



[HTTPS://CONFERENCE.HITB.ORG/HITBSECCONF2024BKK](https://conference.hitb.org/hitbseccconf2024bkk)

Silencing Spies: Revealing Microphone Nonlinear Behavior and Building an Ultrasonic Jammer

Hetian Shi

NISL LAB, Tsinghua University



29 AUG

#HITB2024BKK

■ About me

- Hetian Shi

- Researcher, NISL Lab, Tsinghua University
- Specializing in Hardware and IoT Security with a focus on uncovering physical layer vulnerabilities in IoT devices. Achievements include multiple vulnerability disclosures and winning prestigious competitions such as the Tianfu Cup 2021 and GeekPwn, GeekCon in 2022 & 2023.

#HITB2024BKK



Agenda

- Research background and related news
- Deep Dive into TSCM: Defense to Microphone Eavesdropping
- Our Ultrasonic Jamming Device
 - Effective Solutions for Handling Various Workplace Challenges
 - Ethical Considerations
 - Takeaways

Research Background and Related News

#HITB2024BKK



目前，饶河县公安局已抓获犯罪嫌疑人14人，扣押违法所得60万余元，查明组织架构7级，查获非法生产工厂1个，窃听窃照专用器材销售点7处，储存仓库4个，缴获窃听窃照专用器材成品5万余个，用于制造器材的光成品及配件51万余件，总价值四千万



民警在黑龙江省饶河县一体育馆内清点缴获的窃听窃照器材。（饶河县公安局供图）



\$ 8000 illegal gains







gettyimages®

Credit: Jacobs Stock Photography
Ltd

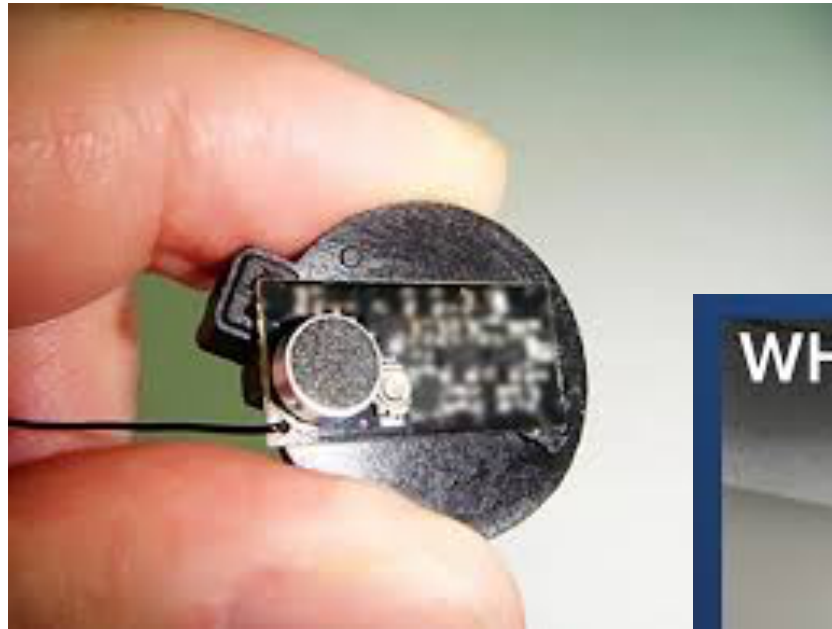
劉青雲 古天樂 吳卓熾 張靜初 方中信 王敏德 陳偉霆



Background

- With the advent of the information society, protecting sensitive information of individuals and organizations has become crucial. Eavesdropping threats can lead to the leakage of vital national security information, business secrets or personal privacy.
 - National Security
 - Corporate Competition
 - Personal Privacy
- Given the complexity of eavesdropping technology and the severity of the threats, adopting effective **preventive measures** becomes paramount. Encrypted communication, **physical security measures**, and network security strategies are all essential means to counter eavesdropping threats.

Miniature Eavesdropping Devices





【CCTV展播品牌】随身录音笔神器

¥98.91 折后价 1万+人看过

先用后付 新品 赠运费险 淘工厂 包邮

源头好货 限时放价



录音笔专业高清降噪上课用学生

无操作系统 录音功能 锂电池
操作系统 附加功能 电池规格

¥137 300+人付款

直降11元 领券满99减10 先用后付

jnn维罗纳专卖店 进店>



录音笔随身录音神器专业高清降噪设备可以语音转文字超长待机

智能操作系统 录音功能 锂电池
附加功能 附加功能 电池规格

¥123 券后价 2万+人付款

领券满100减5 先用后付 赠运费险 包邮

本月上新3件 卡丁猫数码旗舰店>



自动高清降噪录音笔声控监听神器

支持GPS功能 录音功能 锂电池
附加功能 附加功能 电池规格

¥238 券后价 400+人付款

领券满198减20 包邮

易创数码科技店 进店>



新款录音笔随身神器挂环式转文字

无操作系统 录音功能 锂电池
操作系统 附加功能 电池规格

¥107 4000+人付款

直降11元 领券满99减10 先用后付

jnn维罗纳专卖店 进店>



3.6cm 长度 3.6cm 宽度 1.1cm 宽度

智能声控录音

有声音即录，无声音自动暂停，提高工作效率，节省电量和内存

反馈

顶部

Intelligent Audio Record Function

Deceptive Shape Eavesdropping Devices



Fabby 12 Pack Voice Recorder for Stuffed Animal 30 Seconds Push Button Sound Recorder Heart Shaped Recordable Button Voice Recording Button Box Device for Plush Toy Bear...

★★★★☆ < 10

100+ bought in past month

\$49.99

Ages: 6 years and up

Delivery Thu, Dec 28

Ships to Singapore

Only 14 left in stock - order soon.



Recordable Talking Button with Keychain, 20s Voice Recording Time Sound Button Answer Buzzers Funny Buttons Record Your Own Words Also Used for Dog Pack of 2 - White and...

\$19.99

Delivery Thu, Dec 28

Ships to Singapore

Only 1 left in stock - order soon.



64GB Digital Voice Recorder with Playback - Keychain Voice Activated Recorder Audio Recording Device - 760 Hours Capacity for Lectures Meetings Music

★★★★☆ < 7

100+ bought in past month

\$49.99

List: \$59.99

Save 10% with coupon

Delivery Thu, Dec 28

Ships to Singapore

Background

- Eavesdropping technology has undergone significant development over the past few decades. From the initial simple listening devices to today's advanced electronic and network eavesdropping, the technology in this field continues to evolve.
- With the digitization of communication and information, eavesdropping technology has become more secretive and sophisticated. The processing of digital signals eliminates the need to capture sound clearly for eavesdropping.
- The diversification of eavesdropping threats has become one of the challenges faced by contemporary society. It includes not only traditional physical eavesdropping devices but also network-based electronic eavesdropping and information gathering on social media.



Attack technology optimization



Increased Defense Difficulty



Diversification of Threats

How to start ?

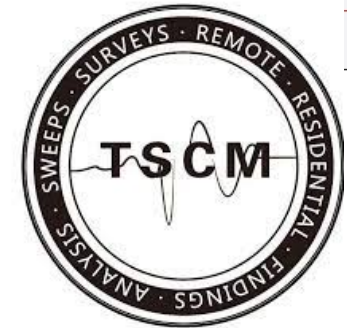
- Literature Review, Data Exploration, and Procurement of Eavesdropping & Anti-Eavesdropping Devices
 - Understand Eavesdropping and Anti-Eavesdropping devices.
- Selection of A Specific Direction Among Diverse Counter-Surveillance Technologies and Devices
 - Choose a specific direction from the list of counter-surveillance technologies and devices available. This selection serves as the focus for in-depth exploration and analysis.
 - Offer our own design, including Software & Hardware, to address specific workplace challenges.
- Analysis Using Matlab or Python, Conducting Experiments and Comparative Assessment
 - Utilize Matlab or Python for systematic analysis and conduct experiments to validate our approach.
 - Compare our unique advantages with those of current commercial devices

Deep Dive into TSCM: Defense to Microphone Eavesdropping

#HITB2024BKK



Technical Surveillance Counter-Measures (TSCM)



Counter-surveillance Technology:

- Employing various approaches, such as physical inspections, electronic reconnaissance, and information security reviews to ensure that national institutions, businesses, and individuals are protected from eavesdropping and surveillance threats.
- The aim is to detect and eliminate various eavesdropping threats.

Key Points of TSCM:

1. **Physical Inspection:** Conducting thorough examinations of buildings, equipment, and communication systems to identify potential eavesdropping devices.
2. **Electronic Reconnaissance:** Using specialized equipment to detect wireless and wired eavesdropping devices by scanning the radio frequency spectrum.
3. **Information Security Review:** Examining communication systems, networks, and information flows to safeguard sensitive information.
4. **Training and Awareness Enhancement:** Providing training on eavesdropping threats to enhance security awareness.

TSCM - Advanced Eavesdropping Device Detection Equipments

Utilizing Diverse Physical Media



Electromagnetic
Wave



Infrared Light



RF Signal

TSCM — Eavesdrop-proofing Devices via Ultrasonic Wave



\$ 2249



\$
239



\$
1145



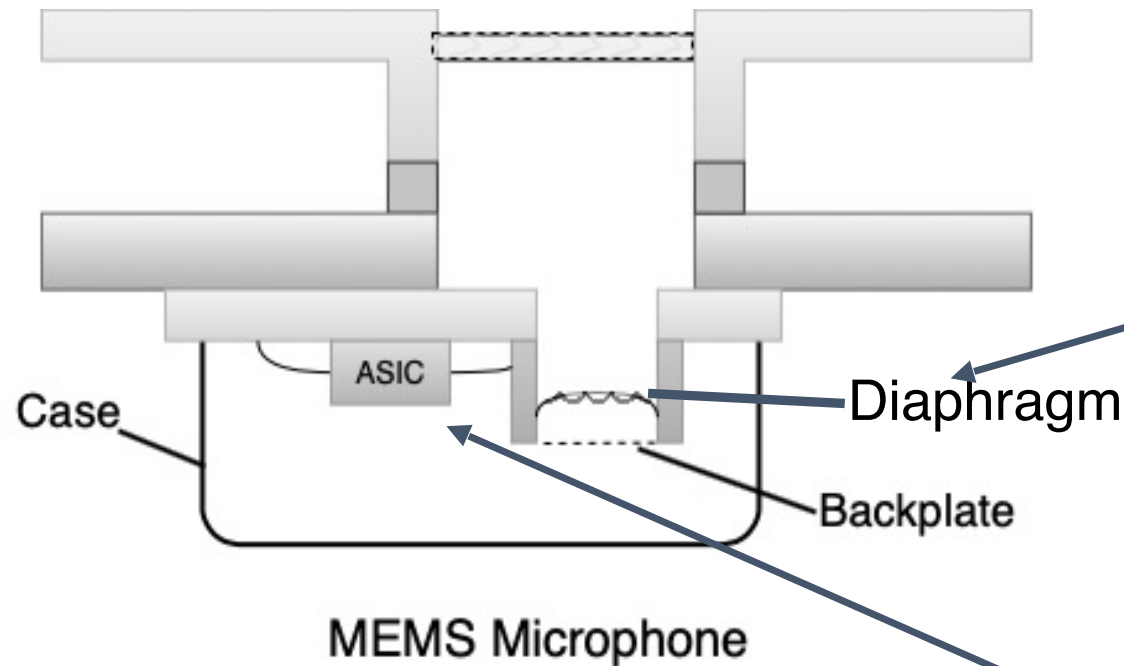
¥
1288

Introduction of Ultrasonic Jamming Technology

- Operating Principle:
 - Utilizing ultrasonic frequency sound waves (greater than 20,000Hz) to disrupt and confuse the receiving systems of microphones or eavesdropping devices, thereby thwarting eavesdropping attempts.
- Applications:
 - Commercial Spaces: Used to prevent eavesdropping on business negotiations and confidential meetings.
 - Government Institutions: In government and military settings, ultrasonic interference technology can be employed to protect sensitive information.
- Key Application Scenarios:
 - Meeting Rooms, One-on-One Conversation Offices
- Advantages:
 - No need for physical dismantling of devices, enabling discreet eavesdropping interference.

#HITB2024BKK

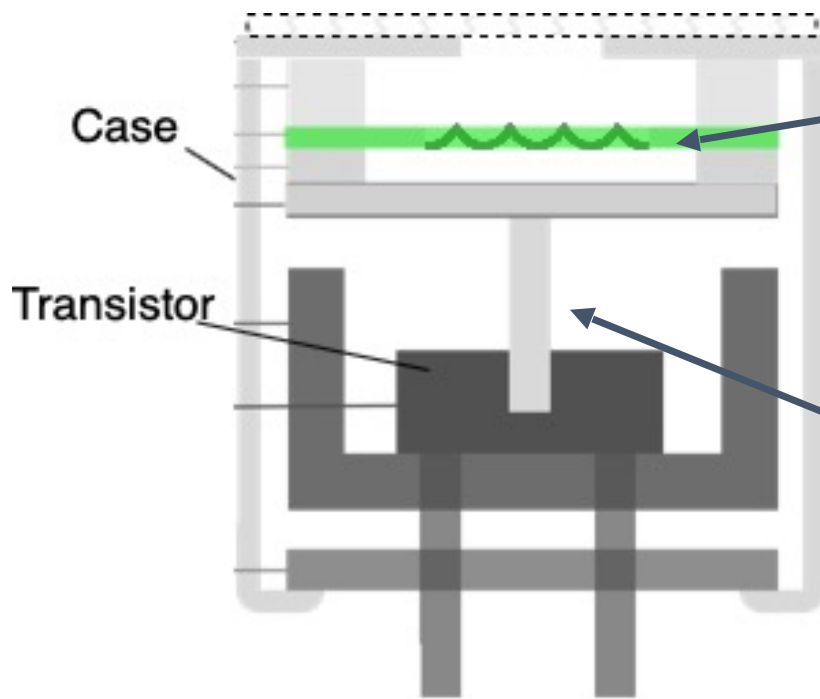
Delve into analysis structure of three common types of microphone



- Sound hits the diaphragm, causing the distance between the diaphragm and backplate to change.

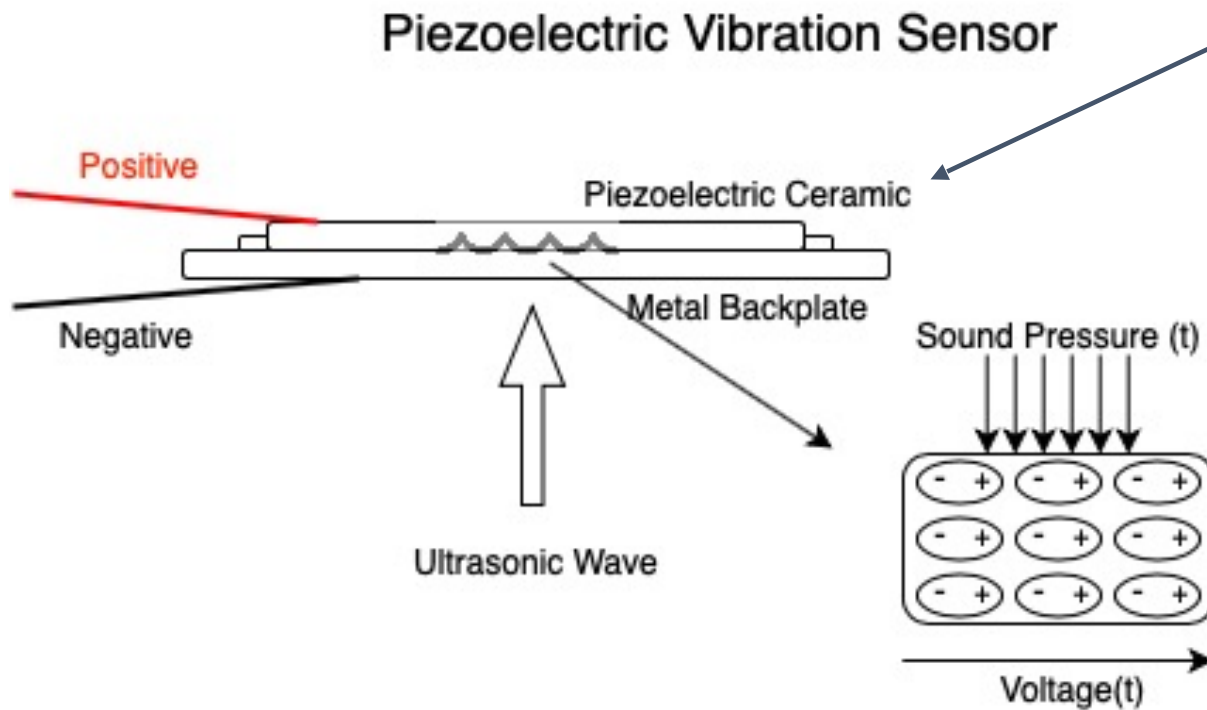
- ASIC provides a fixed voltage to the backplate, then converts vibrations into electrical signals.

Electret Condenser Microphone (ECM)



- Sound waves induce vibrations in the diaphragm, resulting in changes in capacitance and the generation of electrical signals.
- The diaphragm is permanently charged with a fixed charge (Q).

Piezoelectric Ceramic



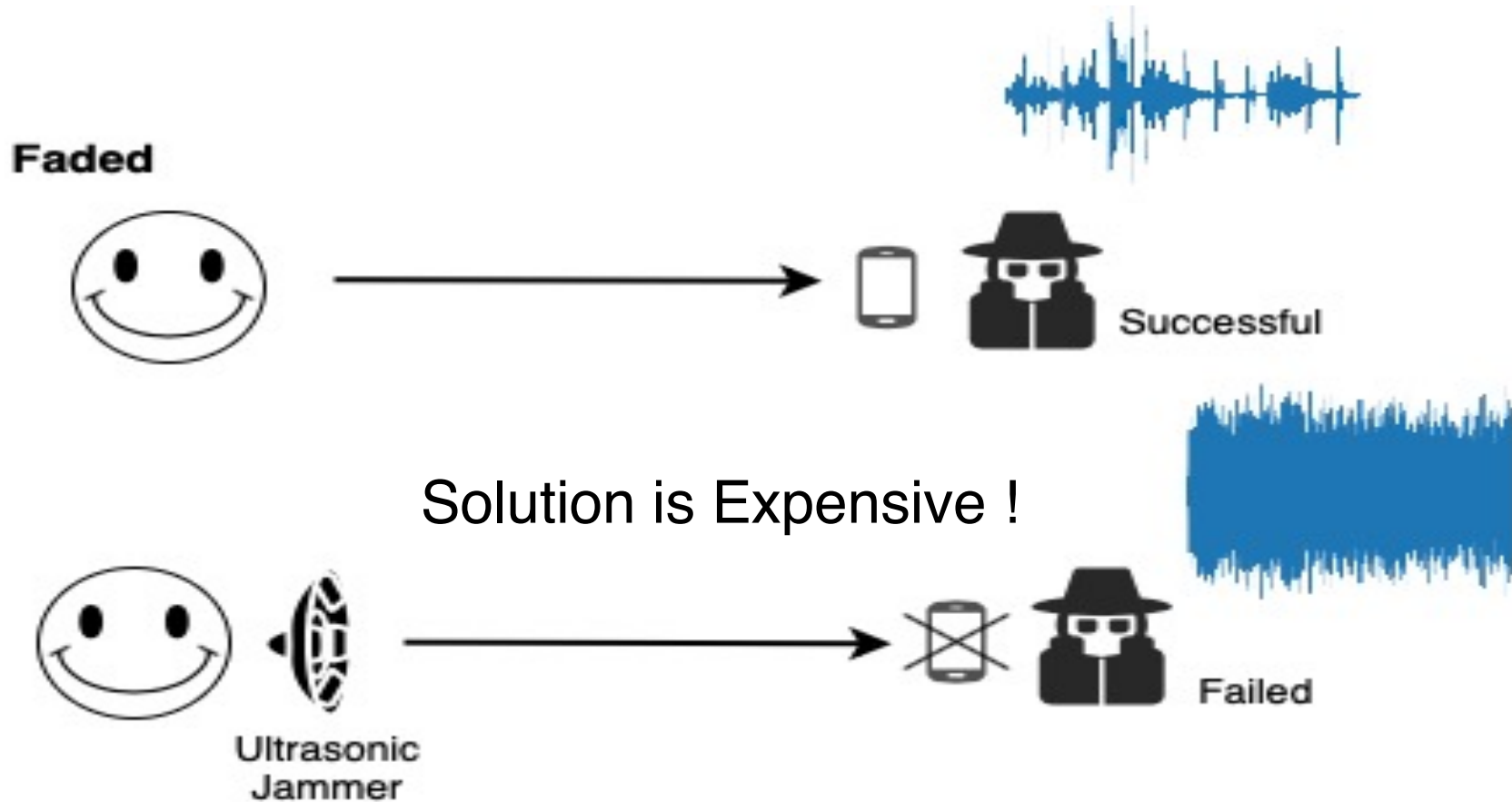
- The piezoelectric material, such as ceramic, exhibits the property of generating an electric charge in response to mechanical stress.
- When sound waves impinge upon the ceramic, the molecules within ceramic undergo a regulated arrangement, generating electrical signals.

Just Imagine!

#HITB2024BKK



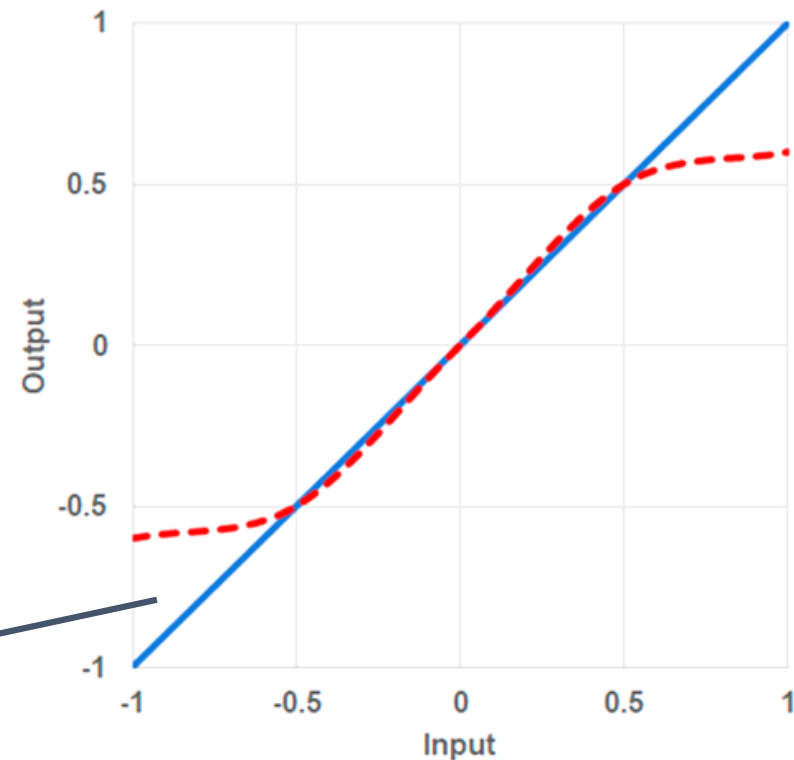
A spy is hiding somewhere and eavesdrops on you.



Why can Ultrasound interfere with the Reception of Low-frequency Signals ?

Non-Linear Phenomenon

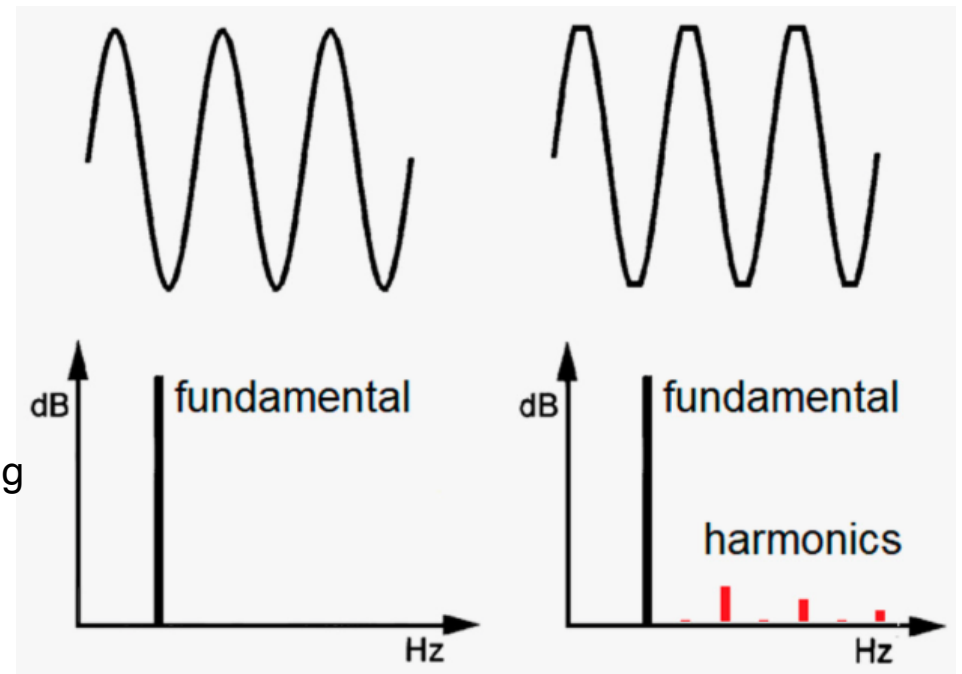
- ❑ The microphone belongs to the category of transducers and can be abstracted in the circuit as an "operational amplifier" (op-amp).
- ❑ Factors such as material, spatial layout, shape, size, etc., influence the amplification factor A of the microphone.
- ❑ Operational amplifiers have linear and nonlinear regions, and typical circuit devices keep the op-amp operating in its linear region.



The blue curve: Linear response
The red dashed curve: Nonlinear response

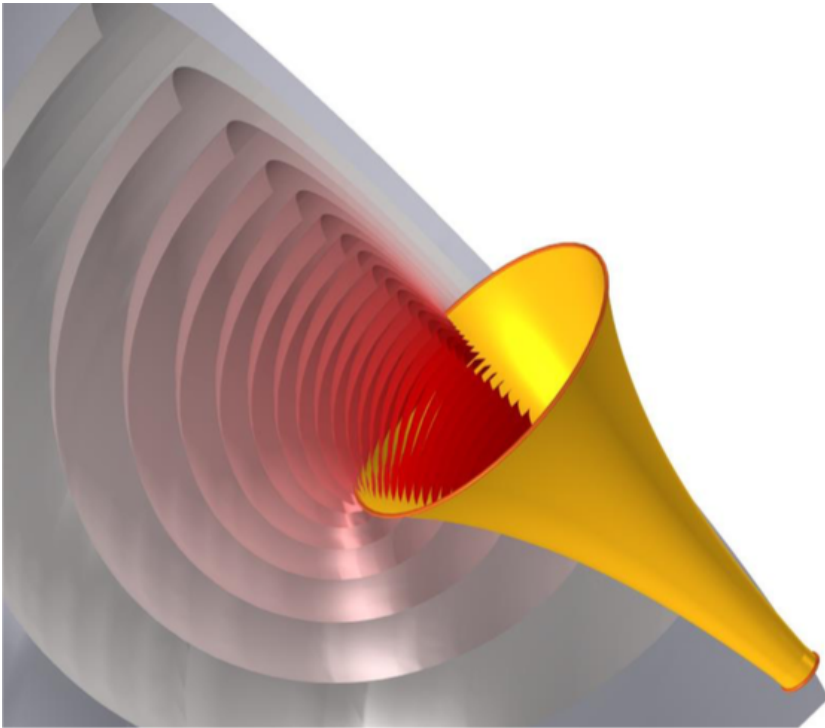
Total Harmonic Distortion (THD)

- THD quantifies signal distortion, representing the percentage of higher-order harmonics' root mean square (RMS) values relative to the fundamental frequency amplitude.
- Distorted signals, such as through symmetrical clipping, generate additional frequency components, known as harmonics, which are integer multiples of the fundamental frequency.
- A common preference is for THD to be below 1%, indicating that unwanted frequency components are 40 dB below the fundamental frequency. This limit is also "visual" as distortion becomes apparent in waveforms.
- Measuring THD at low to medium Sound Pressure Levels (SPLs) is challenging due to potential distortion from the loudspeaker. As SPL approaches the microphone's limits, THD may increase rapidly.

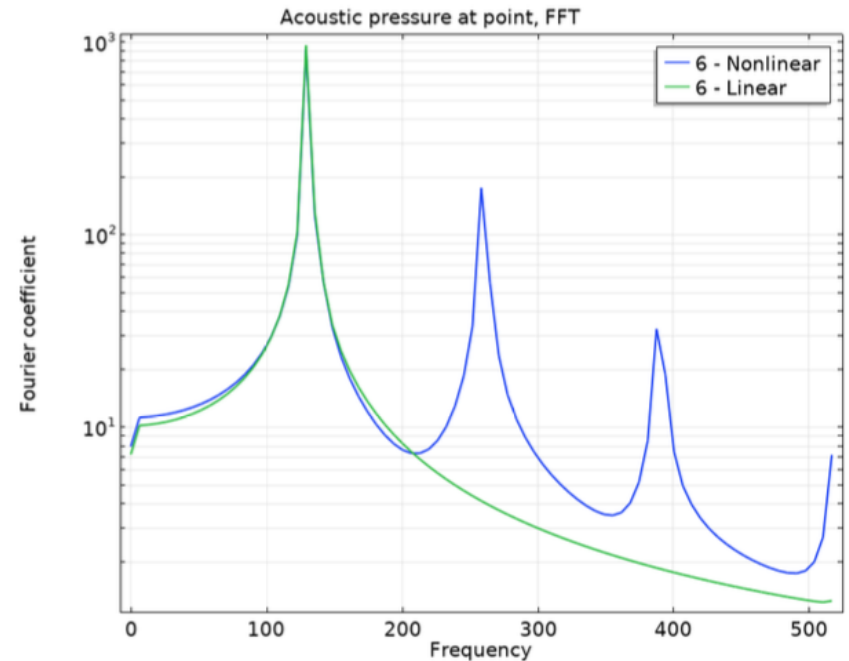


When SPL is Excessively High, what will happen ?

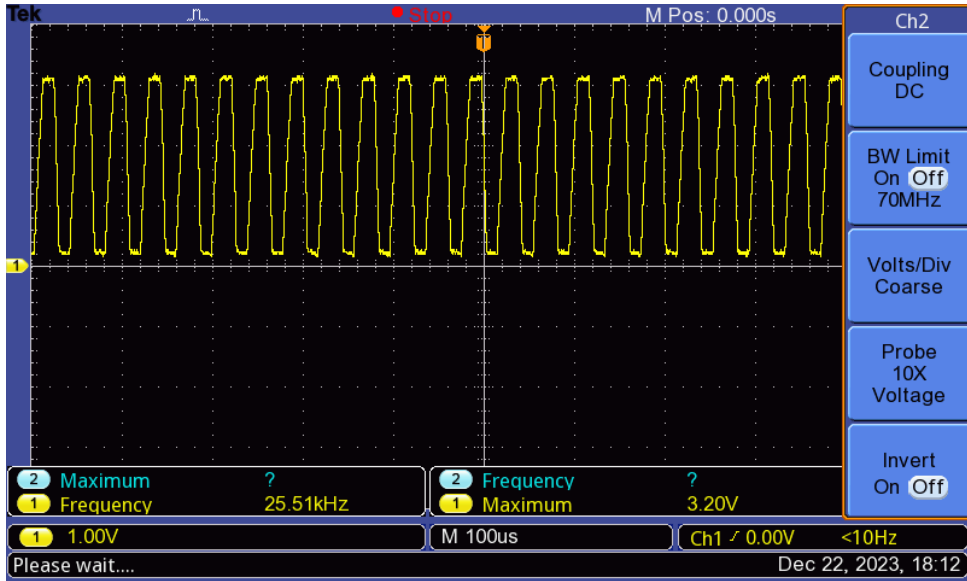
Simulation Using Comsol Software



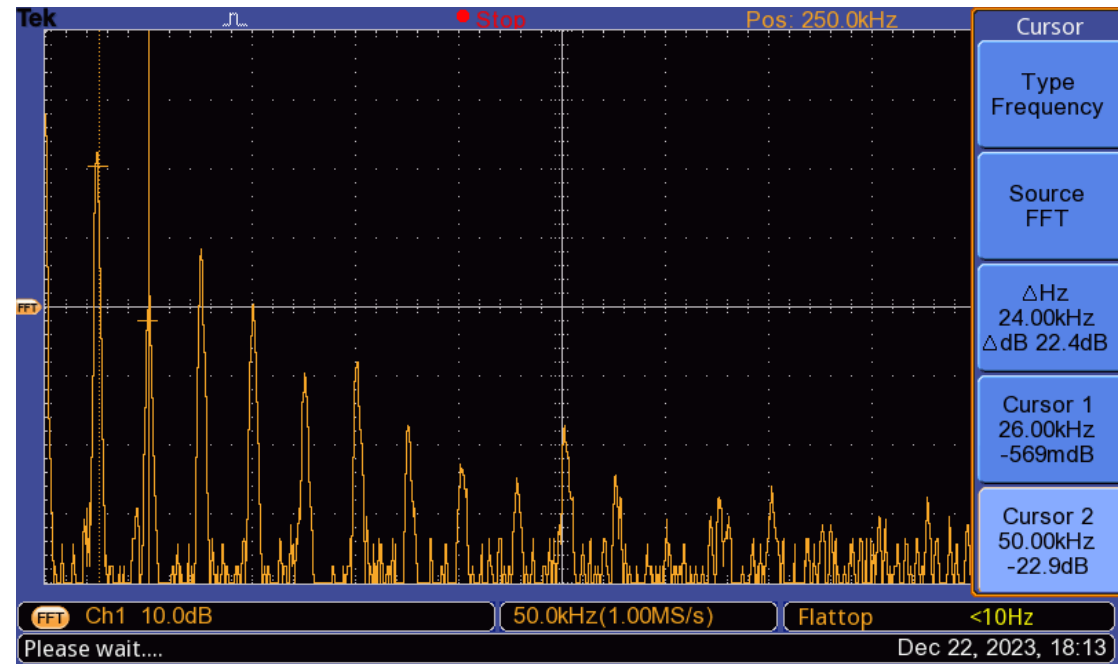
@ www.comsol.com/model/54021



- Variations in acoustic density and sound speed with changes in pressure

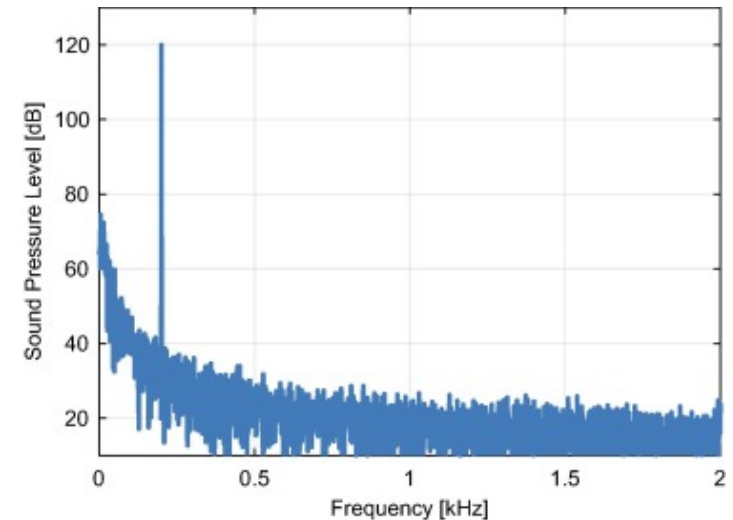


Microphone type: ADMP 401 MEMS
 microphone
 Oscilloscope: TeK 1126D

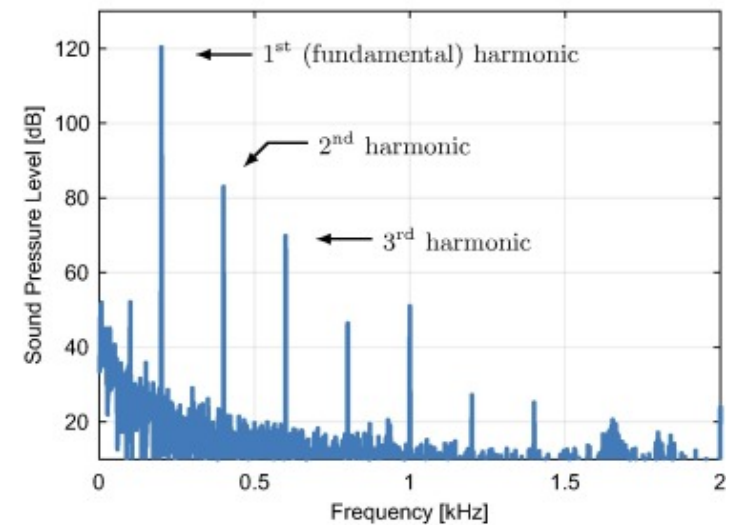


What Happens When the Signal Frequency Exceeds the Microphone's Designed Response Range?

When the signal frequency exceeds the designed frequency range, undesirable output responses occur. The human vocal frequency range is approximately 85Hz to 255Hz, and ultrasonic frequencies undoubtedly fall outside the linear feedback range of the microphone.

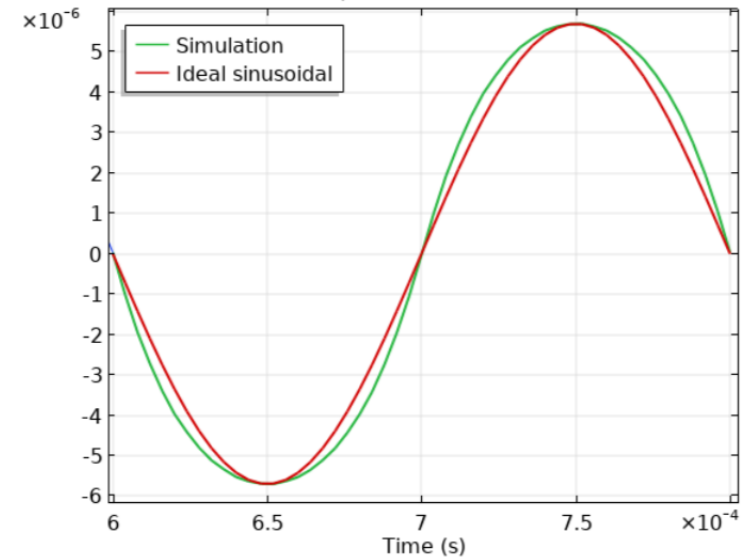
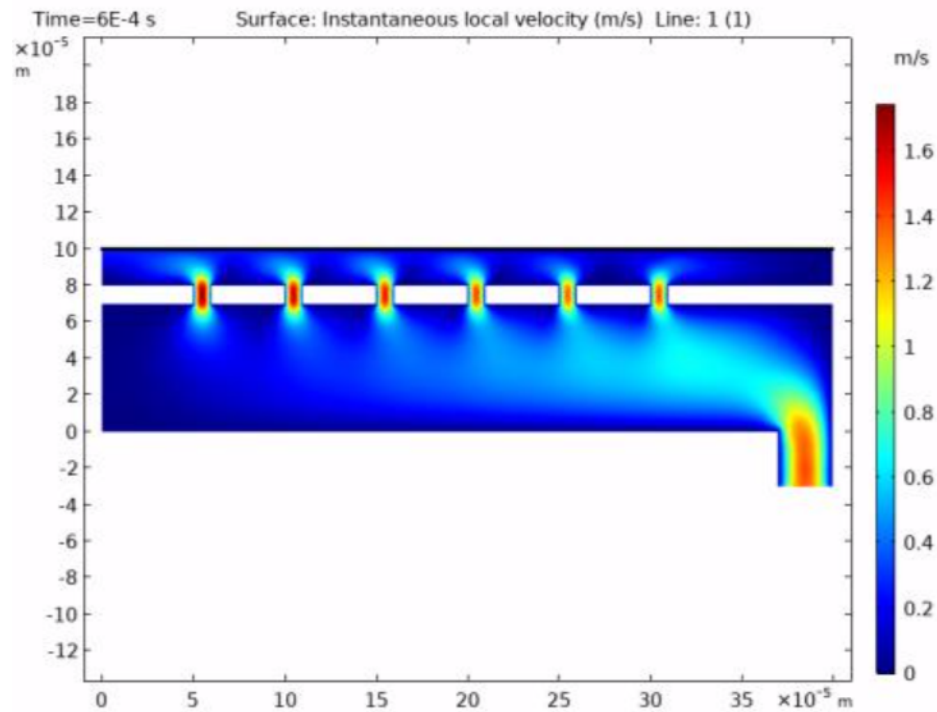


(a) reference microphone



(b) MEMS microphone under test

Simulation of Ultrasonic Wave Injection into Microphone Devices using Comsol Software



There are two reasons for the generation of nonlinearities in sound:

1. Excessive sound pressure levels (resulting in changes in energy density and sound velocity with pressure).
2. Nonlinearity in the strain gap of the microphone components.

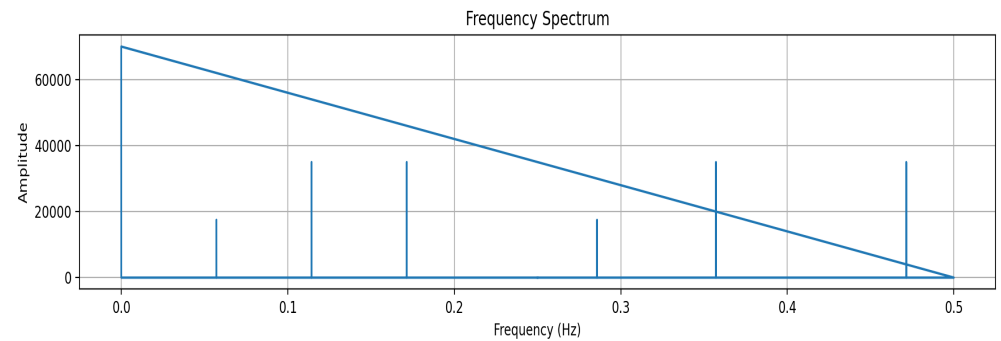
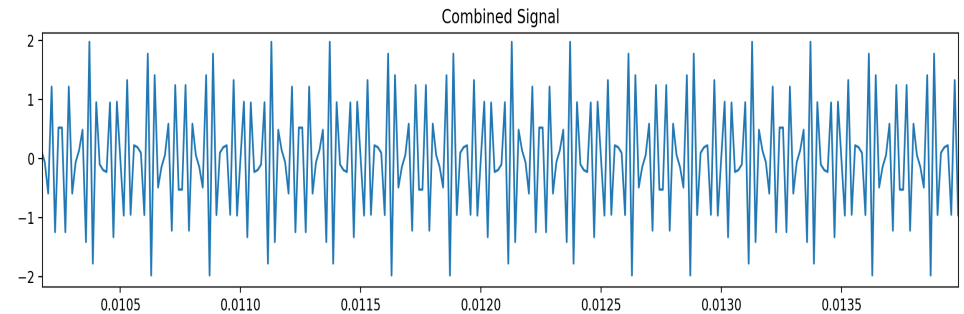
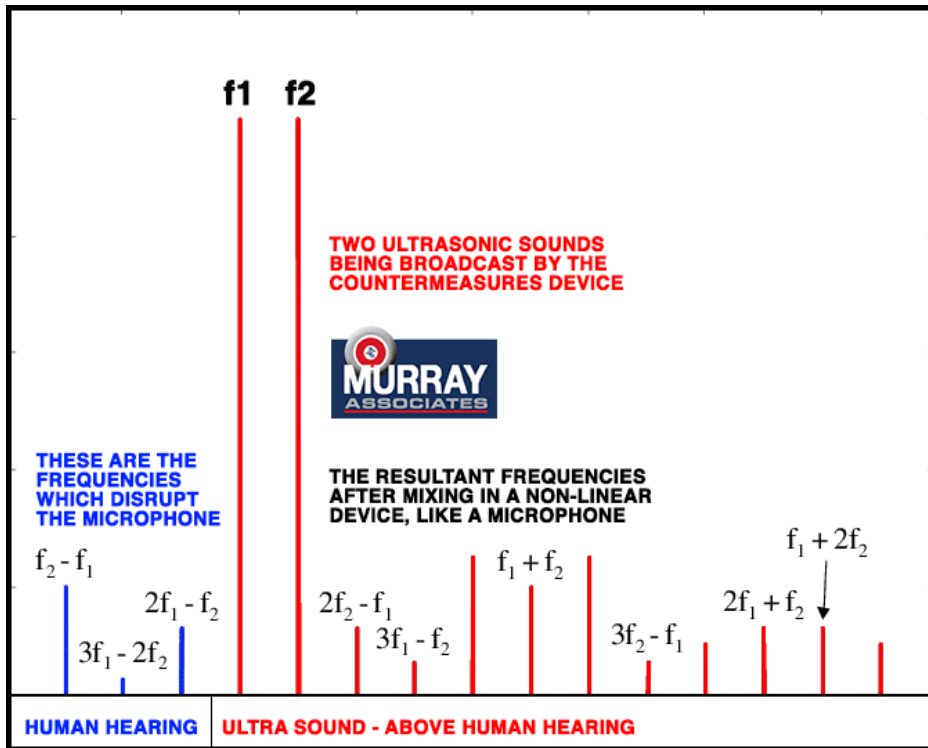
Intermodulation Algorithm

Equations:

$$S_{out} = A_1S + A_2S^2 + A_3S^3 + \dots + A_N S^N$$

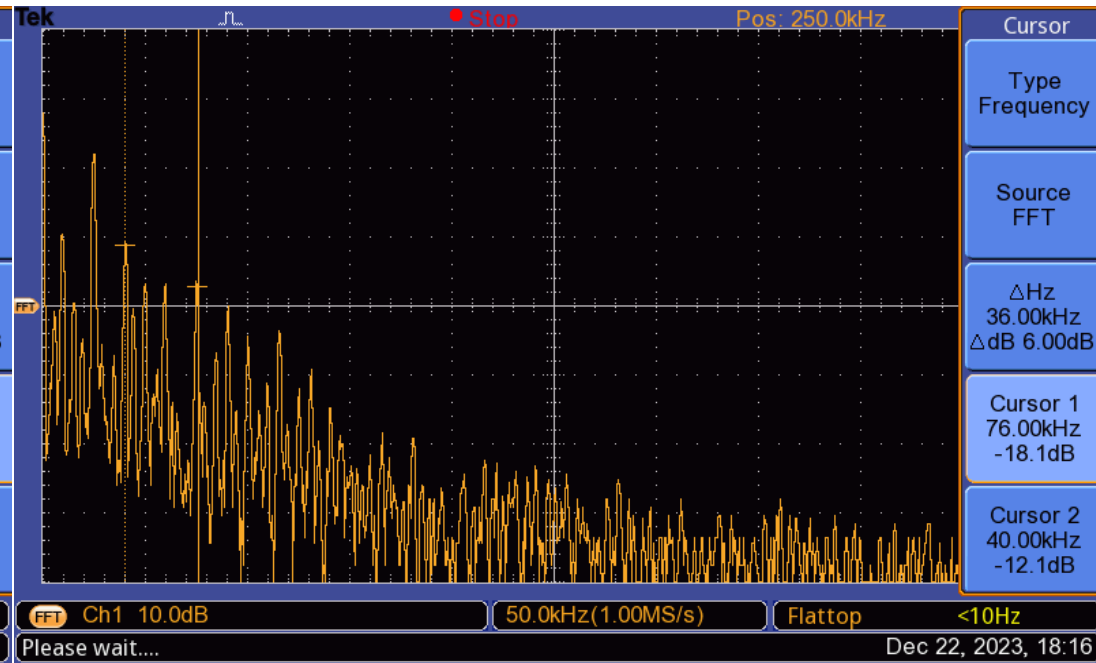
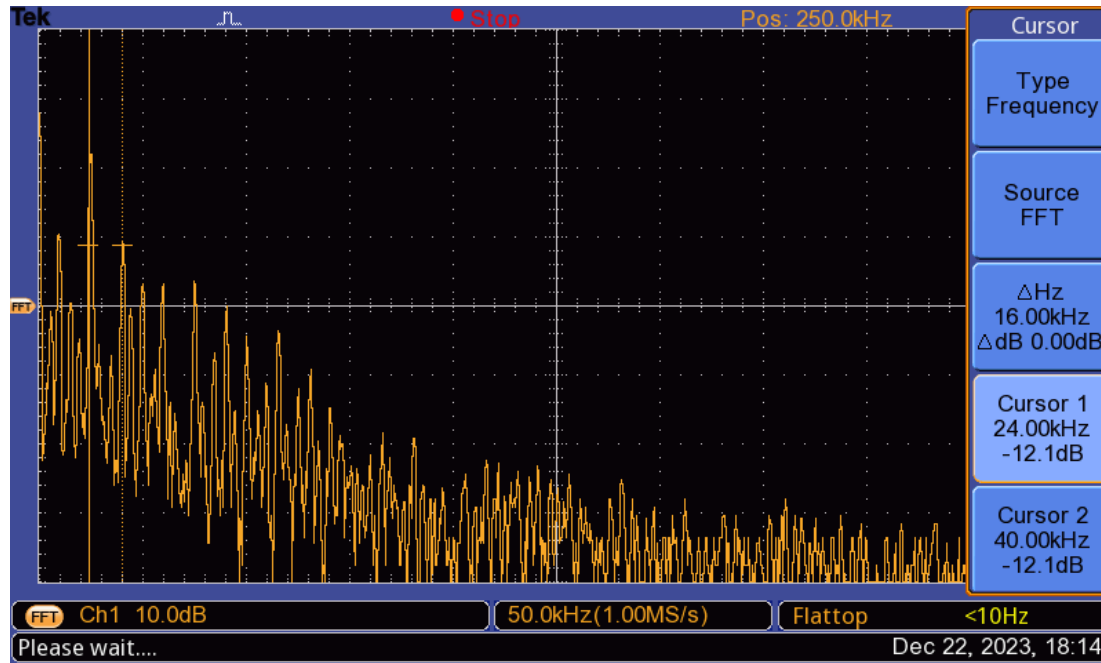
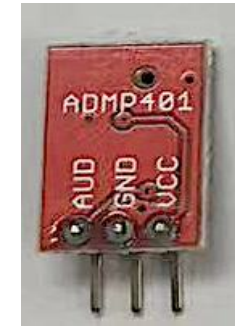
$$S = \cos(2\pi f_1 t) + \cos(2\pi f_2 t)$$

$$S_{out} = A_1S + A_2S^2 = A_1(\cos(2\pi f_1 t) + \cos(2\pi f_2 t)) + A_2(\cos(2\pi f_1 t) + \cos(2\pi f_2 t))^2$$

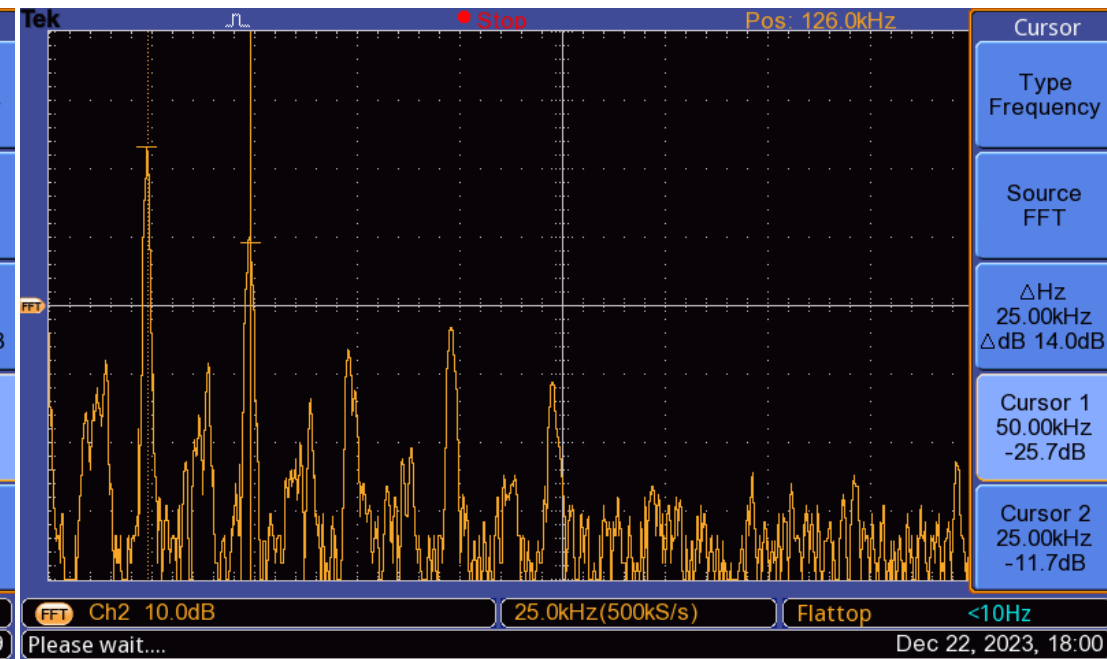
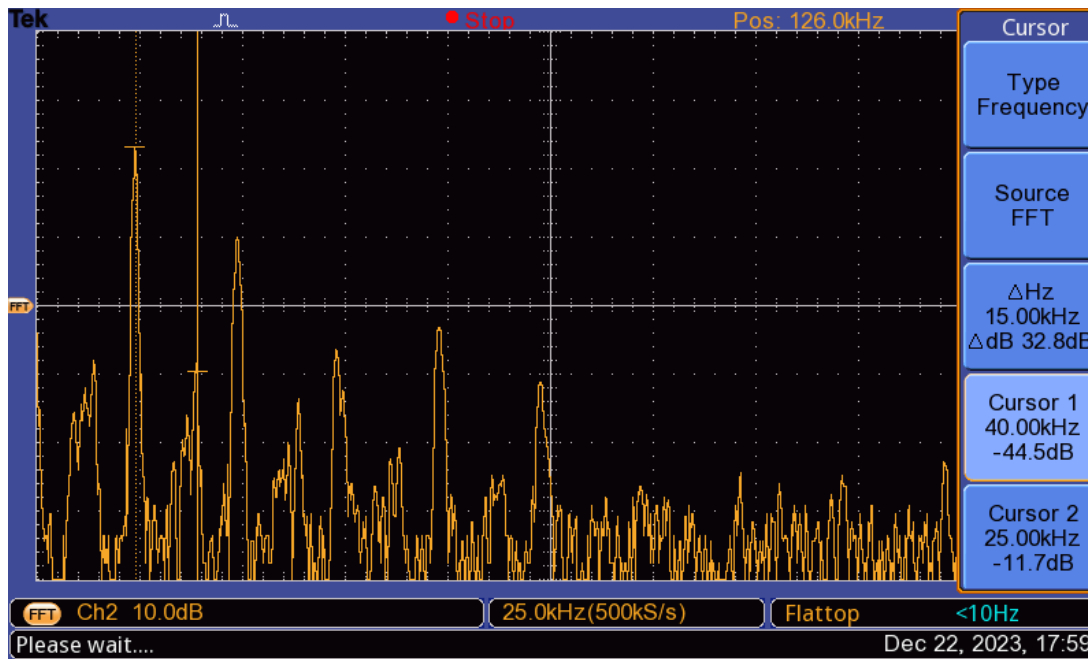
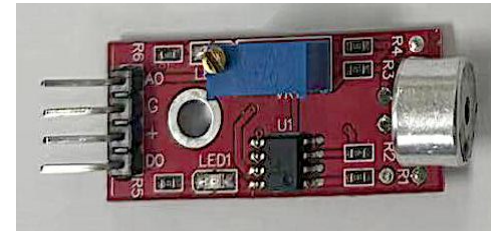


- To further validate our assumptions and simulation results, we employed the newly proposed dynamic intermodulation modulation algorithm.
- In the experiment, the interference distance between the jammer and the target was set to 1 meter, involving microphone types such as MEMS (ADMP 401 module), ECM, and piezoelectric microphones.
- In the actual environment, we recorded the authentic Fourier spectrum responses of each microphone, comparing them with the simulated spectrum responses generated by a Python program.
- This comparison aimed to assess the concordance between the real and simulated responses, providing empirical evidence for the nonlinear characteristics of the three types of microphones in response to ultrasonic waves.

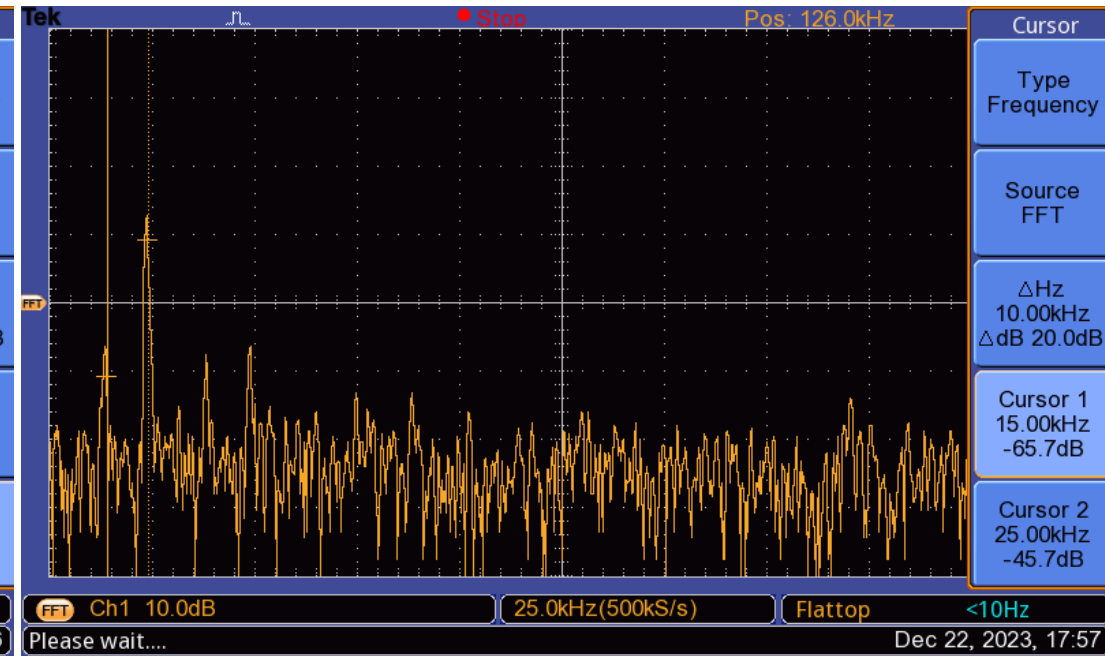
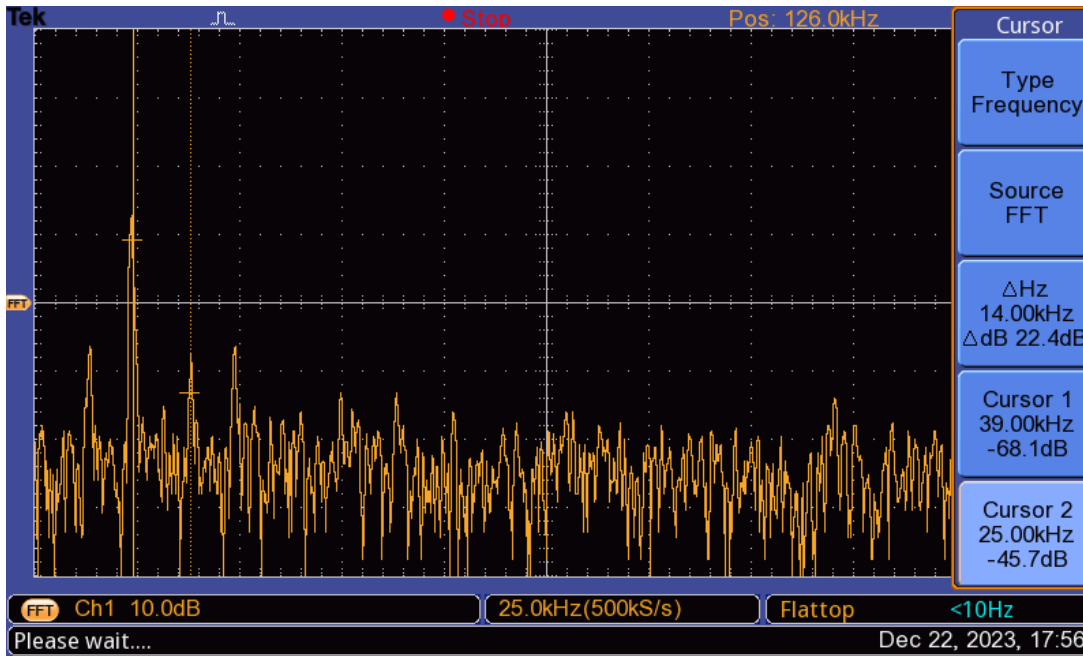
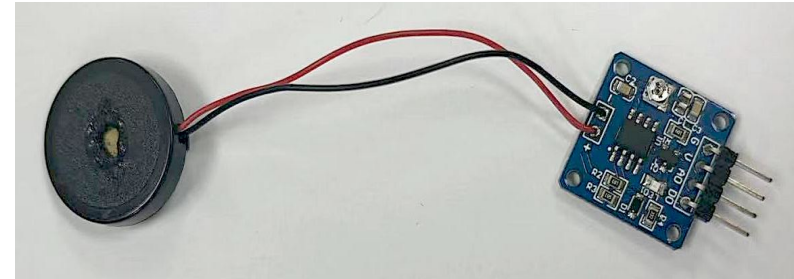
MEMS (ADMP401 Module)



ECM Module



Piezoelectric Ceramic



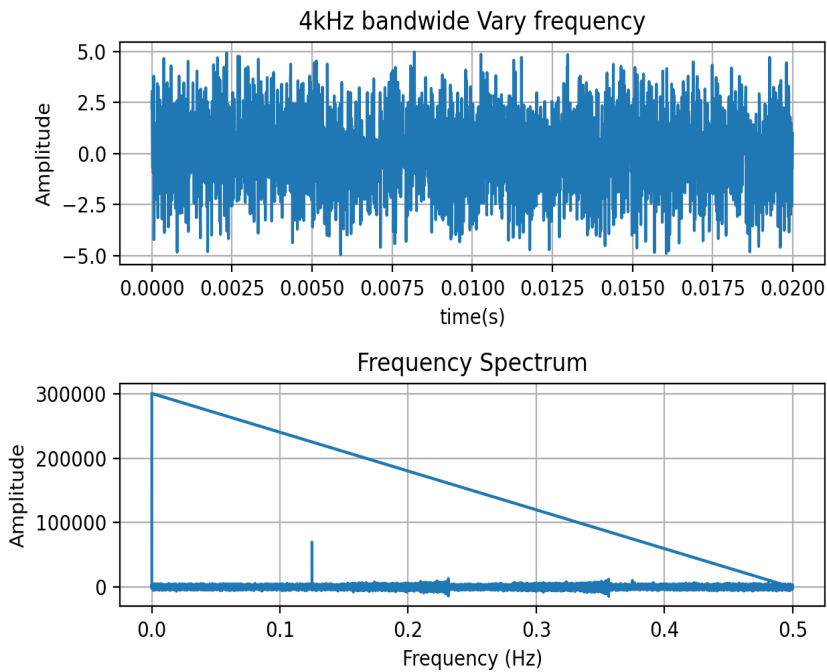
Our Ultrasonic Jamming Device

#HITB2024BKK



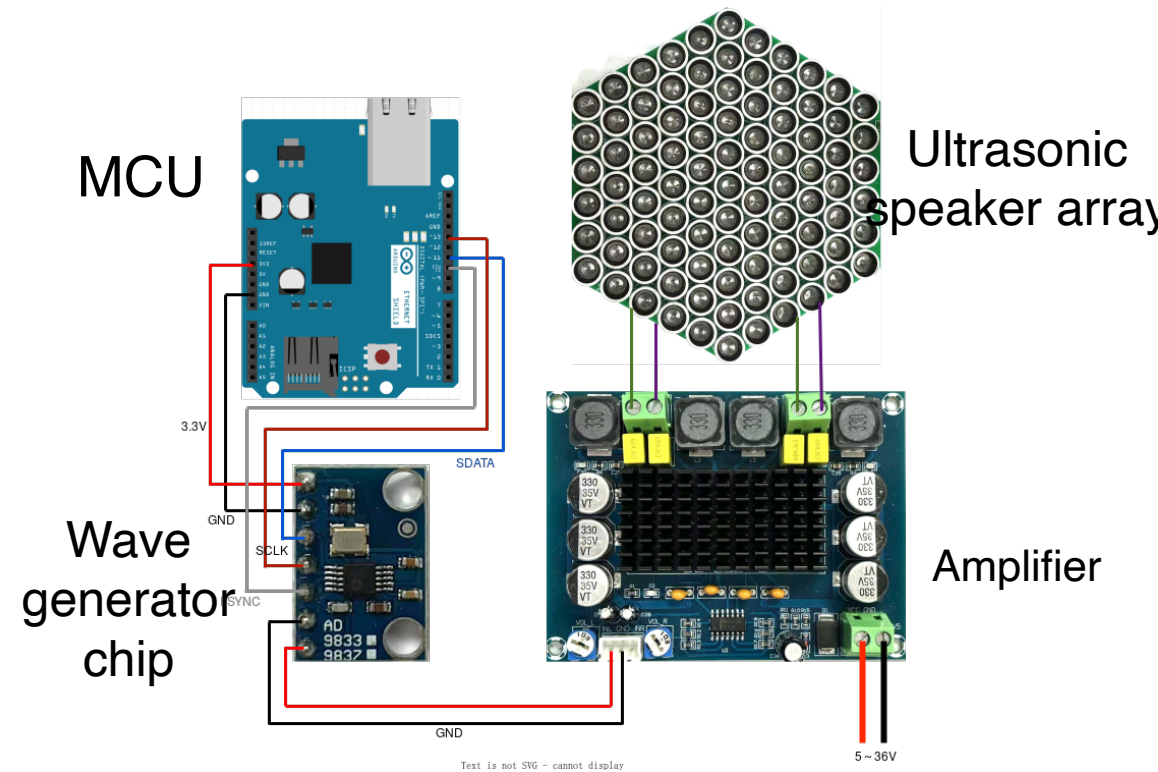
Version 1

GeekCon Modulation Method



40kHz with a bandwidth of 4kHz

GeekCon Implementation

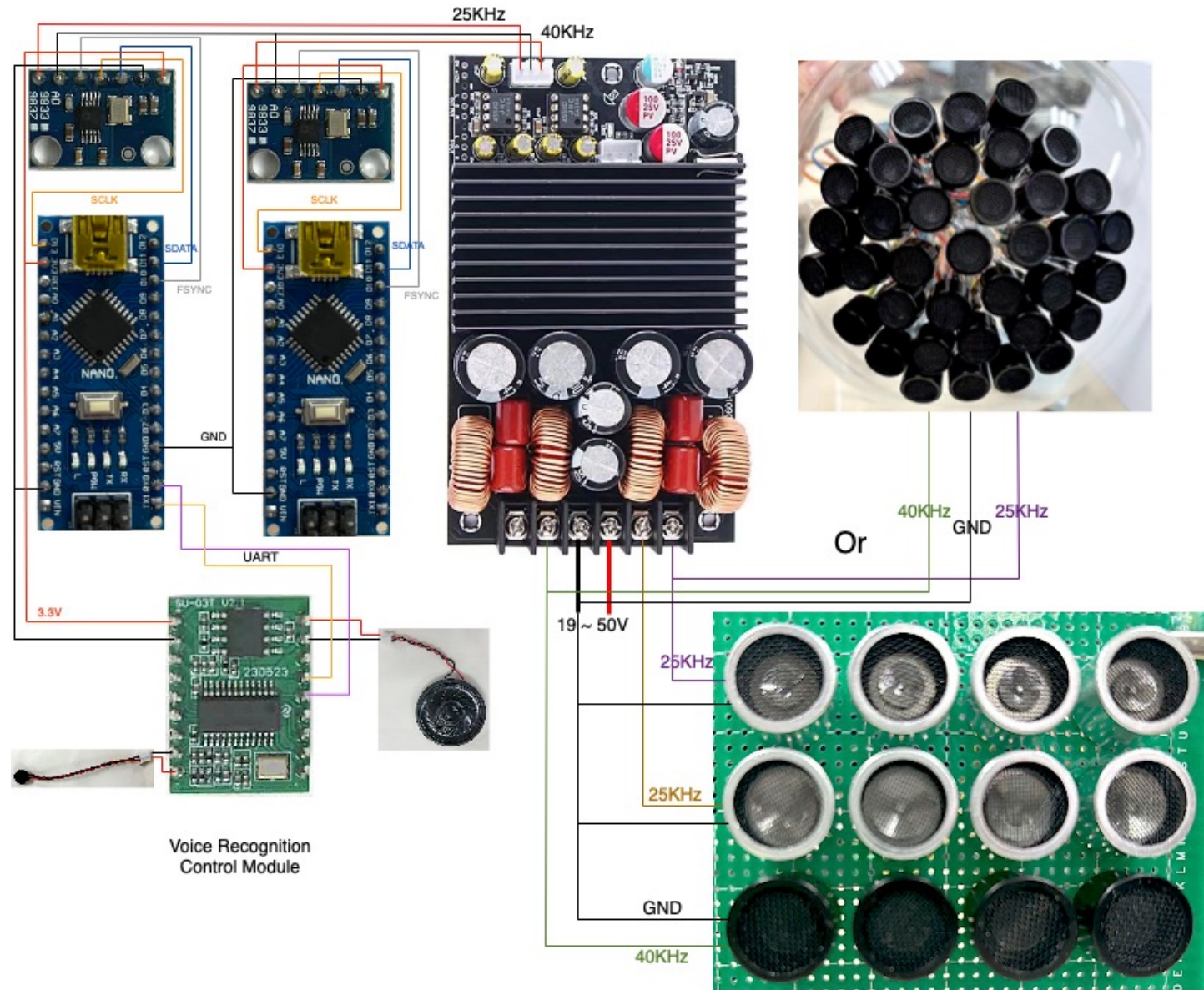


Version 2: Ultrasonic Jammer

#HITB2024BKK



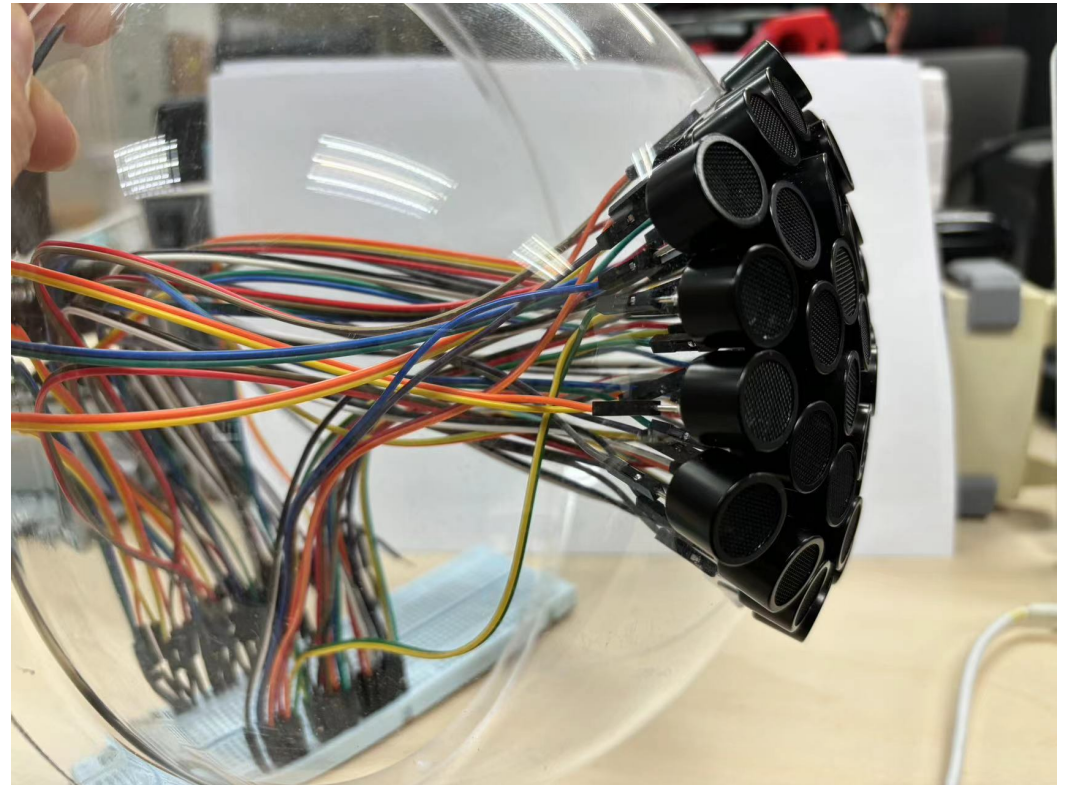
Version 2



Hemispherical Ultrasonic Speaker Array



Front view



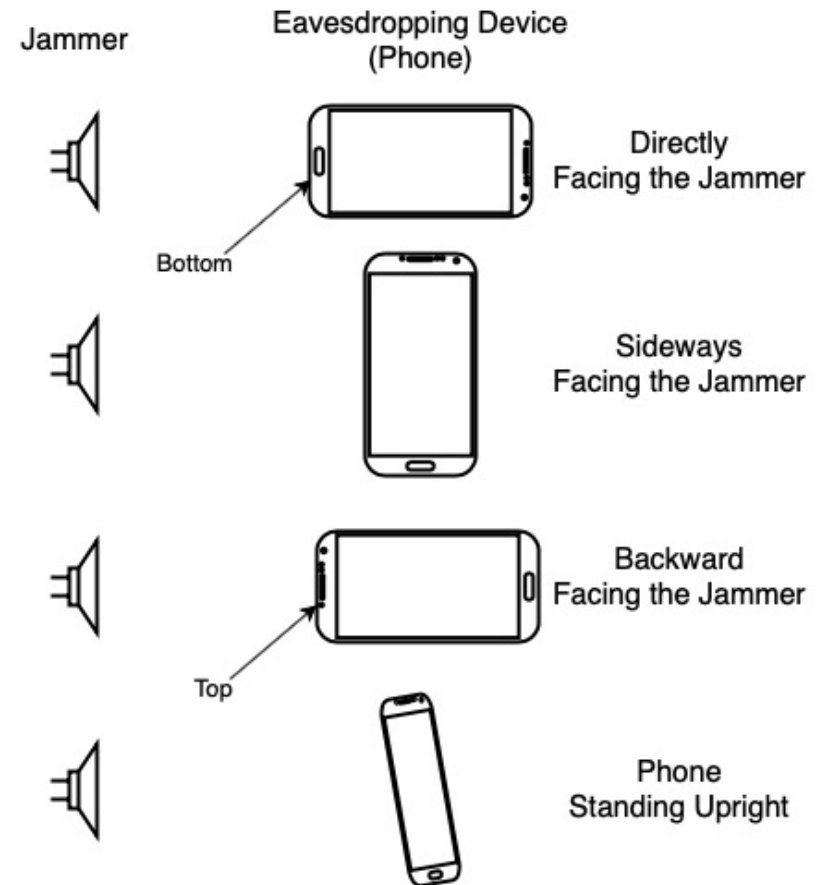
Sideway view

Effective Solutions for Handling Various Workplace Challenges

#HITB2024BKK










- We conducted multiple test experiments in a real conference room.
- Using TTS software, we played 'one to ten' repeatedly to simulate a genuine speaking scenario in the meeting room. The interference distance was set at 2 meters. (This distance we deemed reasonable as it approximates the placement of our device on the roof or at the center of a conference room table.)
- To vary the difficulty of interference, we positioned eavesdropping devices (Phone) differently: facing the disruptor directly, positioned sideways, facing the disruptor backward, and standing upright (as illustrated on the right).



Scenario 1 : Meeting Room

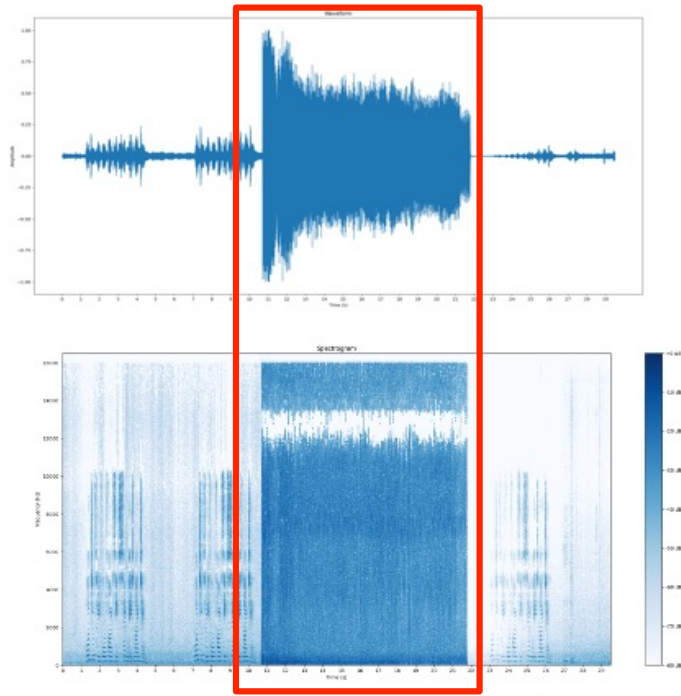
The audio test results are shown in the table below:

	Our Ultrasonic Jammer	Commerical Ultrasonic Jammer
Directly		
Sideway		
Backward		
Stand upright		/

Scenario 1 : Meeting Room

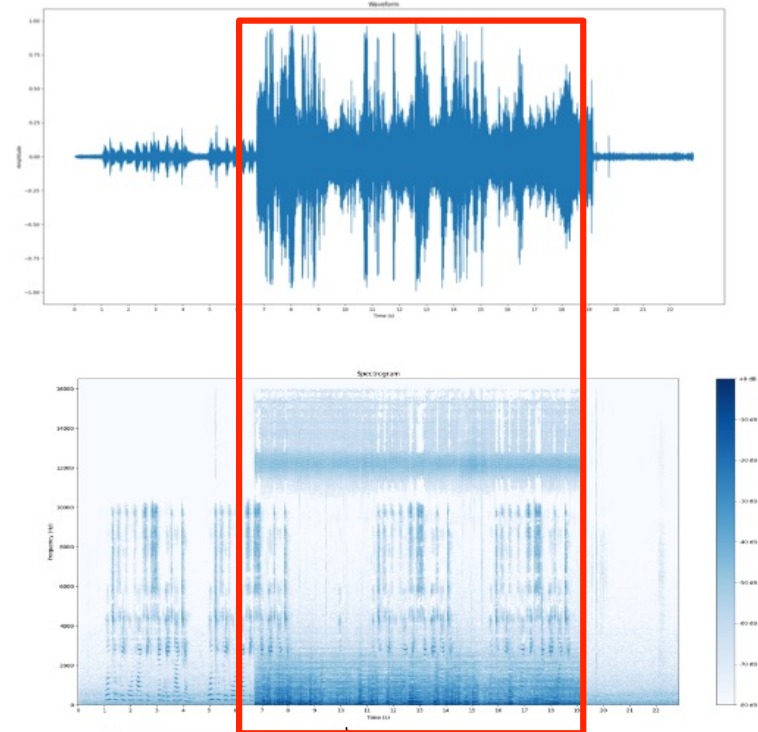
- To demonstrate the optimization of our ultrasonic jammer, we have illustrated the test results of our jammer and commercial jammers in various scenarios through waveform diagrams, spectrograms, and corresponding speech-to-text (STT) transcriptions using iFLYTEK and otter.ai models respectively.
- By comparison, we've proven the enhanced performance of our jammer in various scenarios relative to existing commercial devices.

Result Figures (Directly)



iFLYTEK: 123456789, 10, 123456789, 10. 3456789, 10,
otter.ai: 1-234-567-8910 1-234-567-8910 1-234-567-8910

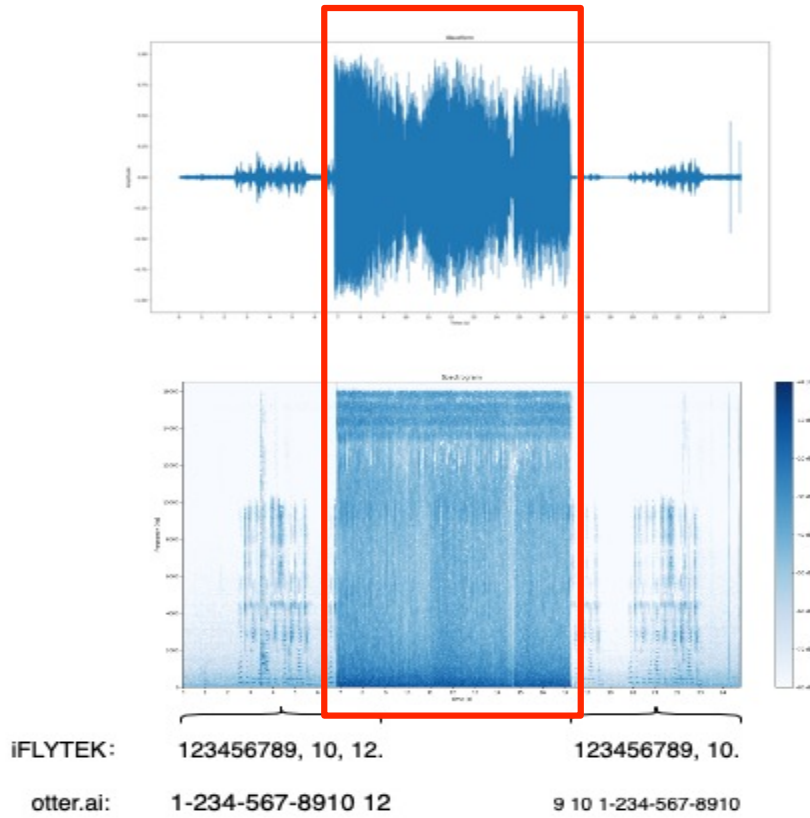
Our Jammer



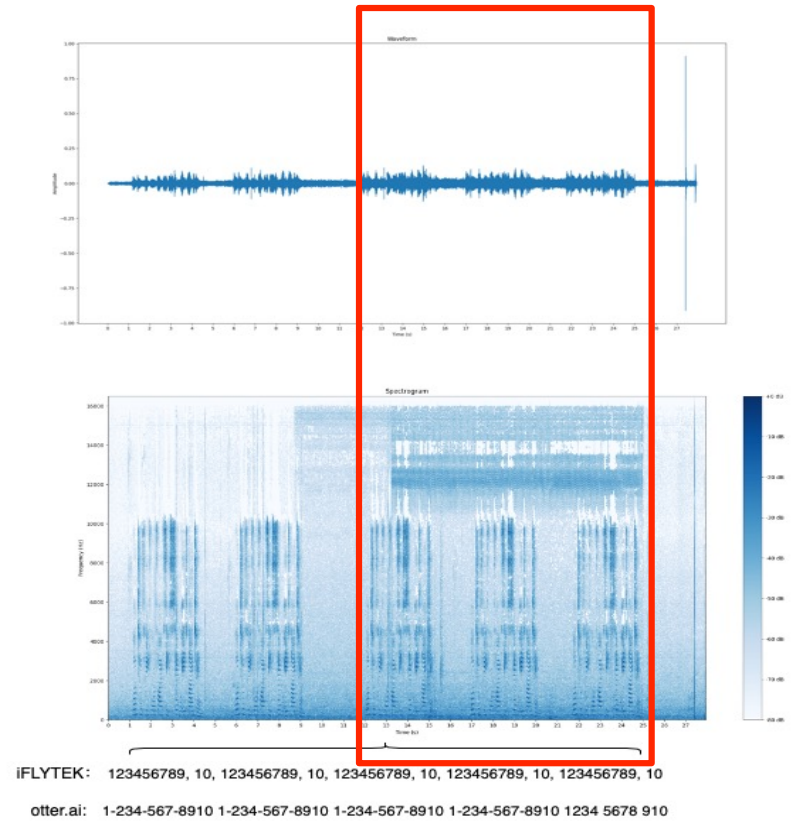
iFLYTEK: 123456789, 10, 123456789, 10, one, 11234567892, 1234567892.
otter.ai: 1-234-567-8910 1234567892123456 the same way to nine to 123567892

Commercial Jammer

Result Figures (Sideaway)

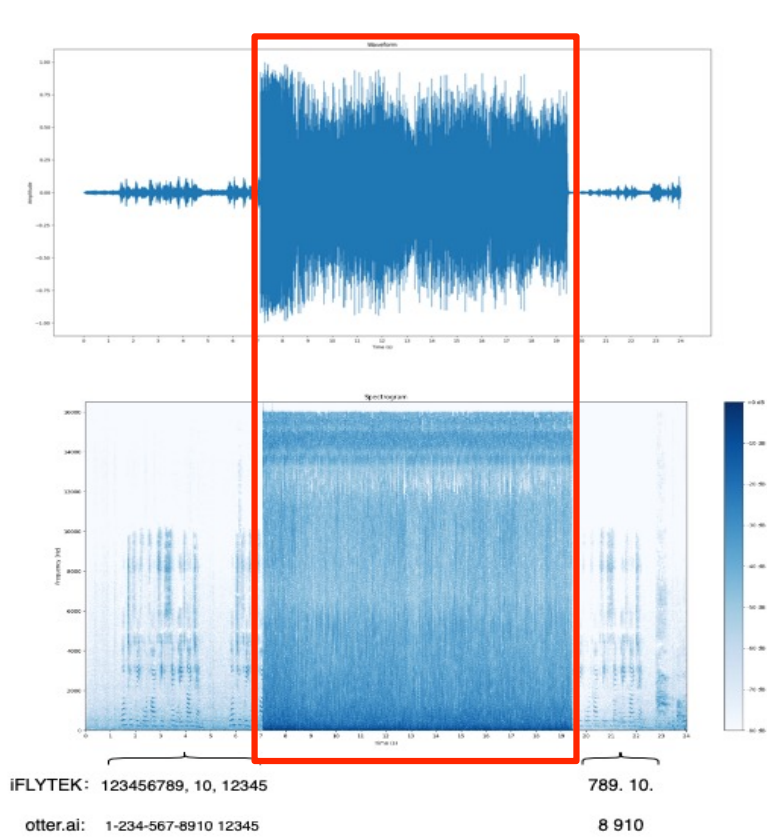


Our Jammer

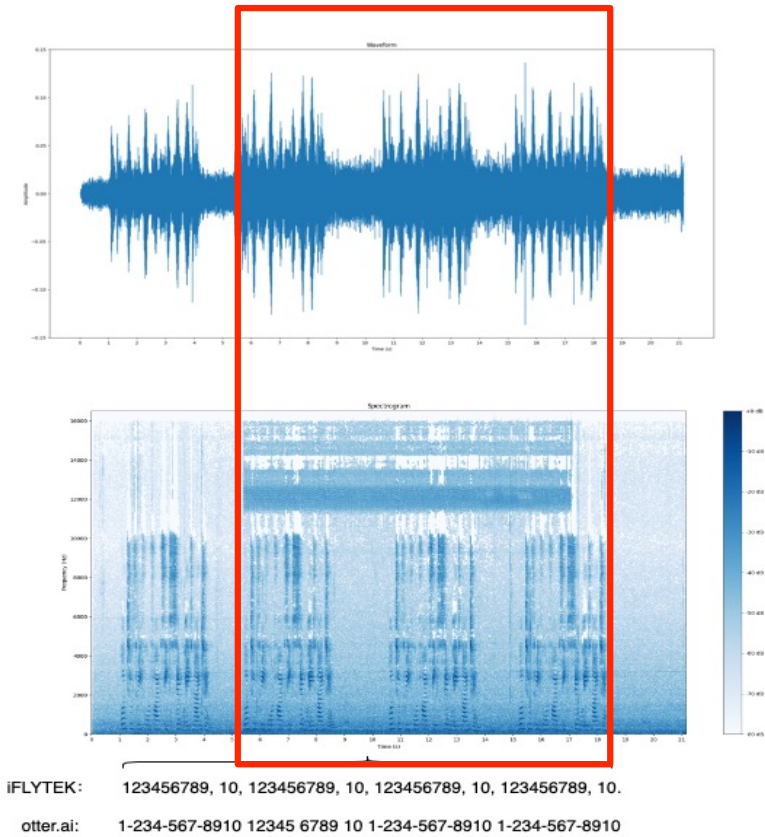


Commercial Jammer

Result Figures (Backward)

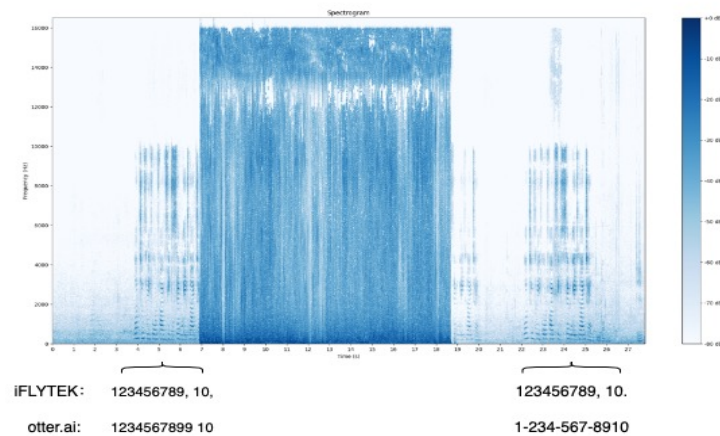
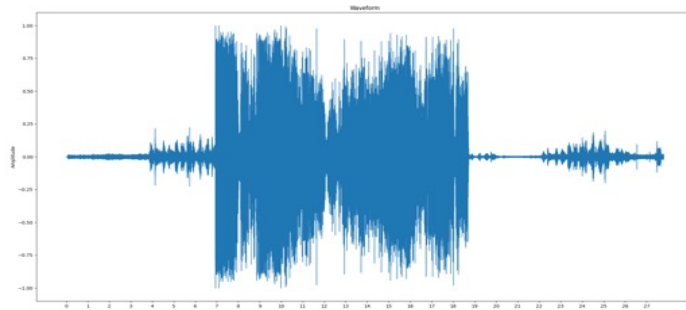


Our Jammer



Commercial Jammer

Result Figures (Stand Upright)



Our Jammer

- The results above demonstrate that when our jammer is activated, it generates a wide-band interference signal that renders both STT models (iFLYTEK and otter.ai) unable to recognize any meaningful information.
- In contrast, commercial jammers, when activated, produce interference signals that can be observed in the corresponding waveform and spectrogram. However, they fail to effectively disrupt eavesdropping devices from capturing information, and both STT models can still identify the transmitted 'one to ten' message.

Scenario 2 : Real Eavesdropping (Hold in hand and simulate phone use)



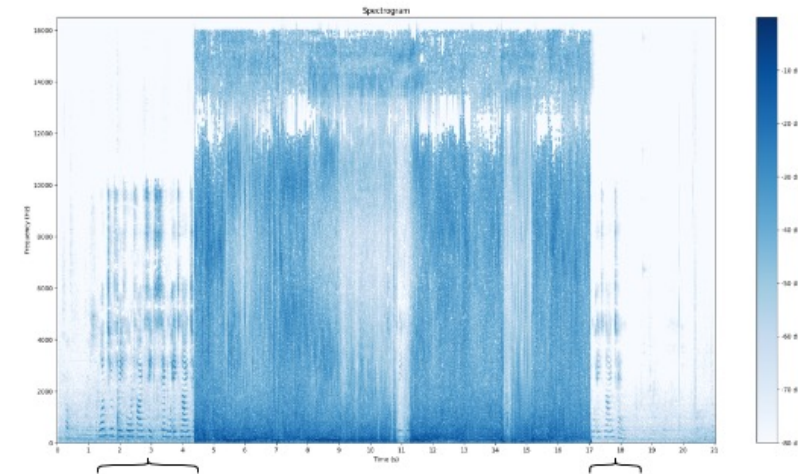
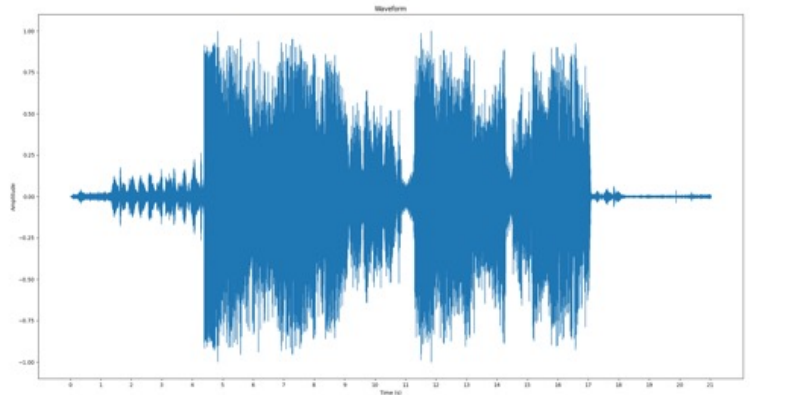
•Emulating real spy scenarios, we hold our eavesdropping device (phone) like left photo shown, with the ultrasonic jammer positioned to my left at a distance of 2 meters.

Result audio:

•In the audio results, we are unable to hear the background sound of the 'one to ten' playing while the jammer is active. This effectively demonstrates the practical value of our current ultrasonic jamming device.

In the Real Eavesdropping Scenario:

- The left picture displays the waveform, spectrogram, and STT transcriptions of record from the phone.
- Activating our jammer disrupts the background noise, rendering Speech-to-Text models unable to recognize the audio, as shown in left picture.



iFLYTEK: 123456789,10.

otter.ai: 1-234-567-892

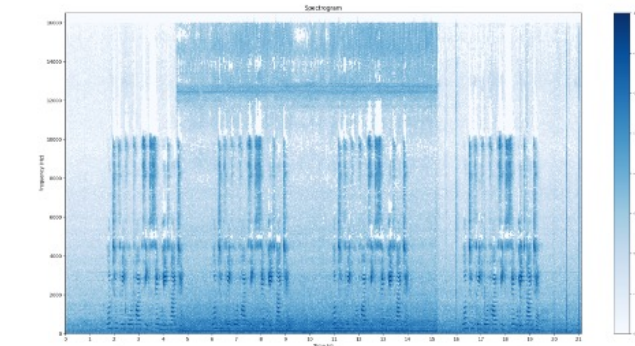
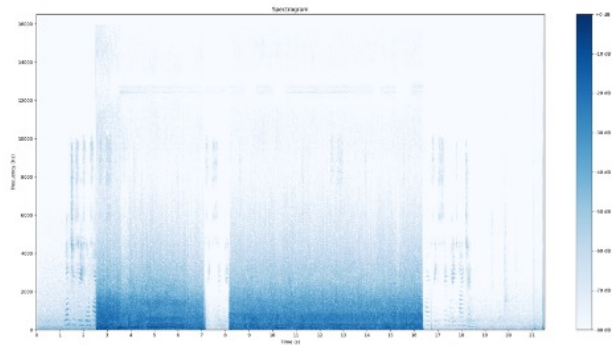
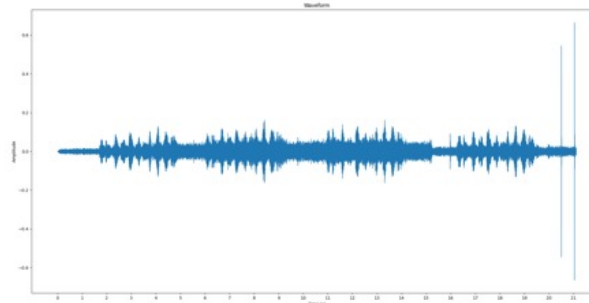
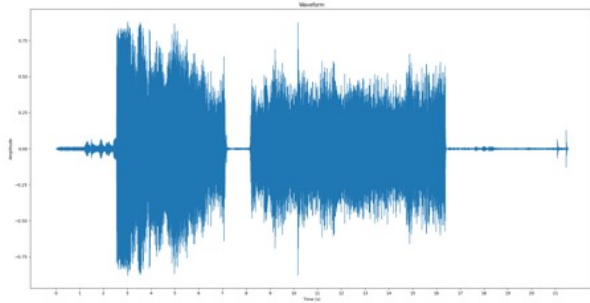
89,10

Scenario 3 : Version 1 VS Version 2

Directly :

Backward:

- Two figures display the results of version 1.
- When the phone is positioned backward facing the jammer, the jammer is unable to interfere with the eavesdropping device's recording.

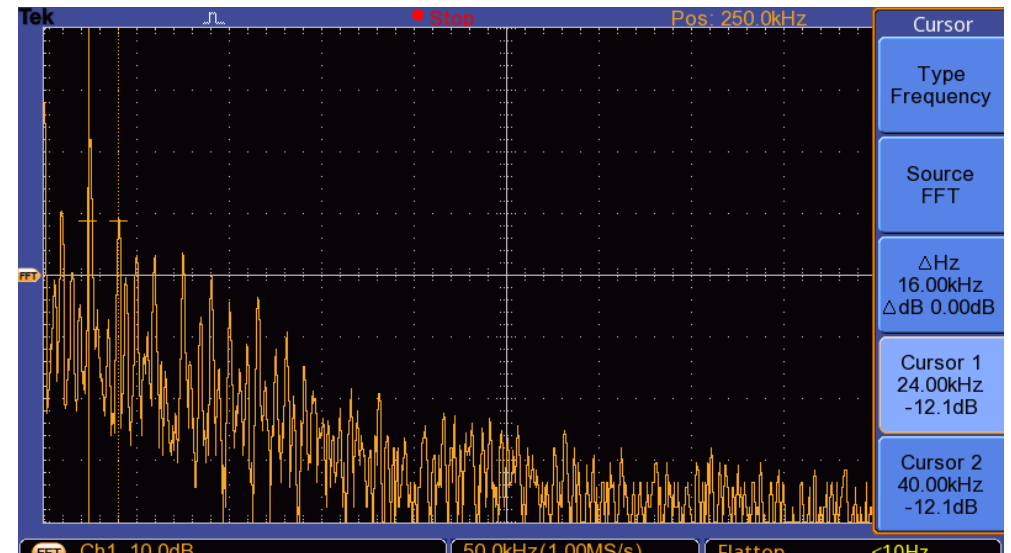
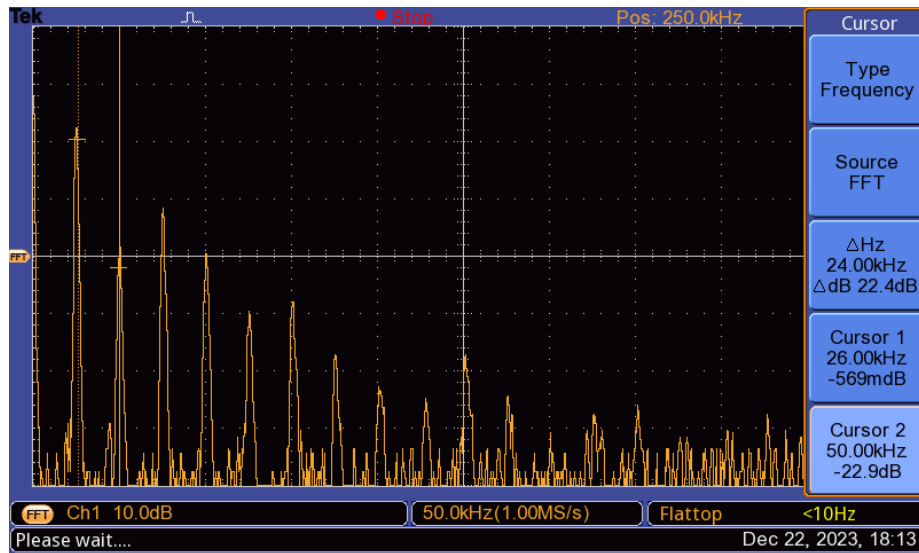


iFLYTEK: 12345
otter.ai: 12345 8910

iFLYTEK: 123456789, 10, 123456789, 10, 123456789, 10, 123456789, 10.
otter.ai: 1-234-567-8910 1-234-567-8910 123456789 1-234-567-8910

Scenario 3 : Version 1 VS Version 2

Eavesdropping device: ADMP401
Microphone



In our experiment, we used MEMS microphones as injection devices to measure the real-time Fourier spectra of the actual jamming audio for version 1 (left image) and version 2 (right image).

Due to the introduction of the Dynamic Intermodulation (DIM) algorithm, the central frequency distribution of the jamming signal's energy is denser and more varied, which reduces the noise reduction effectiveness of devices and enhances the jamming effect of our jammer.

Scenario 4 : Eavesdropping Device in Leather Pouch

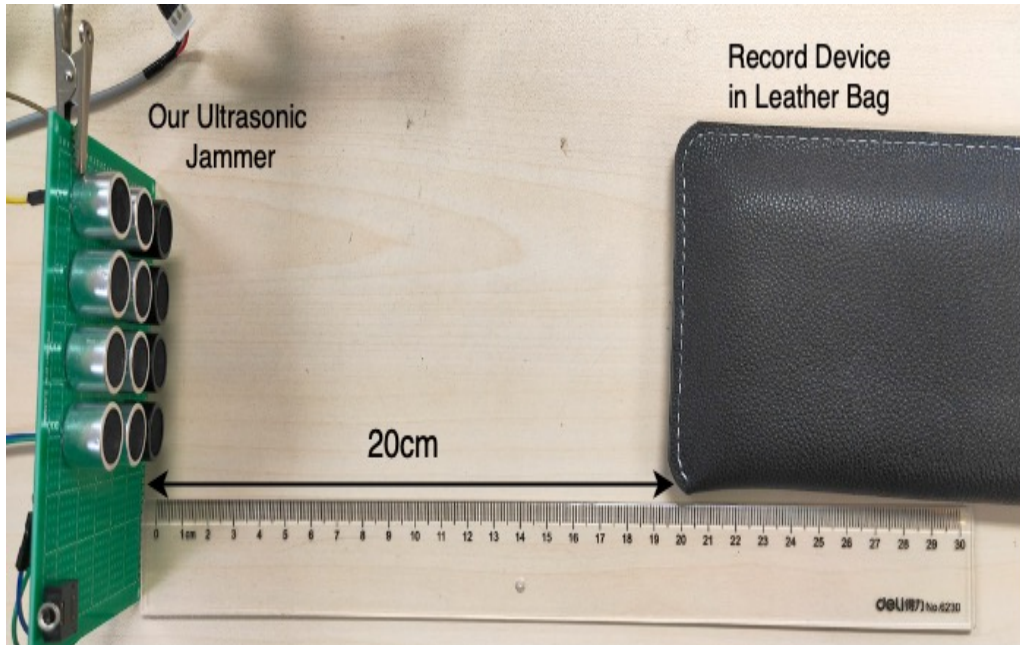


Result
audio:

Experimental Procedure:

Start by placing the phone outside, then insert it into the leather pouch before retrieving it.

Scenario 4 : Eavesdropping Device in Leather Pouch



- In the scenario with a disruption distance of 20 centimeters, careful listening to the audio obtained from real tests reveals a significant reduction in ultrasonic signals due to the presence of the leather pouch.
- The current power level is not sufficient to completely disrupt eavesdropping devices placed inside a leather pouch.
- While at times increased power can enhance algorithm performance, surpassing the current power level may lead to heightened human awareness and auditory discomfort. Therefore, for this ultrasonic modulation method, there still exists a certain interference threshold beyond which it becomes noticeable and causes discomfort.

Ethical Considerations

#HITB2024BKK



Ethical Considerations

1. Legality and Authorization:

- Ensure that the use of ultrasonic jammers is legal and authorized.
- Obtain necessary permissions and adhere to relevant regulations.

2. Privacy Protection:

- Safeguard individuals' privacy rights when employing ultrasonic jammers.
- Clearly inform involved parties (e.g., employees or residents) about the purpose and usage of the device.

3. Minimization of Interference:

- Follow the principle of minimal interference.
- Only operate the device within the legal and authorized scope to prevent unnecessary disruption to other innocent devices or communication systems.

4. Technical Feasibility:

- Ensure that the design and use of ultrasonic jammers are technically feasible.
- Prevent negative impacts on normal communication and device operation while maintaining effective counter-surveillance.

5. Transparency and Communication:

- Practice transparency and open communication.
- Clearly communicate the purpose and operation of the ultrasonic jammer, and provide channels for addressing concerns or objections.

Takeaways

#HITB2024BKK



Takeaways

- Ultrasonic jammer utilizes sound waves at frequencies beyond the audible range to disrupt and confuse the receiving systems of microphones or eavesdropping devices, thwarting eavesdropping attempts discreetly.
- Ultrasonic waves exceed the frequencies audible to the human ear, enabling a covert defense against eavesdropping, and ultrasonic waves at a certain power level pose no harm to the human body.
- However, ultrasonic anti-eavesdropping technology has its limitations, such as leather, denim, coats, etc., are impervious to ultrasonic waves.
- It demands stringent conditions in practical scenarios, as there should be no sturdy obstacles between the device and the eavesdropping equipment, such as walls, doors, or sound-reflective materials.

Q&A

This work link:

https://github.com/Moriartysherry/Ultrasonic_Jammer



#HITB2024BKK

