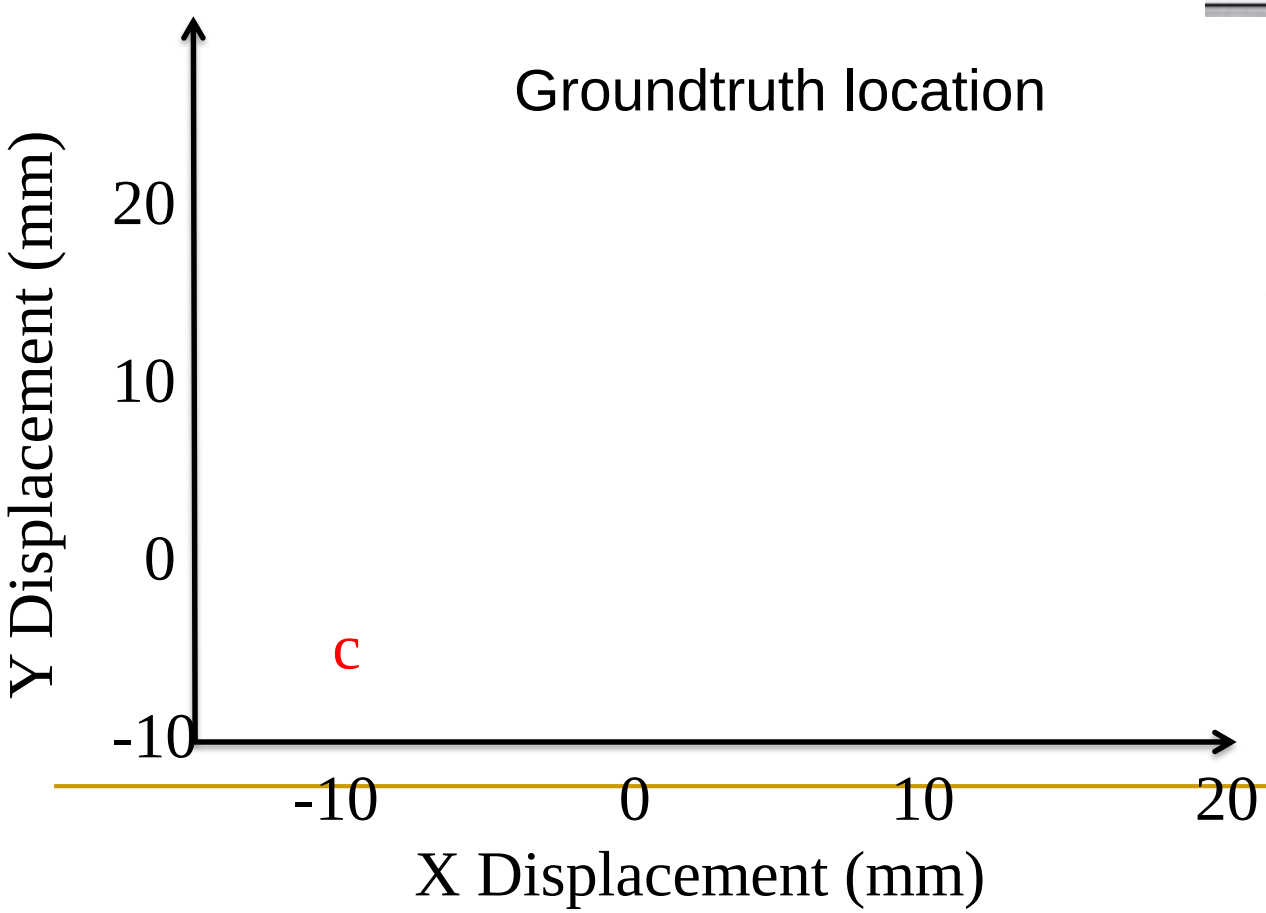
Step2: Predicting the Character



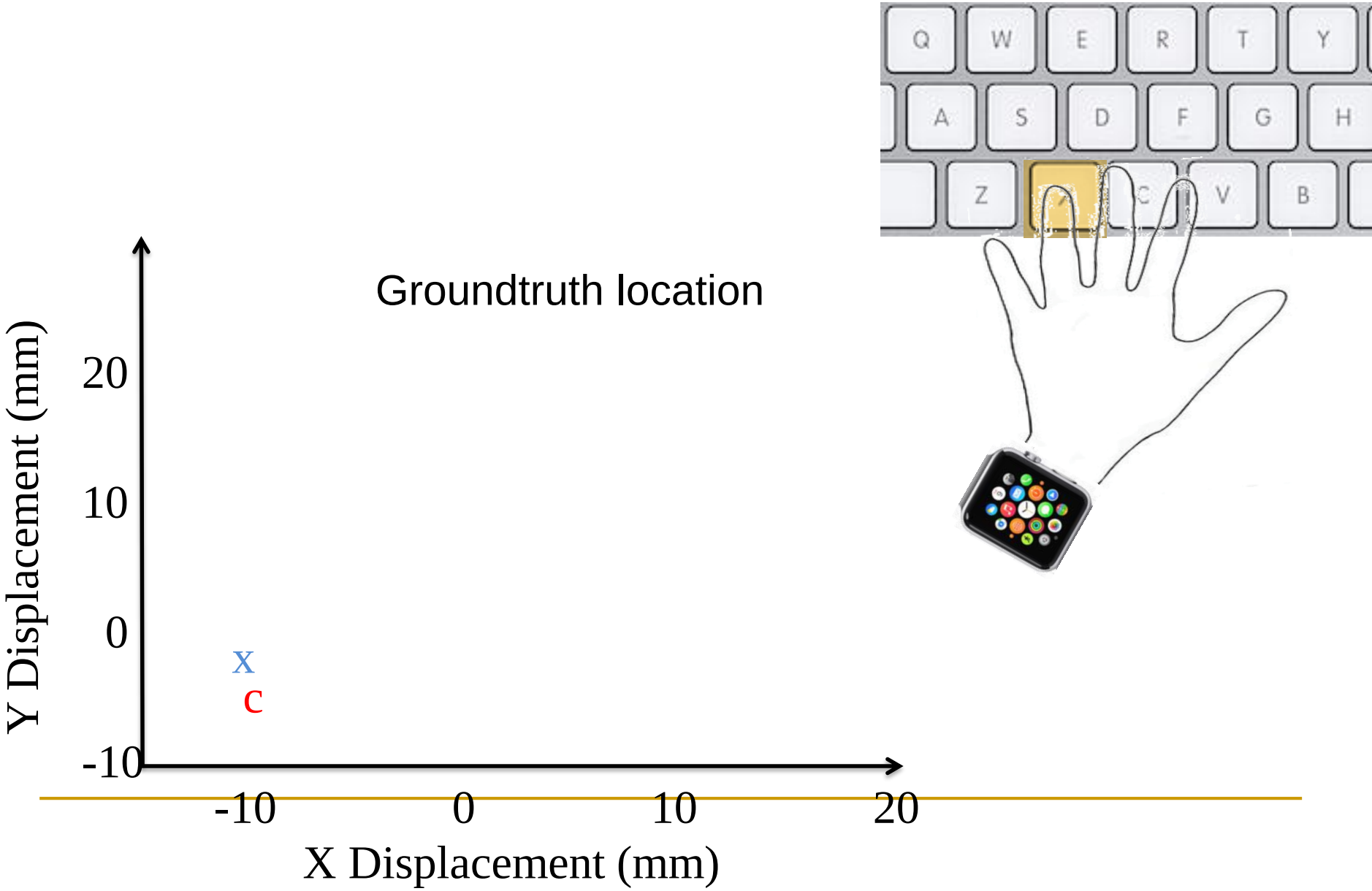
Step2: Predicting the Character



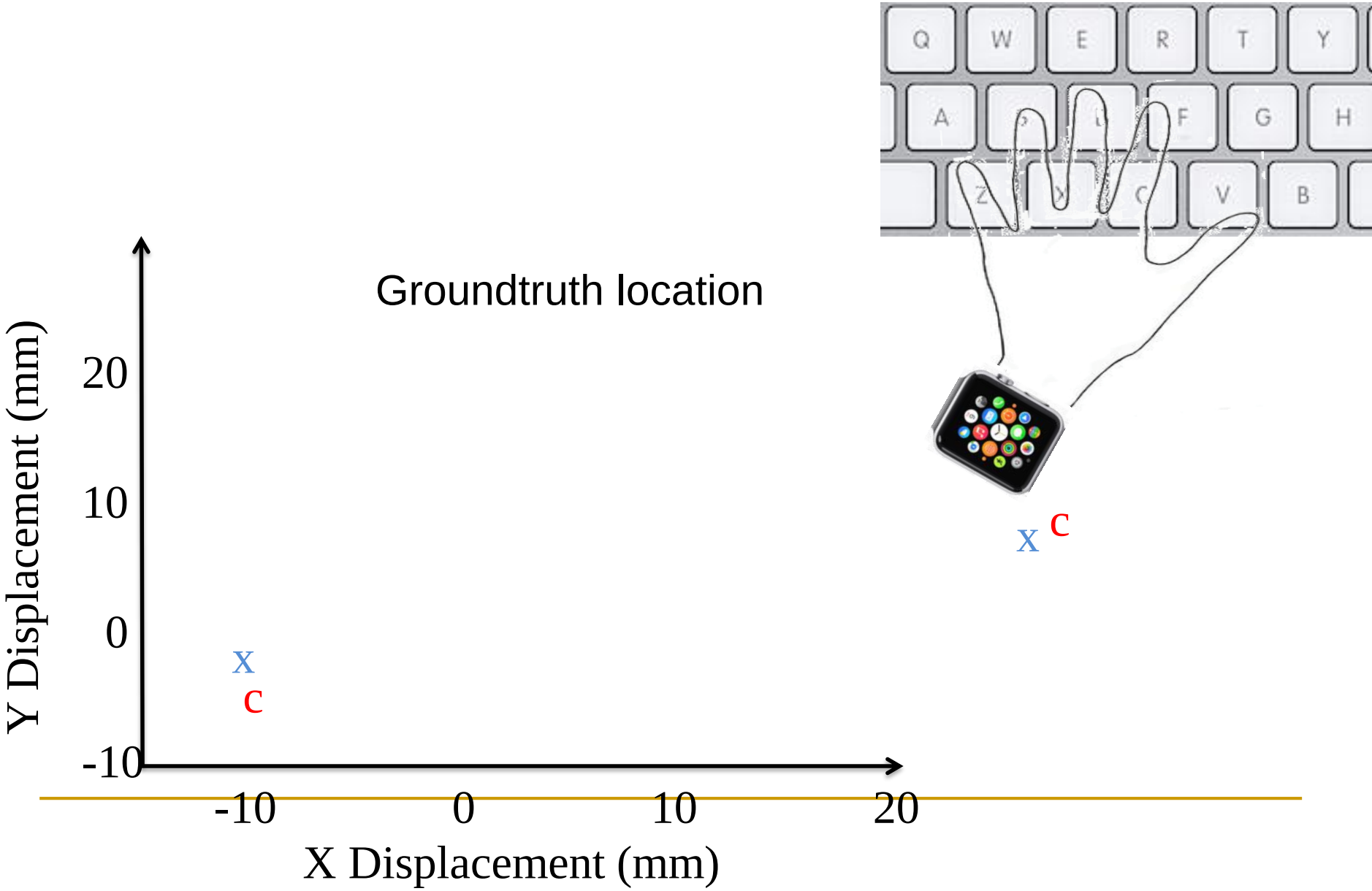
Step2: Predicting the Character



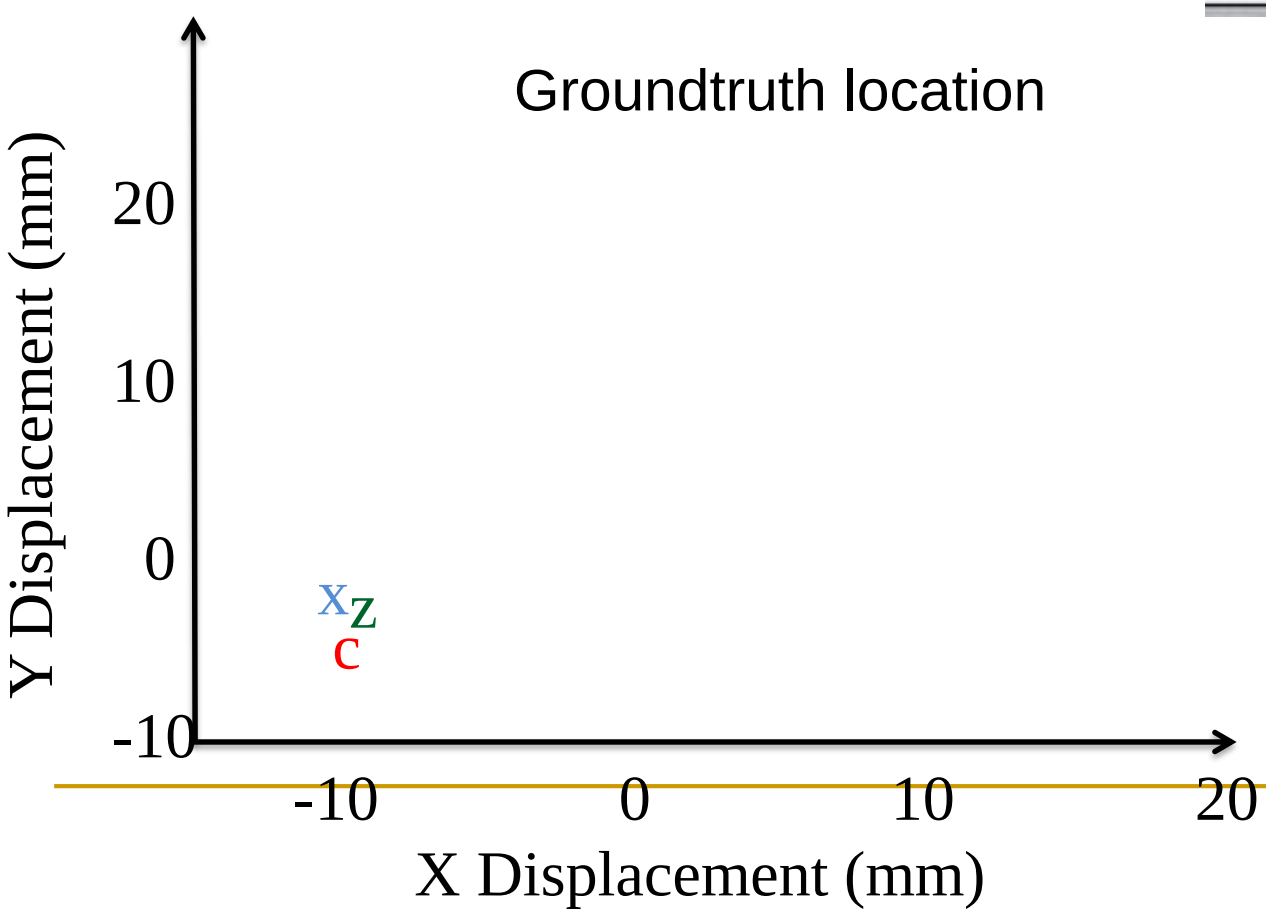
Step2: Predicting the Character



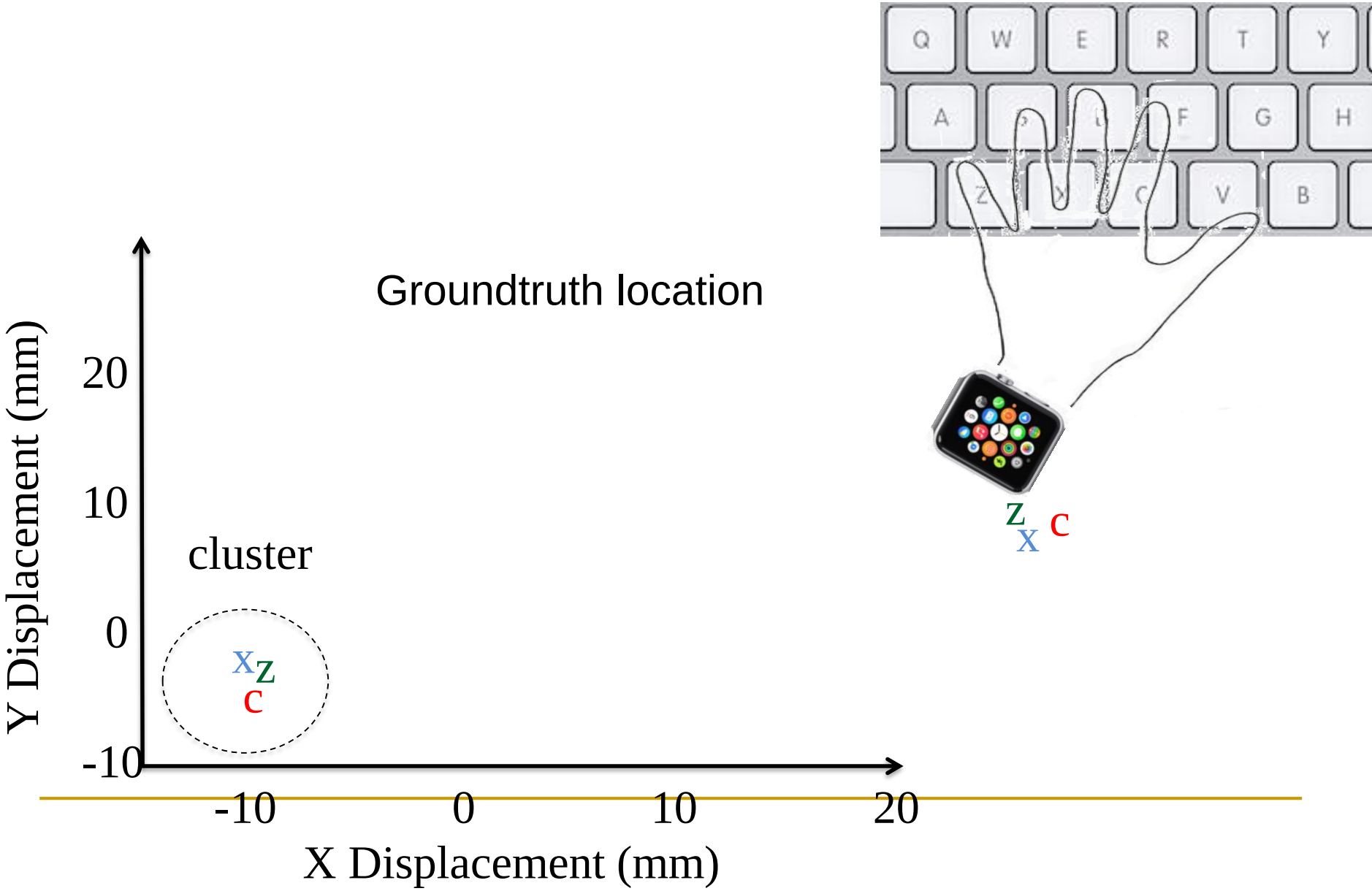
Step2: Predicting the Character



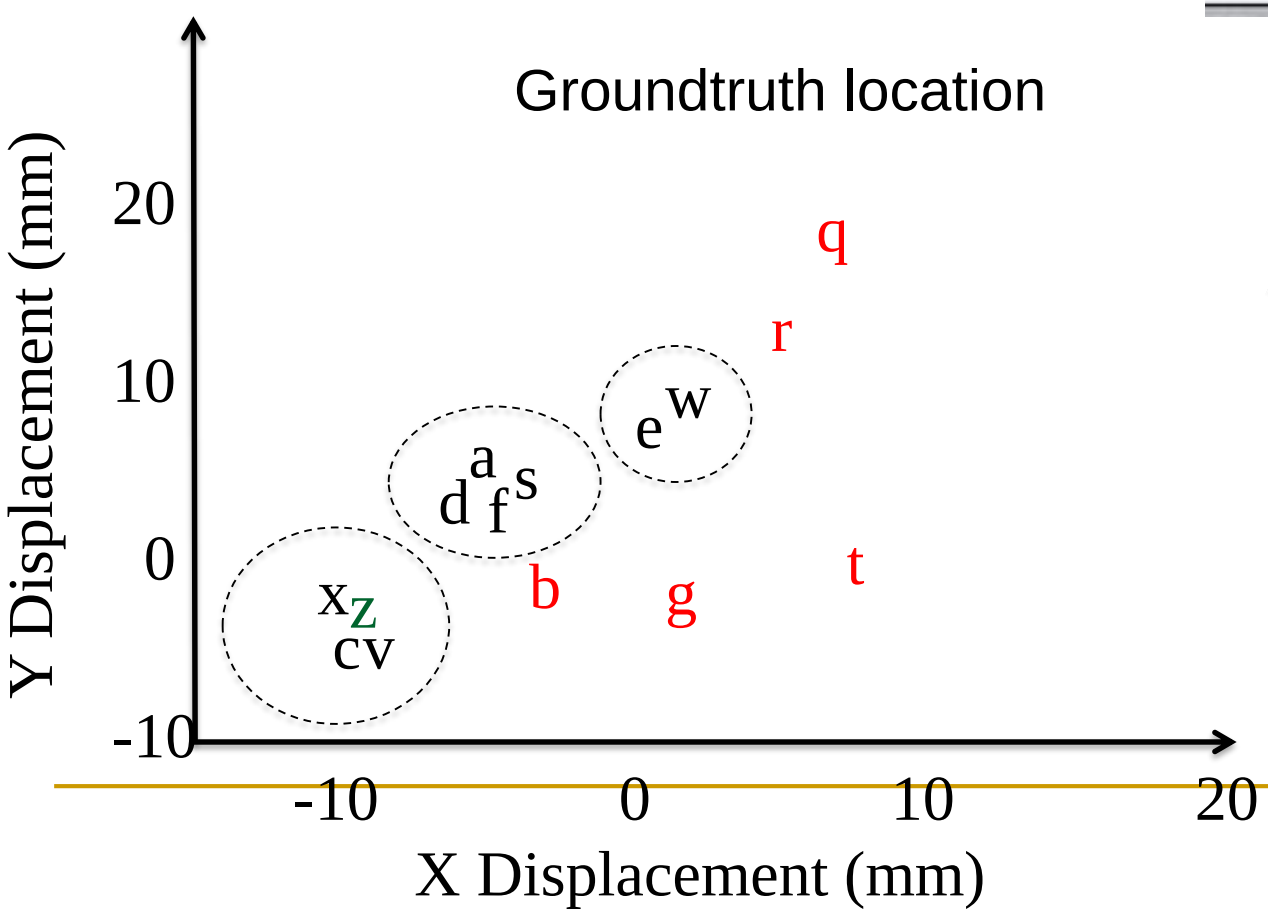
Step2: Predicting the Character



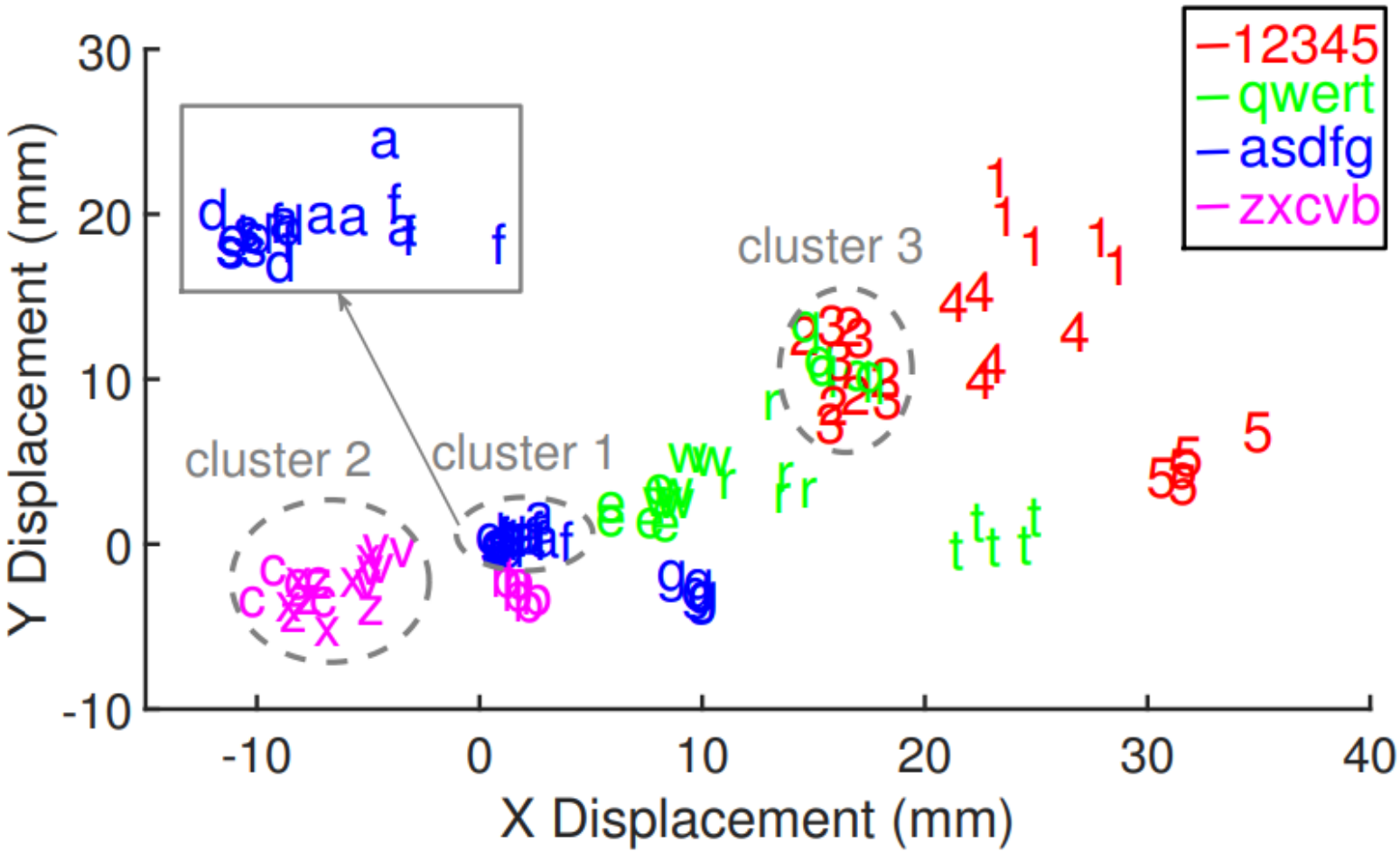
Step2: Predicting the Character



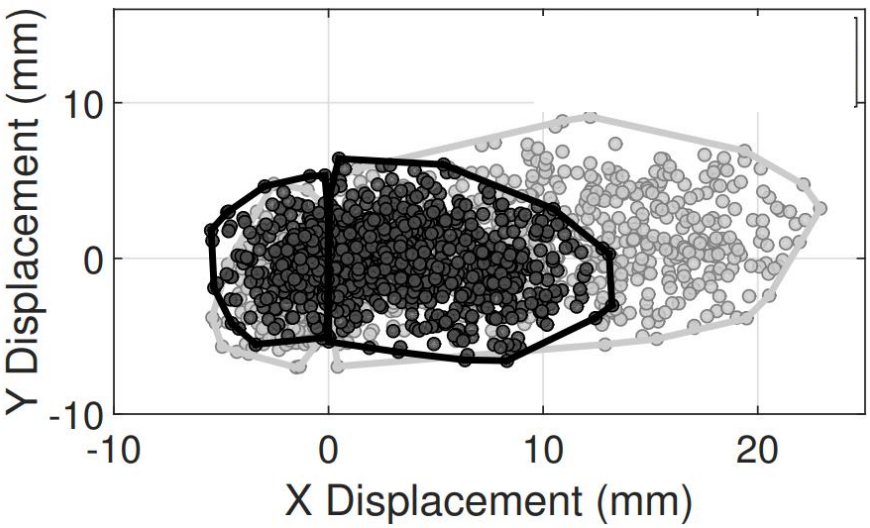
Step2: Predicting the Character

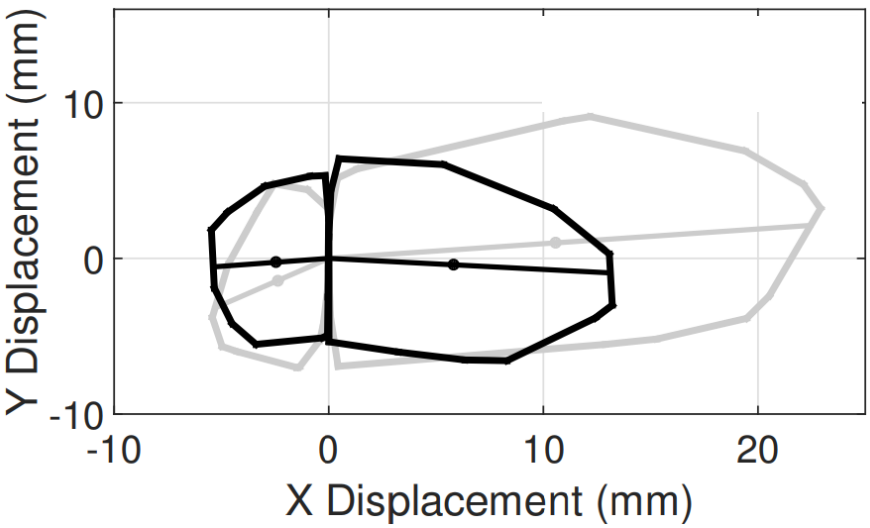


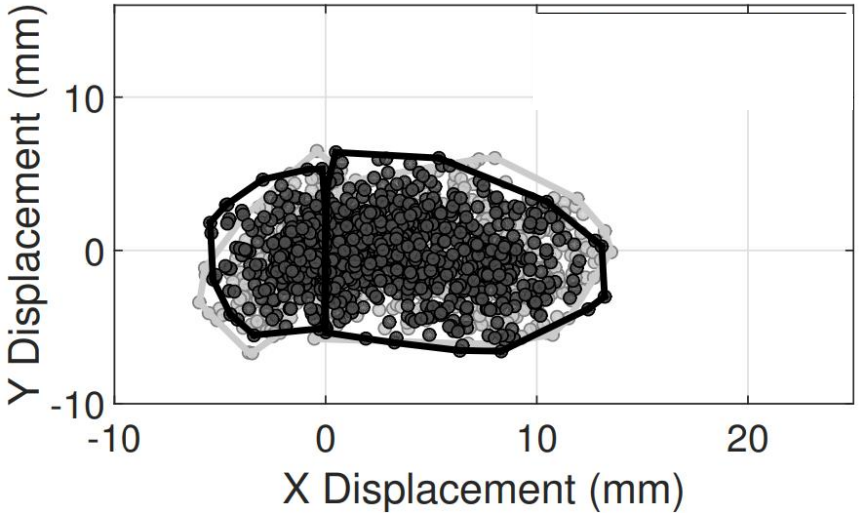
Step2: Predicting the Character



Step2: Predicting the Character

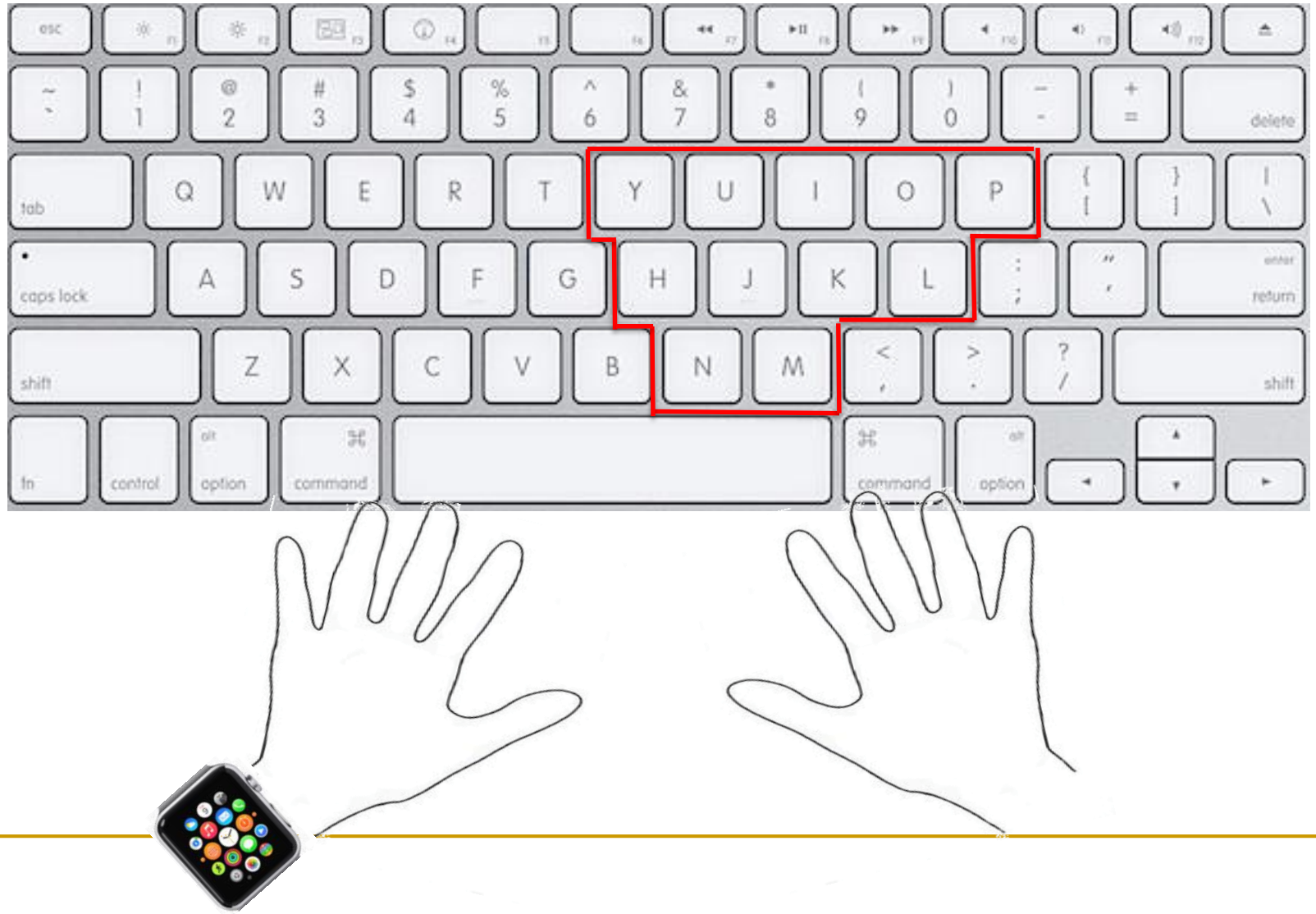






Rotate and scale

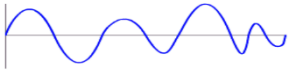
Step3: Predicting the Typed Word



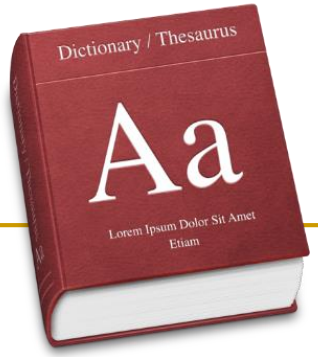
Bayesian Inference

Input "confident"

Observed watch motion



Compute likelihood



$word_1$
$word_2$
$word_3$
…
$word_{4999}$
$word_{5000}$

Output list

Rank	word guess
1	confident
2	consider
3	commander
4999	are
5000	is

Bayesian Inference

$$P(W_i \mid O)$$

prob of observation

- W_i: Candidate word_i in dictionary
- O: Motion observation

Bayesian Inference

word frequency

$$P(W_i \mid O) \propto P(O \mid W_i) \times P(W_i)$$

- W_i: Candidate word_i in dictionary
- O: Motion observation

Bayesian Inference

Likelihood function

$$P(W_i \mid O) \propto \boxed{P(O \mid W_i)} \times P(W_i)$$

- W_i: Candidate word_i in dictionary
- O: Motion observation

Let’s do the Guess Work

Rank	W1	W2	W3	W4	W5	W6	W7	w8
1	motor	pistol	profound	technologies	angel	those	that	disappear
2	monitor	list	journalism	remaining	spray	today	tight	discourse
3	them	but	originally	telephone	super	third	tightly	secondary
4	the	lost	original	meanwhile	fire	through	thirty	adviser
5	then	most	profile	headline	shore	towel	truth	discover

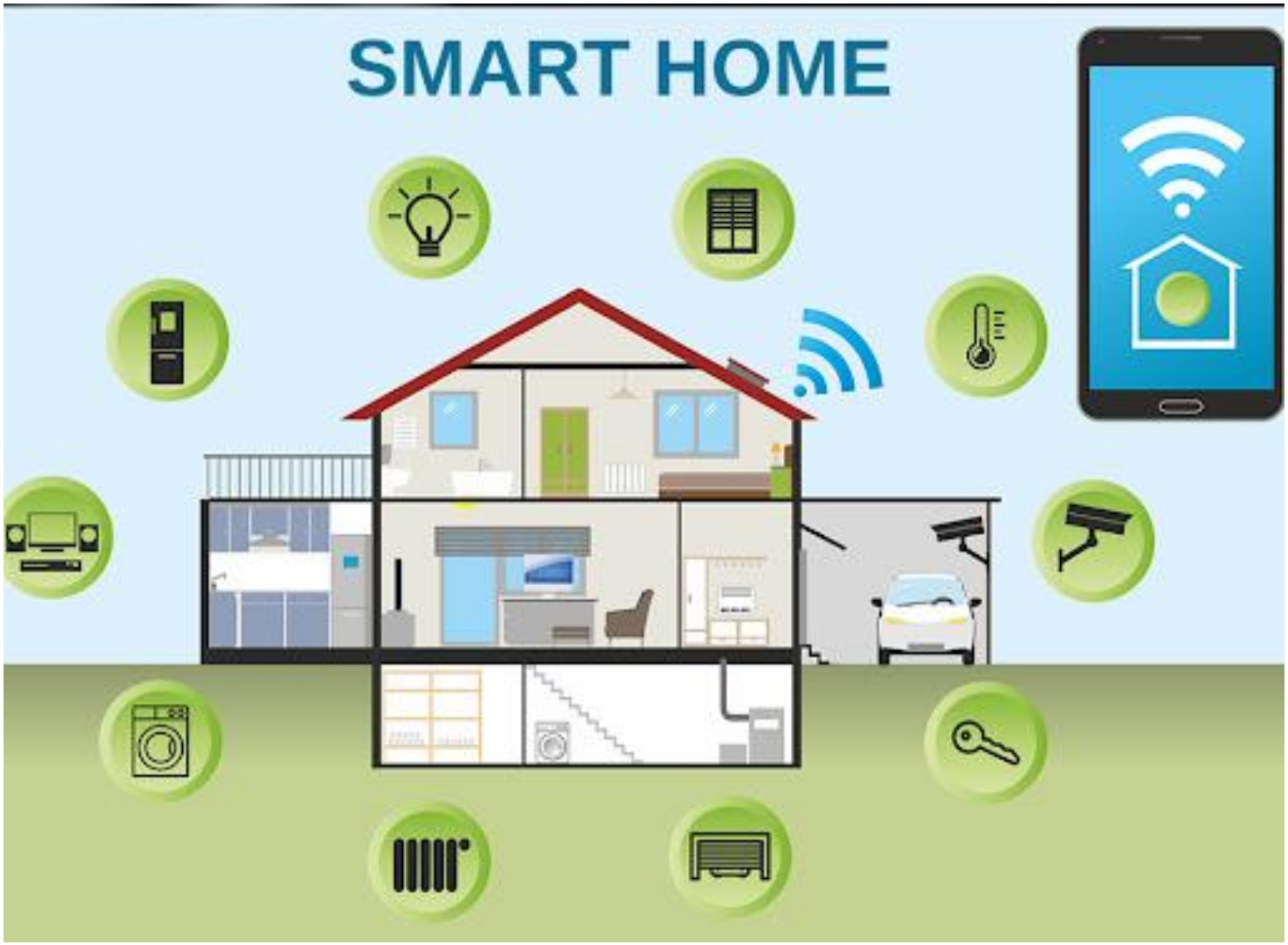
Let’s do the Guess Work

Rank	W1	W2	W3	W4	W5	W6	W7	w8
1	motor	pistol	profound	technologies	angel	those	that	disappear
2	monitor	list	journalism	remaining	spray	today	tight	discourse
3	them	but	originally	telephone	super	third	tightly	secondary
4	the	lost	original	meanwhile	fire	through	thirty	adviser
5	then	most	profile	headline	shore	towel	truth	discover

are

Hacking your Speaker using Inaudible Acoustics

What is Smart Home?

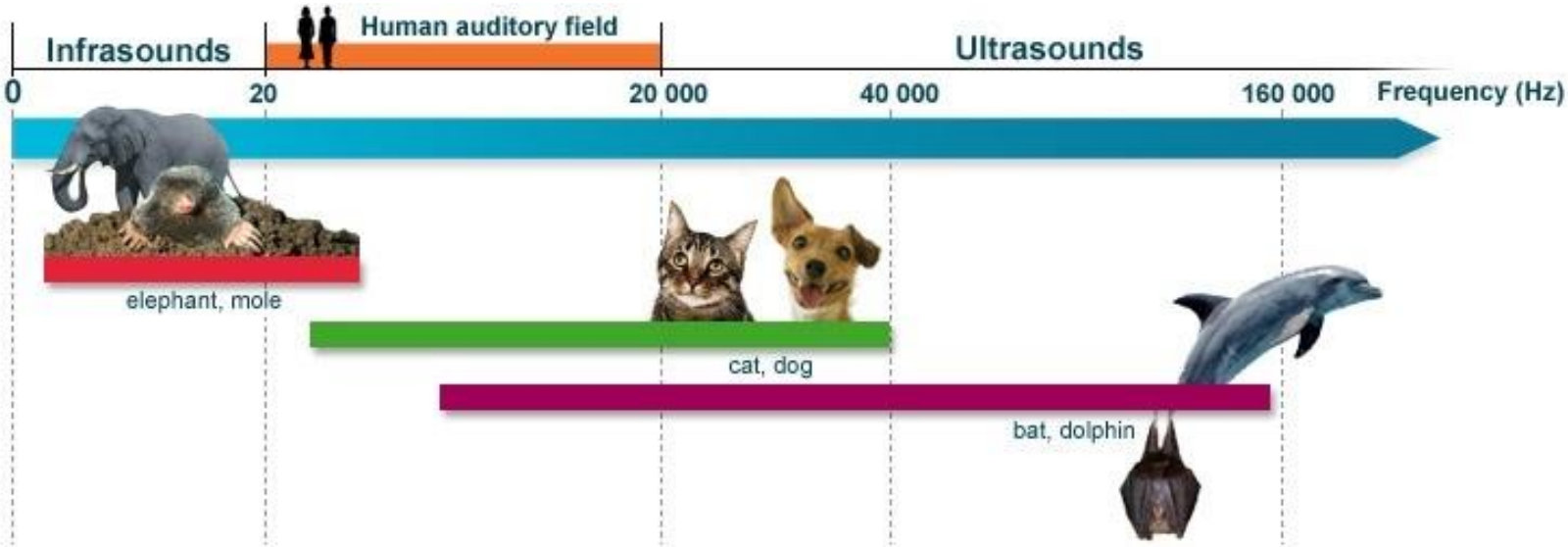


http://www.pert.me/tag/alexa-smart-home-devices/

Inaudible Acoustics

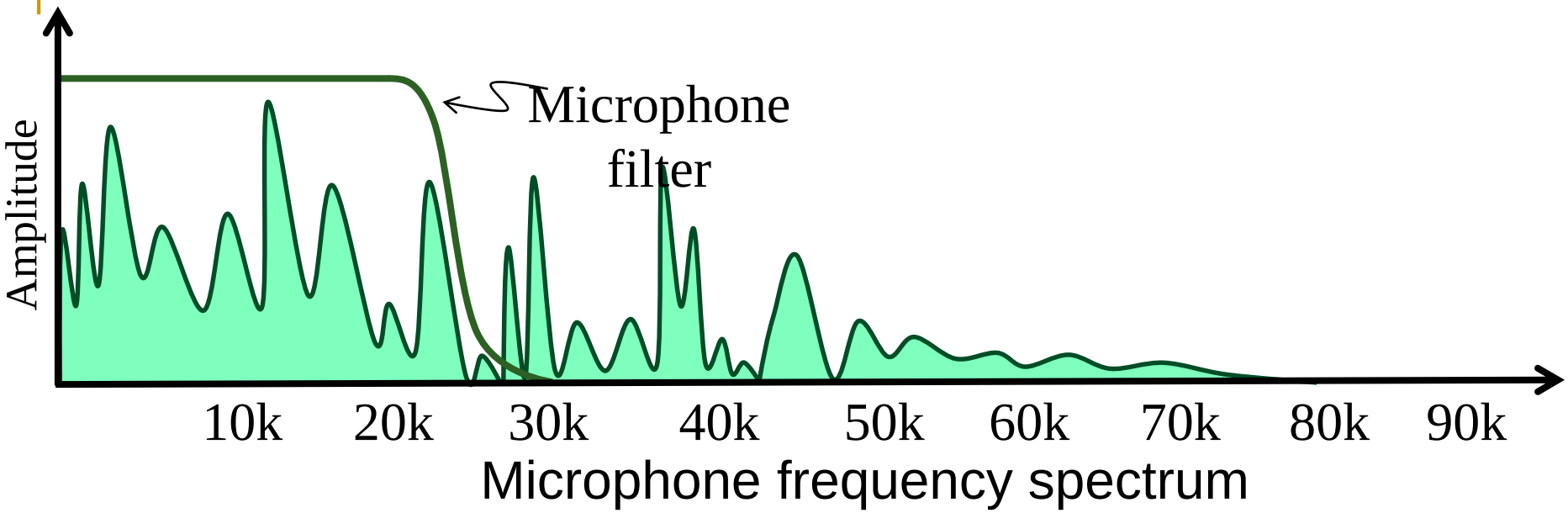
- Audible sound → < 20 kHz range
  - Both human and microphone can hear
- Ultrasound → > 20 kHz range
  - Neither human nor microphone can hear

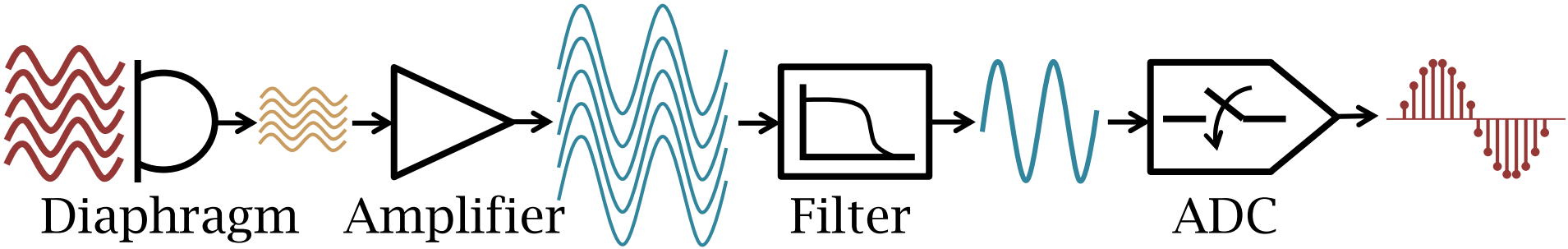
- Can we design a sound that is not heard by human, but can be heard by your microphone?
  - Then we can launch an attack on Alexa, without even notifying the user



https://www.quora.com/Why-cant-we-hear-ultrasonic-and-infrasonic-sound-waves

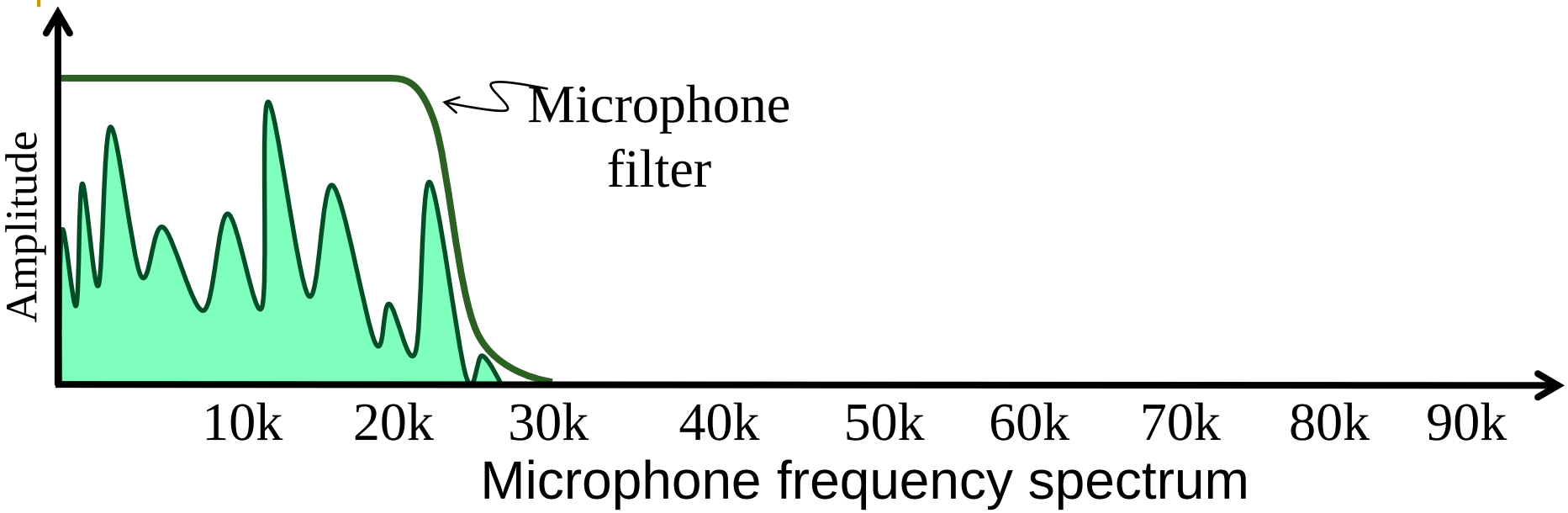
Inside a Microphone

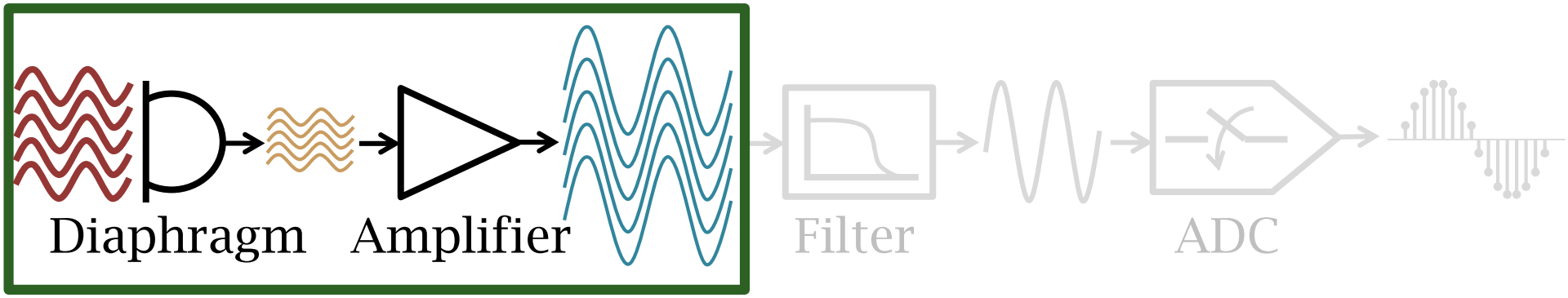




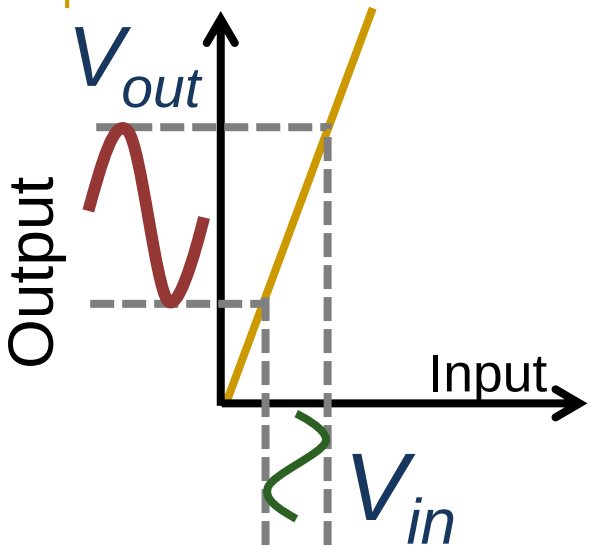
https://courses.grainger.illinois.edu/cs434/sp2021/

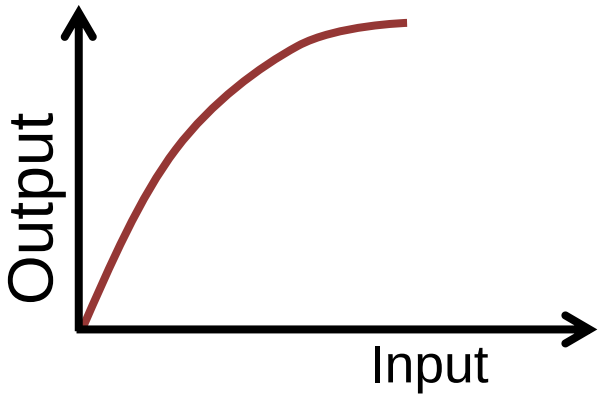
Inside a Microphone





Inside a Microphone

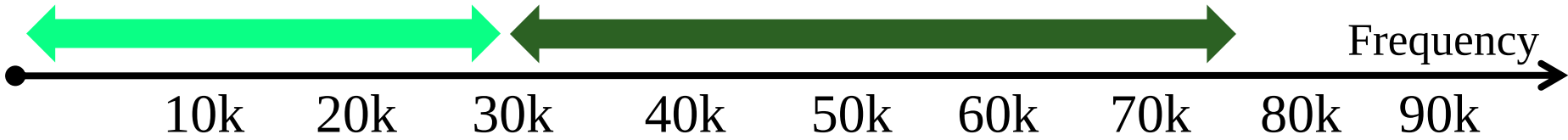


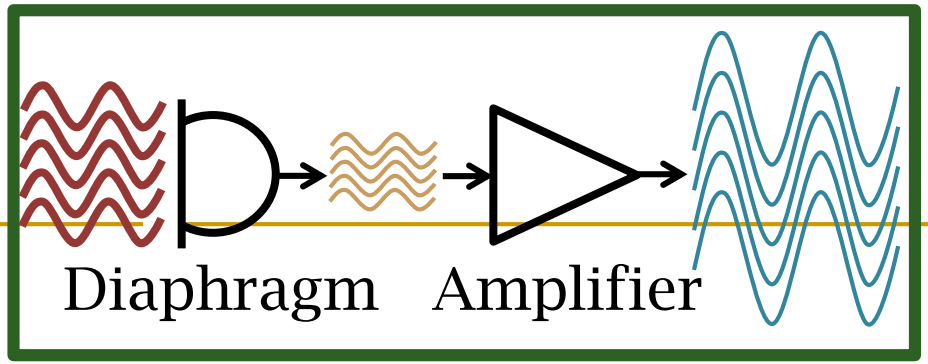


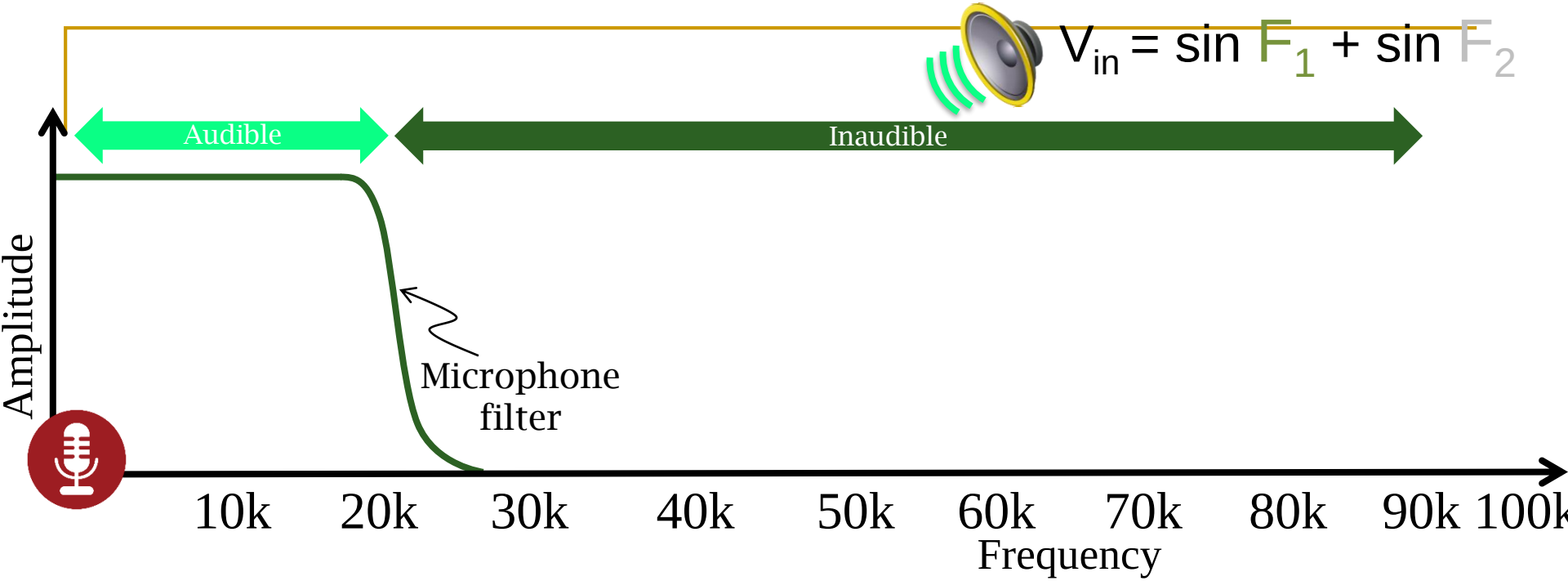
Nonlinear

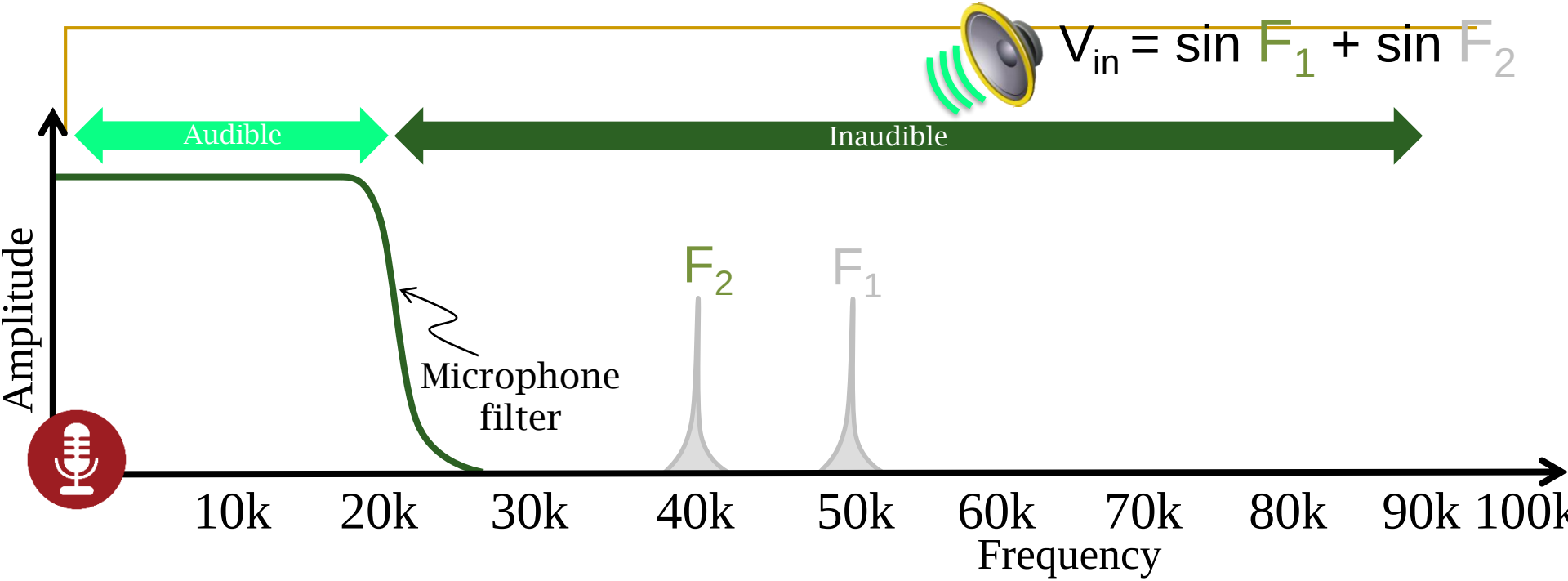
$$V_{out} = a_1 V_{in}$$

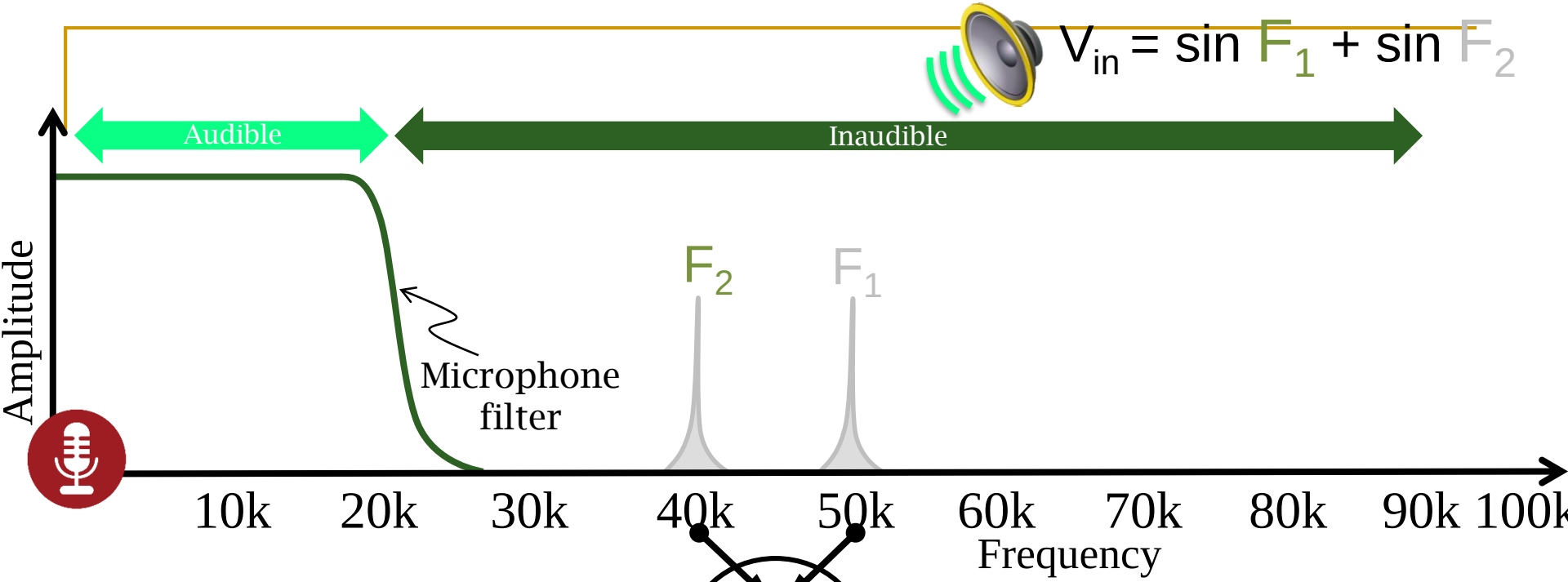
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2 + a_3 V_{in}^3 + \ldots$$






$V_{in} = \sin F_1 + \sin F_2$
Audible
Inaudible
Amplitude
Microphone filter
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency


$V_{in} = \sin F_1 + \sin F_2$
Audible
Inaudible
Amplitude
F_2
F_1
Microphone filter
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency

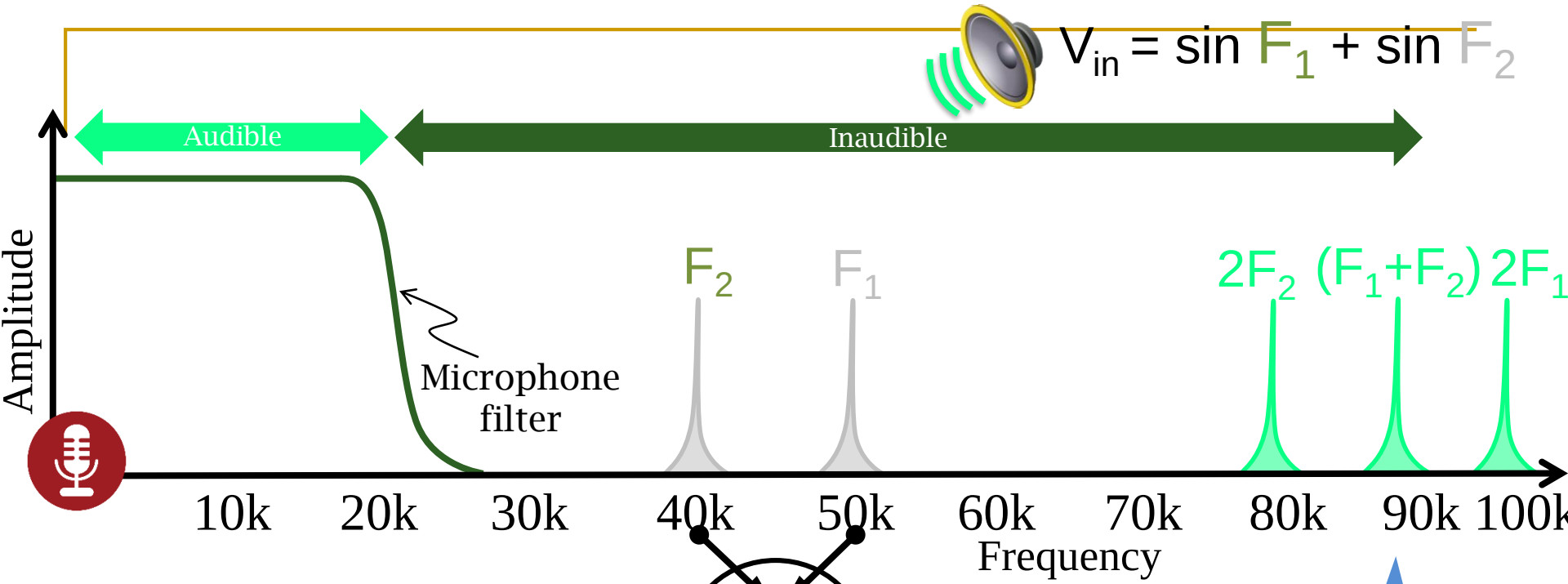


$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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

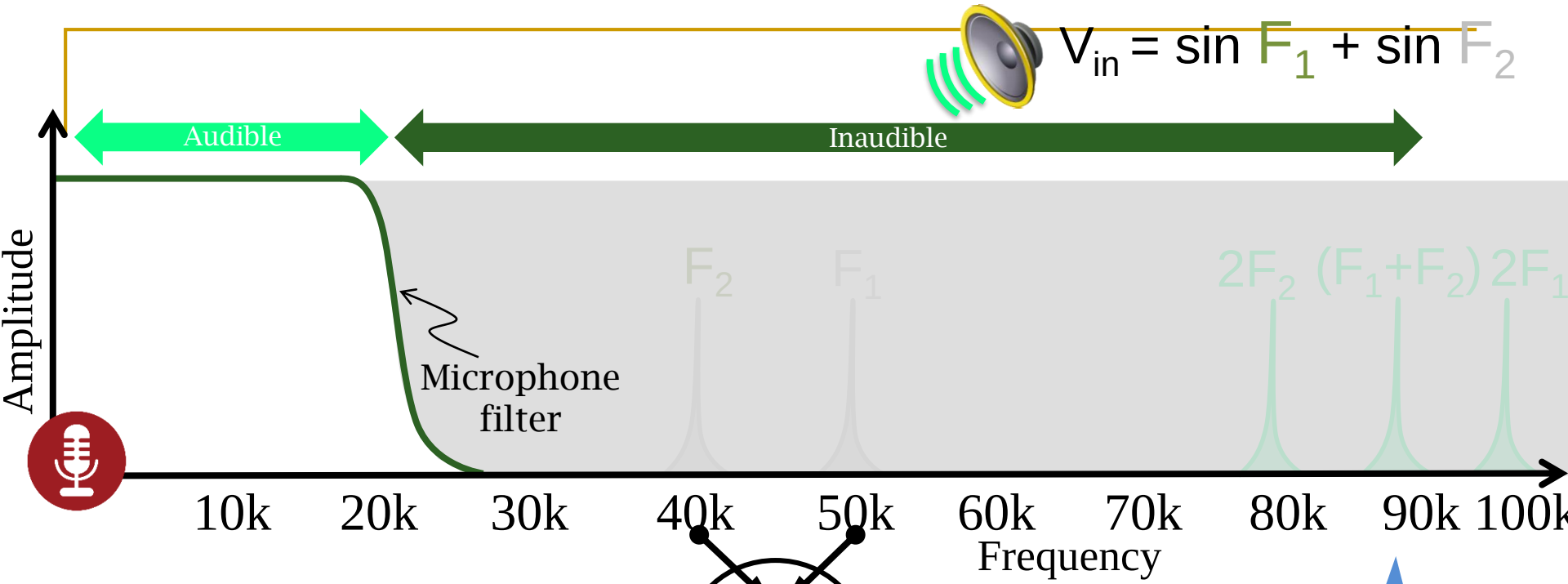
$$\sin^2 x = \frac{1 - \cos 2x}{2}$$

$$\sin A \sin B = \frac{1}{2}[\cos(A-B) - \cos(A+B)]$$



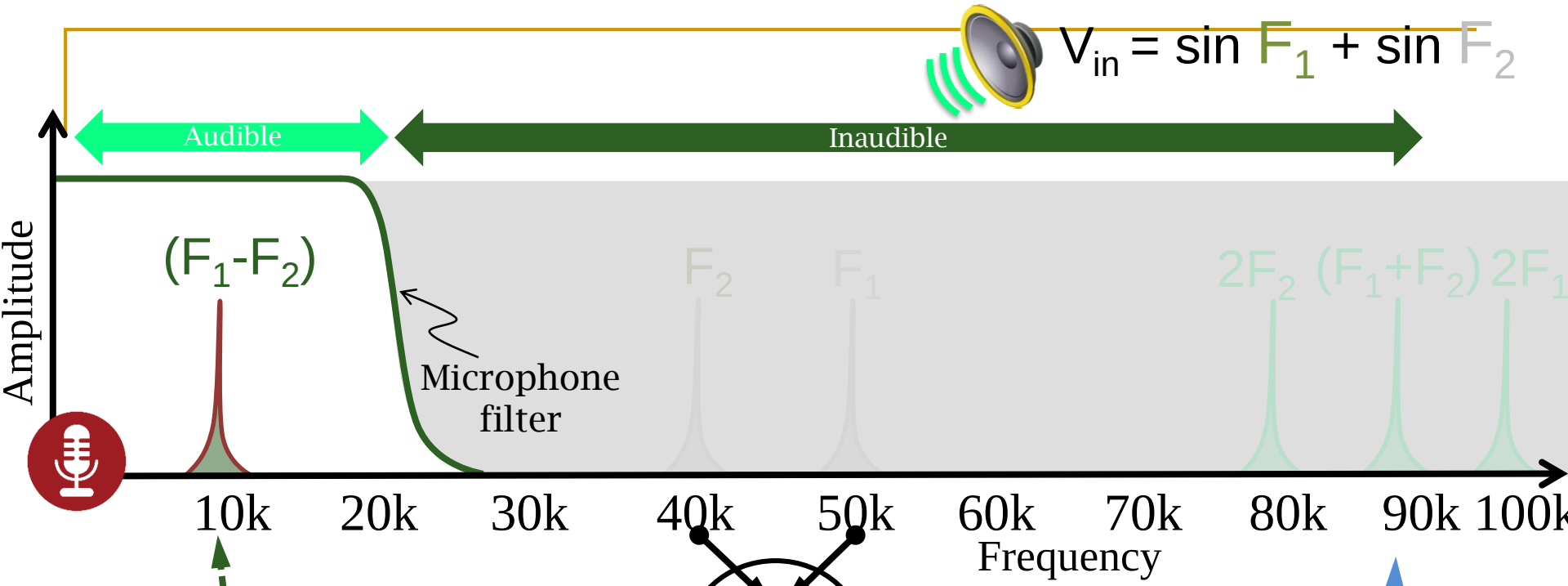
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

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



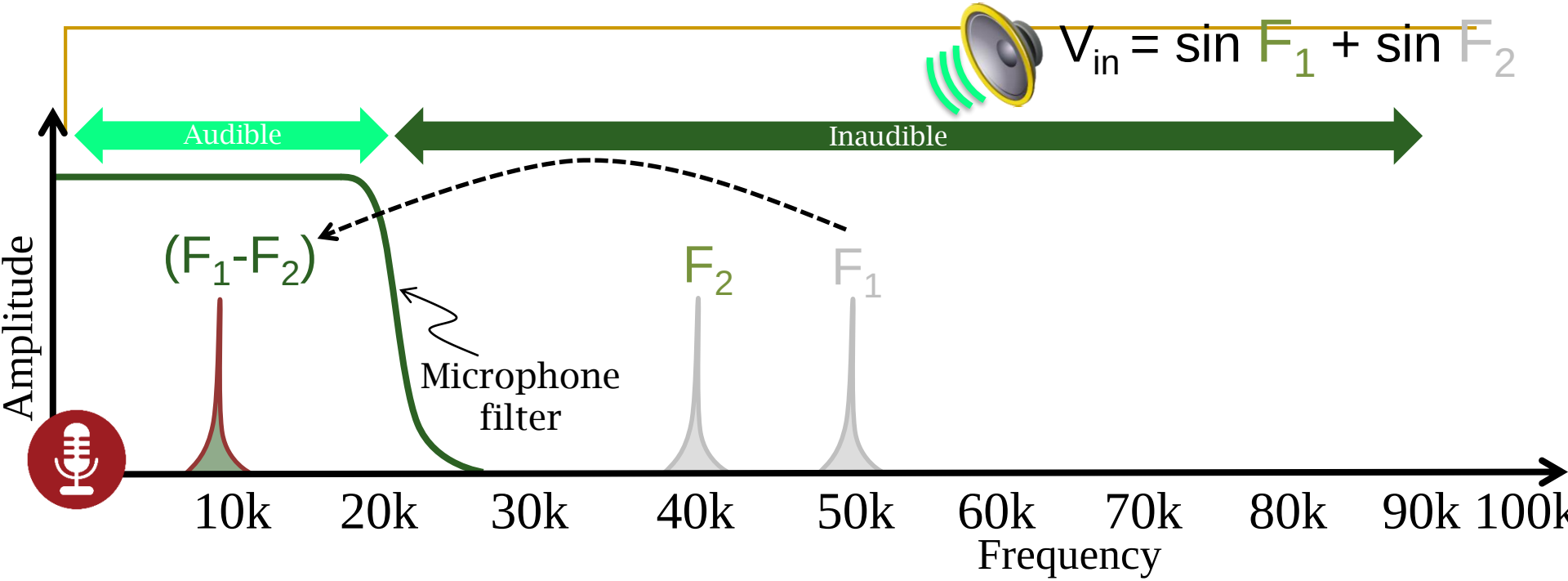
$$V_{out} = a_1 V_{in} + a_2 V_{in}^2$$

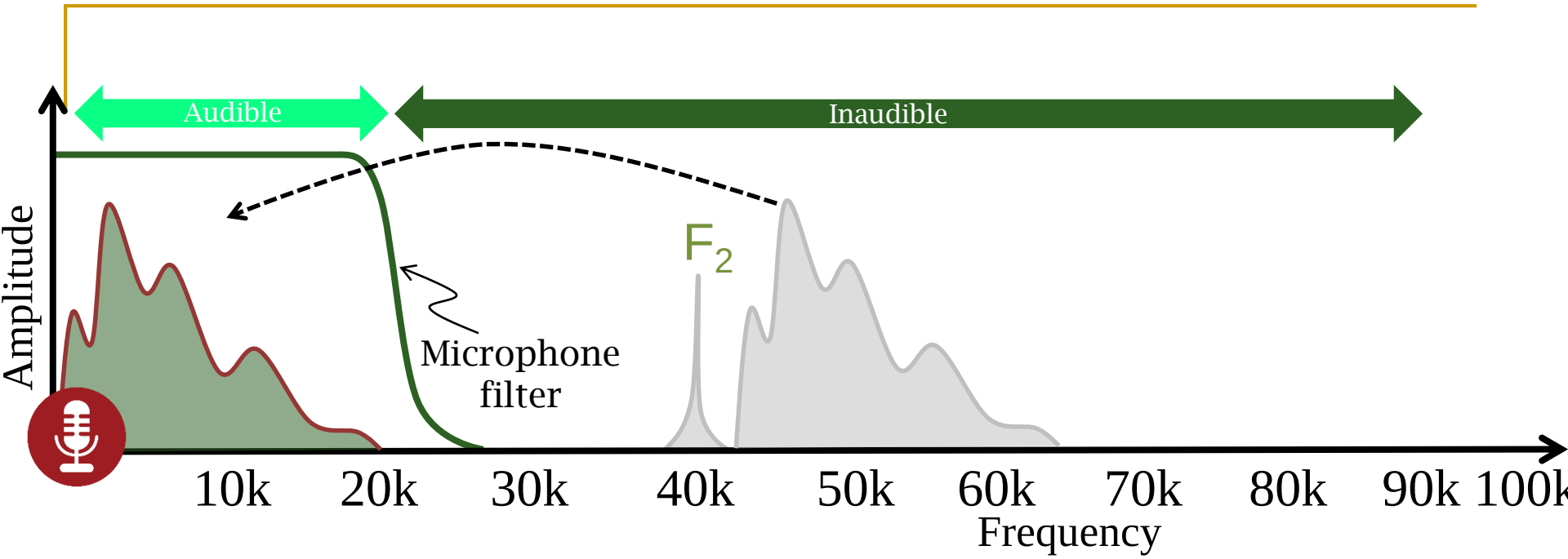
$$(\sin F_1 + \sin F_2)^2 = -\cos 2F_1 - \cos 2F_2 - \cos (F_1+F_2) + \cos (F_1 - F_2)$$



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

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


$V_{in} = \sin F_1 + \sin F_2$
Audible
Inaudible
Amplitude
(F_1-F_2)
F_2
F_1
Microphone filter
10k
20k
30k
40k
50k
60k
70k
80k
90k
100k
Frequency



We can take any signal → modulate it with F_1 and can launch the attack