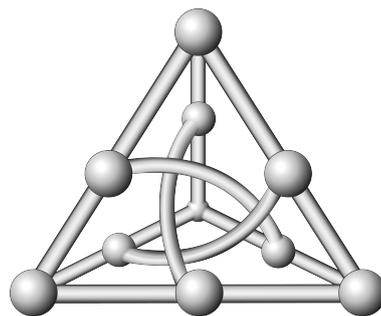


A NOSSA UNIVERSIDADE



FACOM-UFMS

UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL
FACULDADE DE COMPUTAÇÃO
CURSO DE GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

ALEXANDRE YUITI FERNANDES SHIMIZU

Condicionamento de Sinais de Sensores Piezoelétricos:
Detecção de Eventos em Sistemas Mecânicos

Campo Grande
2024

ALEXANDRE YUITI FERNANDES SHIMIZU

Condicionamento de Sinais de Sensores Piezoelétricos:
Detecção de Eventos em Sistemas Mecânicos

Trabalho de Conclusão de Curso de Graduação em Engenharia da Computação da Faculdade de Computação da Universidade Federal de Mato Grosso do Sul como requisito para a obtenção do título de Engenheiro da Computação.
Orientador: Dr. Milton Ernesto Romero Romero

Campo Grande
2024

AGRADECIMENTOS

Expresso minha gratidão aos professores da banca examinadora pela disponibilidade e pelo tempo que dedicado à análise deste trabalho. Reconheço a importância de sua contribuição para a validação e aprimoramento deste estudo e agradeço por sua participação neste processo.

RESUMO

Este trabalho investiga o uso de sensores piezoelétricos do tipo pastilha para o condicionamento e preparação de sinais, com o objetivo de viabilizar seu condicionamento por microcontroladores. O estudo se fundamenta em modelos matemáticos e simulações de circuitos para analisar a viabilidade de detecção de eventos mecânicos em sistemas de vibração. As ondas mecânicas geradas em diferentes cenários são modeladas como ondas de Rayleigh, sendo analisadas tanto em domínios temporais quanto frequenciais.

Para a validação, foram projetados circuitos amplificadores que condicionam os sinais dentro das especificações de tensão dos microcontroladores utilizados, garantindo a integridade das leituras mesmo em condições adversas. Simulações e ensaios experimentais exploraram aspectos como eficiência energética, robustez dos circuitos e qualidade dos sinais obtidos.

Os resultados indicam que a proposta é viável, apresentando potencial para aplicações em contextos como segurança cibernética e monitoramento de eventos mecânicos. A simplicidade do circuito e o uso de componentes acessíveis tornam a abordagem adequada para pesquisadores e entusiastas em áreas técnicas.

Palavras-chave: Vibrações e Ondas Mecânicas; Sensores Piezoelétricos; Coleta e análise de sinais; Circuitos Amplificadores; Microcontroladores.

ABSTRACT

This study investigates the use of wafer-type piezoelectric sensors for signal conditioning and preparation to enable their integration with microcontrollers. The research is based on mathematical models and circuit simulations to assess the feasibility of detecting mechanical events in vibration systems. Mechanical waves generated in different scenarios are modeled as Rayleigh waves and analyzed in both time and frequency domains.

Validation was conducted through the design of amplifier circuits that condition signals within the voltage specifications of the microcontrollers used, ensuring data integrity even under adverse conditions. Simulations and experimental trials evaluated aspects such as energy efficiency, circuit robustness, and signal quality.

The results suggest that the proposed approach is feasible, showing potential for applications in contexts such as cybersecurity and mechanical event monitoring. The simplicity of the circuit and the use of readily available components make this approach suitable for researchers and technical enthusiasts.

Keywords: Mechanical Waves and Vibrations; Piezoelectric Sensors; Signal Acquisition and Analysis; Amplification Circuits; Microcontrollers.

LISTA DE FIGURAS

Figura 1 – Circuito de condicionamento	18
Figura 2 – Comparativo entre a amplificação simulada e a amplificação ensaiada .	19
Figura 3 – Sinal gerado e condicionado	21
Figura 4 – Comportamento DC do circuito amplificador simulado e ensaiado . . .	22
Figura 5 – Resposta do circuito amplificador para uma entrada senoidal em alta freqüência	23
Figura 6 – Resposta do circuito amplificador para uma entrada quadrada	24
Figura 7 – Ensaio do ruído de fundo	24
Figura 8 – Simulação de limites de tensão	25
Figura 9 – Croquis com auxílios visuais para a análise realizada em 2.1	29
Figura 10 – Comparativo entre métodos de captura de eventos	30
Figura 11 – Consumo energético para quatro circuitos	31

LISTA DE TABELAS

Tabela 1 – Tempos de detecção por microcontrolador	15
Tabela 2 – Relação de faixas de frequência com diferentes vulnerabilidades	16
Tabela 3 – Componentes utilizados no circuito	17
Tabela 4 – Croquis - Legenda	29

LISTA DE ABREVIATURAS E SIGLAS

ADC	Conversor Analógico-Digital
DMA	Direct Memory Access
RTC	Real Time Clock, modo mutualmente exclusivo ao DMA para ADC
sps	<i>samples per second</i> [Amostras por segundo]

SUMÁRIO

1	INTRODUÇÃO	9
1.1	OBJETIVOS	10
2	TRABALHOS RELACIONADOS	11
3	ANÁLISE DA VIABILIDADE DA AFERIÇÃO	13
3.1	ANÁLISE POR DIFERENCIAIS TEMPORAIS:	13
3.2	ANÁLISES FREQUENCIAIS	15
4	MATERIAIS E MÉTODOS	17
4.0.1	Sensores Piezoelétricos	17
4.1	CONDICIONAMENTO	17
4.1.1	Circuito Amplificador	17
4.1.2	Condicionamento de sinais	19
4.2	SOFTWARES UTILIZADOS	20
5	RESULTADOS E DISCUSSÃO	21
5.1	DOS SENSORES	21
5.2	DOS CIRCUITOS	22
5.3	DOS RUÍDOS	23
6	CONCLUSÃO	26
	Referências Bibliográficas	27
	APÊNDICE A – Croquis da Superfície de um Alvo Hipotético	29
	APÊNDICE B – Uso do osciloscópio nos ensaios	30
	APÊNDICE C – Consumo energético simulado	31
	APÊNDICE D – Ensaios do protótipo	32
	APÊNDICE E – Códigos de prototipagem	33
	ANEXO A – Modelo de AmpOp em SPICE	36

1 INTRODUÇÃO

Sensores piezoelétricos são transdutores amplamente utilizados em diversas aplicações devido à sua capacidade de converter vibrações mecânicas em sinais elétricos. No contexto de edificações, são empregados para detectar eventos estruturais, como variações de carga e fissuras¹. Na indústria, desempenham um papel importante no monitoramento de componentes mecânicos, como o afrouxamento de parafusos e porcas².

Além de aplicações técnicas, sensores piezoelétricos têm relevância na área artística, particularmente na lutheria, onde permitem a análise e ajuste da resposta acústica de instrumentos musicais de corda antes da finalização de sua construção³. Na área médica, são utilizados tanto como sensores biodegradáveis quanto como fontes de energia para o monitoramento de sinais vitais⁴.

No campo da segurança cibernética, sensores piezoelétricos podem ser explorados para ataques laterais, utilizando vibrações mecânicas como fonte de dados sigilosos. Ataques laterais⁵ são métodos que analisam emissões não intencionais de dispositivos, como consumo de energia ou vibrações, para extrair informações confidenciais⁶.

Este trabalho investiga o uso de sensores piezoelétricos do tipo pastilha em sistemas mecânicos, com o objetivo de condicionar sinais para que sejam processados por microcontroladores. Por meio de análises temporais e frequenciais, busca-se avaliar a viabilidade da detecção de eventos mecânicos, utilizando técnicas baseadas em ondas de Rayleigh. Os objetivos detalhados desta pesquisa são apresentados a seguir.

¹ (Jiao et al., 2020)

² (Gautschi, 2002)

³ (Rau, 2023)

⁴ (Panda et al., 2022)

⁵ Tradução nossa de *side-channel attacks*

⁶ (Koeune; Standaert, 2005)

1.1 OBJETIVOS

Propomos aplicar a flexibilidade dos sensores piezoelétricos para um contexto de segurança cibernética, investigando a possibilidade de utilizá-los como sensores em ataques laterais explorando o ruído mecânico gerado por diferentes atuações especialmente no contexto de botões e teclas. Para isso, estabelecemos as seguintes metas:

Acessibilidade

Desenvolver um dispositivo e método com baixo custo, fácil montagem e adaptação, que seja acessível a usuários comuns, entusiastas e pesquisadores em segurança cibernética.

Baixo custo e consumo energético

Reduzir o número de componentes e o consumo energético para que o dispositivo tenha longo tempo de atividade e seja econômico o suficiente para aplicações de uso único, considerando que o mesmo provavelmente não será recuperado após o uso.

2 TRABALHOS RELACIONADOS

Os ataques laterais têm recebido atenção crescente na literatura devido à sua capacidade de explorar informações indiretas para comprometer sistemas que, em tese, seriam seguros. Trabalhos nesta área têm analisado diversos meios de emanação, como variações no consumo de energia, emissão acústica e padrões de radiação eletromagnética, demonstrando vulnerabilidades em uma ampla gama de dispositivos.

No presente contexto, o uso de sensores piezoelétricos para captar vibrações mecânicas como um canal de informação em ataques laterais é um tema ainda pouco explorado. Estudos anteriores, como em A, B, C e D, concentraram-se na análise de sinais gerados por computadores e periféricos. Outros, como E, investigaram a extração de chaves criptográficas por variações de consumo energético.

Os trabalhos a seguir são exemplos de pesquisas que exploraram diferentes canais de informação em ataques laterais, demonstrando a viabilidade de comprometer sistemas de segurança por meio de vazamentos de informação.

(A)(Song; Wagner; Tian, 2001) - Timing analysis of keystrokes and timing attacks on SSH

Este trabalho demonstrou que é possível inferir o conteúdo de mensagens digitadas em um teclado por meio da análise do tempo entre as teclas pressionadas. Este trabalho foi realizado de forma totalmente remota, capturando pacotes SSH de uma rede e analisando o espaço de tempo entre uma tecla e outra. O trabalho foi realizado no domínio do tempo.

(B)(Backes et al., 2010) - Acoustic Side-Channel Attacks on Printers

Neste projeto os autores analisaram o som de impressoras matriciais, e por meio de análises espectrais aliadas a aprendizado de máquina puderam derivar o conteúdo dos documentos impressos com até 95% de certeza. Seus alvos trabalhavam entre 1 e 48 KHz, posteriormente concluíram que os dados de interesse estavam expostos à partir de 20kHz e que seria interessante filtrar as baixas frequências para evitar os ruídos gerados por atuadores de grande amplitude presentes nos dispositivos. Utilizaram hardwares de uso geral para captura e análise de dados.

(C)(Genkin; Shamir; Tromer, 2014) - RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis

Este trabalho extraiu chaves criptográficas de computadores analisando o som gerado pelos mesmos enquanto realizavam operações de criptografia. Analisaram frequências entre até 300 kHz e posteriormente observaram que até 100 kHz é uma faixa viável para este ataque. Utilizaram hardware de laboratório para a captura do som e posteriormente

postularam que é viável que o trabalho possa ser feito pelo microfone comum de um smartphone caso perto o suficiente.

(D)(Cheng et al., 2019) - SonarSnoop: active acoustic side-channel attacks

Este trabalho utilizou uma análise ativa por meio de sonar para inferir a posição de dedos na tela de um celular. Utilizaram frequências entre 18 e 20 khz e utilizaram o alto-falante e o microfone do próprio alvo para gerar a onda e captar o reflexo dela. Utilizaram um computador para a análise dos dados, utilizando aprendizado de máquina.

(E)(Gamaarachchi; Ganegoda, 2018) - Power Analysis Based Side Channel Attack

Este projeto analisou o ruído elétrico gerado no aterramento de microcontroladores enquanto realizavam trabalhos de criptografia, e por meio de análises espectrais e estatísticas puderam derivar as chaves de encriptação utilizadas. Seus alvos estavam na ordem de dezenas de Mhz. Utilizaram um osciloscópio e um computador para captura e análise de dados.

Os trabalhos apresentados demonstram a diversidade de canais laterais explorados para comprometer sistemas de segurança. No entanto, observa-se que a análise de vibrações mecânicas, especialmente por meio de sensores piezoelétricos, ainda é um campo inexplorado, com potencial para ampliar as possibilidades de ataque e monitoramento. Este estudo busca contribuir para esse campo, buscando caracterizar eventos vibracionais com maior precisão e eficiência.

3 ANÁLISE DA VIABILIDADE DA AFERIÇÃO

3.1 ANÁLISE POR DIFERENCIAIS TEMPORAIS DE DETECÇÃO:

Modelamos a propagação das ondas mecânicas em diferentes meios como ondas de Rayleigh, que se propagam na superfície de sólidos elásticos e têm suas velocidades regidas pela fórmula (1)¹:

$$v_R = \beta \cdot v_s \quad (1)$$

v_s sendo:

onde:

- v_R : velocidade de propagação das ondas de Rayleigh.
- β : fator de correção, que depende da relação de Poisson ν , $\beta \approx 0,87$ para a maioria dos sólidos.
- v_s : velocidade de propagação das ondas cisalhantes (2).

$$v_s = \sqrt{\frac{\mu}{\rho}} \quad (2)$$

onde:

- μ : módulo de cisalhamento (ou de elasticidade transversal) do material.
- ρ : densidade do material.

Assumindo um dispositivo embarcado hipotético de formato trapezoidal com base inferior medindo 42 por 27 centímetros, altura de 15 centímetros e base superior de 42 por 13 centímetros, com quatro de seus vértices conectando arestas em ângulos retos e com os botões atuadores na metade direita da face angulada, maquinado de chapas de aço dobradas com espessura pequena, de modo a desprezar os efeitos tridimensionais da propagação das ondas e calcular o tempo que uma onda levaria para chegar até um par de sensores instalados em diferentes pontos de sua superfície, na esperança de poder identificar um botão específico pela diferença de tempo de detecção da onda pelos diferentes sensores.

Melhor caso:

Os valores utilizados para o aço 310² em temperatura ambiente foram os seguintes:

- $\rho \approx 7,83 \text{ g/cm}^3$
- Módulo de Young = 190,3 GPa nos leva a $\mu \approx 73,2 \text{ GPa}$

Encontramos a $v_s \approx 3 \text{ km/s}$ e subsequentemente $v_R \approx 2,65 \text{ km/s}$ Considerando a melhor hipótese de aferição da diferença de tempo entre a detecção da onda por dois sensores em pontos opostos da superfície do dispositivo, os sensores estariam nos vértices da base inferior do dispositivo, um logo abaixo do teclado e outro na diagonal oposta. Esta con-

¹ (Rayleigh, 1885)

² (Lide, 2004)

figuração maximiza a distância entre os sensores, aumentando a diferença de tempo de detecção da onda entre eles e facilitando a identificação do botão atuado.

No cenário ideal, considera-se que um atuador esteja localizado exatamente acima do vértice proporcionando uma detecção instantânea por um dos sensores, a diferença de tempo de detecção seria o tempo de propagação da onda entre as diagonais inferiores do dispositivo, resolvendo para o tempo:

$$t = \frac{\sqrt{(0,42)^2 + (0,27)^2}}{2,65 \times 10^3} \approx 0,188\mu s$$

Veremos na secção de materiais e métodos os clocks e as taxas de amostragem dos diferentes microcontroladores que desejamos que atendam o projeto, os arduinos levam 13 ciclos de clock por bit por conversão, considerando o clock em 16MHz, temos 8,125 microssegundos por conversão para seus 10 bits, o ESP32 tem 12 bits de resolução e 200ksps, o que nos dá 5 microssegundos por conversão sem o uso de DMA, o que é suficiente para a detecção de um botão mesmo no pior dos casos de velocidade de conversão, o tempo de leitura ainda é ordens de grandeza mais rápido do que o tempo de propagação da onda.

Pior Caso:

O pior caso considerado ocorre quando o atuador está localizado no centro da aresta de conexão entre a face angulada e a base superior.

Inicialmente calcularemos a menor distância entre o atuador e cada um dos sensores, para isto “abriremos” as chapas metálicas³ e aplicaremos a fórmula da distância entre dois pontos no plano cartesiano, onde o sensor mais distante da face angulada estaria na origem, o sensor que desprezamos a distância do atuador anterior estará no ponto (0,42;-0,27) e o atuador analisado estará no ponto (0,21;-0,48) para efeito de análise do sensor mais próximo a ele, enquanto o atuador poderá ser considerado em três posições diferentes devido aos diferentes caminhos em que a onda poderá viajar na superfície tridimensional⁴, sendo estes pontos (-0,29;-0,27), (0,21;-0,48) e (0,21;0,28).

Calculando a distância entre os pontos, temos para o sensor mais próximo 29,36cm e para o sensor mais distante temos as distâncias 39,62 cm, 52,39 cm e 35 cm, respectivamente. Para os cálculos, utilizou-se o caminho de 35 cm pela traseira do dispositivo, que é o menor dos três e o mais relevante para inviabilizar a análise. Utilizando a velocidade encontrada de 2650 m/s⁵, temos para o sensor mais próximo um tempo de propagação de 111 μs e para o sensor mais distante 132 μs , o que nos dá um tempo de conversão necessário de

³ Um croquis da superfície do trapezóide desmontado está nos apêndices (A), para auxílio de visualização.

⁴ Não consideraremos efeitos de autointerferência nesta análise, mas num caso prático a autointerferência poderia ser desejável pois geraria frequências de ressonância diferentes para cada posição de atuação, podendo assim fortalecer os métodos frequenciais que serão abordados à frente.

⁵ Para simplicidade analítica, consideraremos a propagação como puramente uma onda de Rayleigh, ainda que o fenômeno inclua ondas de cisalhamento devido às mudanças de direção da propagação.

no máximo 21 μs , ainda estando dentro das especificações de todos os microcontroladores objetivados, e com uma margem de segurança considerável.

Distância Limítrofe Para Inviabilidade da Detecção:

A menor distância entre pontos de atuação foi calculada para determinar o limite no qual a diferença de tempo de propagação se torna inferior ao tempo de conversão do microcontrolador mais rápido. Neste caso, analisaremos o conversor do ESP32 no modo DMA, com ⁶2Msps, o que nos dá um tempo de conversão de 0,5 μs , multiplicando este valor pela velocidade de 2650 m/s, encontramos a distância máxima de 1,325mm, o que é fisicamente inviável para qualquer aplicação prática.

A análise dos casos⁷ resultou na tabela abaixo:

μC	Modo	Tempo de Conversão(μs)	Distância Mínima(mm)
ESP32	DMA (2 Msps)	0,5	1,325
ESP32	RTC (200 ksps)	5	13,25
Arduino	16 MHz, 10 bits	8,125	21,5

Tabela 1 – Tempos de detecção por microcontrolador e suas respectivas distâncias mínimas para detecção.

Entre os itens analisados, apenas o Arduino em alta resolução poderia ser inviabilizado em aplicações práticas. No entanto, mesmo nesse caso, a distância máxima de pouco mais de 2 cm é pequena no contexto de sistemas embarcados projetados para detectar eventos mecânicos gerados por pessoas.

3.2 ANÁLISES FREQUENCIAIS:

Segundo (Main, 1993), uma onda sinusoidal $\psi_i(z, t) = A_i \cos(\omega t - k_i r)$, onde ψ é a quantidade de pressão acústica ou força de um campo elétrico, z é uma representação da fase que deve ser constante durante toda a duração da onda no meio, t é o tempo, A a amplitude, k o vetor direção da onda e r é a medida da posição de um ponto na frente de onda, ao incidir sobre uma borda de superfície se decompõe em duas outras ondas, ψ_r e ψ . Essas representam, respectivamente, as ondas refletidas de volta ao meio original e transmitidas ao novo meio. Considera-se que o ponto de incidência seja perfeitamente plano e de área infinita para os efeitos de interferência, com valores $\psi_r = A_r \cos(\omega t - k_r r)$ e $\psi = A \cos(\omega t - kr)$. Podemos observar que as novas ondas podem ter fases distintas da onda original, mas se mantêm constantes enquanto estiverem dentro do novo meio.

Com base nessa análise, observa-se que uma onda de pressão mecânica pode ser convertida em uma onda de pressão atmosférica (sonora) de forma determinística e vice-versa. Dessa forma, podem ser aplicados métodos já consolidados no campo da criptoanálise acústica

⁶ (ESPRESSIF SYSTEMS, s.d.)

⁷ (Arduino AG., s.d.[a])(Arduino AG., s.d.[b])

para analisar os sinais coletados. A depender da qualidade dos sensores e seus circuitos de condicionamento e sua capacidade de absorção de vibrações de diferentes frequências, diferentes métodos de ataques podem ser aplicados^{8,9,10}, exemplos são:

Faixa de Frequência	Vulnerabilidade
$f < 10$ kHz	Inferência de teclas pelas emanações acústicas da digitação
20 kHz $< f < 50$ kHz	Captura do conteúdo impresso por impressoras matriciais
10 kHz $< f < 100$ kHz	Sequestro de chaves criptográficas pelas emanações acústicas de elementos eletrônicos

Tabela 2 – Relação de faixas de frequência com diferentes vulnerabilidades

O meio altamente rígido em relação ao ar no qual os sensores estarão ancorados oferece benefícios significativos, como baixa absorção e perda de ondas em altas frequências, o que nos leva a crer que a criptoanálise em meios mecânicos possa ter uma eficácia até maior do que a criptoanálise acústica, pois o ar por ser altamente compressível leva a uma grande atenuação dos sinais em alta frequência sendo este o fator determinante na determinação de onde interromper a captura de dados em trabalhos anteriores¹⁰.

Dado o objetivo de alta acessibilidade estabelecido no início do projeto, foram utilizados sensores piezoelétricos genéricos e amplificadores de uso geral nos circuitos de condicionamento. Por esse motivo, o escopo desta análise foi limitado às faixas de frequências audíveis, limitando-nos às inferências por emanações acústicas.

⁸ (Song; Wagner; Tian, 2001)

⁹ (Backes et al., 2010)

¹⁰ (Genkin; Shamir; Tromer, 2014)

4 MATERIAIS E MÉTODOS

4.0.1 Sensores Piezoelétricos

Neste trabalho, foram utilizados sensores piezoelétricos do tipo pastilha, escolhidos por sua simplicidade, acessibilidade e custo reduzido, em alinhamento com os objetivos do projeto. O efeito piezoelétrico, descoberto por Pierre e Jacques Curie em 1880, é a capacidade de certos materiais de gerar uma diferença de potencial elétrico quando submetidos a pressões mecânicas¹. Essa propriedade permite a detecção de vibrações mecânicas em sistemas de estudo e é a base para o funcionamento dos sensores aplicados. Devido à ausência de datasheets dos sensores, foram realizados ensaios e modelagens para determinar seus parâmetros essenciais com maior precisão.

4.1 CONDICIONAMENTO

4.1.1 Circuito Amplificador

O circuito amplificador foi projetado para ajustar os sinais dos sensores às faixas de tensão permitidas pelos microcontroladores ($[0;5]$ V para Arduino e $[0;3,3]$ V para ESP32). A configuração do circuito desloca a referência do sinal para o centro da faixa de tensão de entrada e reduz sua amplitude para evitar saturação, preservando as características da onda original. Os componentes utilizados no circuito são apresentados na Tabela 3.

Tabela 3 – Componentes utilizados no circuito

Componente	Descrição	Função no Circuito
Sensores Piezoelétricos	Pastilhas genéricas sem <i>datasheets</i>	Geração de sinais vibracionais
Amplificador Operacional TL074	Amplificador operacional JFET	Condicionamento do sinal
Resistores	Valores variados	Ajuste da tensão
Microcontroladores	Arduino Mega e ESP32	Aquisição e processamento dos sinais

Inicialmente, o circuito foi simulado no software KiCad e, posteriormente, prototipado em placas de prototipagem pré-perfuradas para testes. O desempenho foi validado com um osciloscópio, conforme apresentado na Figura 1, onde o comportamento do circuito foi comparado entre simulações e ensaios experimentais. O apêndice D apresenta os resultados dos ensaios realizados com o protótipo do circuito.

A escolha dos componentes segue o objetivo de manter o custo reduzido e possibilitar a replicação do experimento por outros pesquisadores e entusiastas. Diversas configurações de circuitos amplificadores atendem às exigências do projeto. Optou-se por uma configuração não inversora com o amplificador operacional TL074², escolhido por seu baixo ruído³, custo acessível e encapsulamento quádruplo, que permite conectar até

¹ (Arnau Vives, 2004)

² Este amplificador pode ser substituído pelo TL084 com praticamente nenhuma alteração no comportamento do circuito

³ (Texas Instruments, 2011)

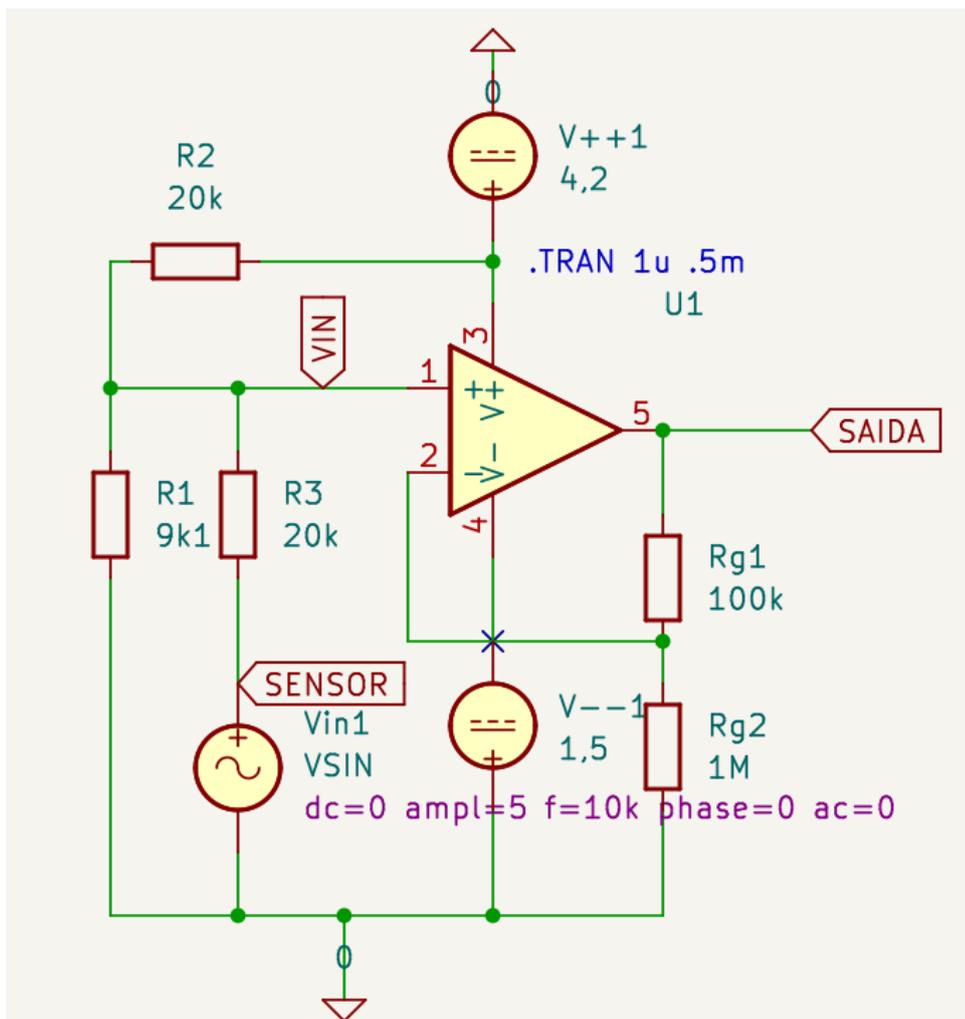


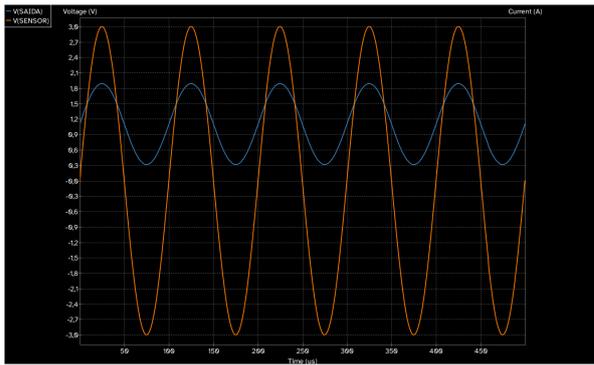
Figura 1 – Esquemático do circuito amplificador projetado para o condicionamento de sinais piezoelétricos. O circuito na configuração somador não-inversor ajusta a tensão para compatibilidade com os microcontroladores e protege contra sobretensão positiva e negativa, enquanto mitiga a saturação.

quatro sensores em um único chip. O fenômeno de saturação do amplificador foi utilizado para limitar a saída do circuito⁴, sendo esta a única proteção contra sobretensão nas entradas analógicas dos microcontroladores. Diodos Schottky em combinação com diodos Zener podem ser usados para proteção adicional, mas optou-se por não utilizá-los para manter o baixo número de componentes e a simplicidade do circuito.

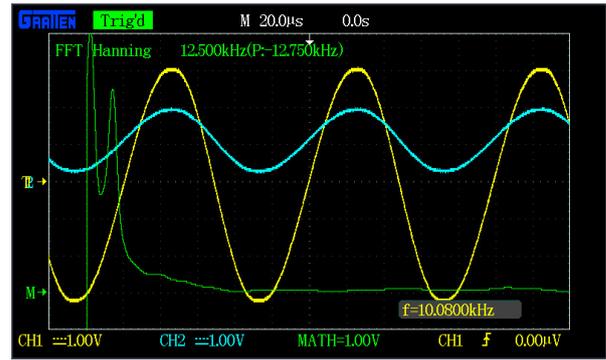
A placa Arduino Mega possui algumas opções para referência analógica⁵. Utilizando a referência de 2,56 V, é possível obter uma resolução de 2,5 mV por passo. Escolhemos esta referência porque, além de ser mais sensível para pequenas variações, está bem próxima da tensão de operação da placa ESP32. Isso permite o uso do mesmo circuito para ambas as placas. O ESP32, com seus 12 bits de resolução, oferece 0,8 mV por passo, embora aproximadamente 23% de sua amplitude de entrada seja podada no caso de

⁴ observável na simulação em 8

⁵ (Arduino AG., s.d.[a])



(a) Simulação em Kicad com uma onda senoidal de 10kHz com amplitude de 3 V para o sinal do sensor.



(b) Ensaio com uma onda senoidal de 10 kHz com amplitude de 3 V para o sinal do sensor. Entrada em amarelo e saída em azul.

Figura 2 – Comparativo entre a amplificação simulada e a amplificação ensaiada. Observa-se comportamento semelhante entre os sinais simulados e os sinais reais. A similaridade dos comportamentos valida a precisão da simulação.

reaproveitamento do circuito⁶.

4.1.2 Condicionamento de sinais

O método de processamento determina o número de sensores necessários. Para análises frequenciais, é necessário um único sensor, enquanto sensores adicionais oferecem maior redundância e resolução. Para análises temporais, ao menos dois sensores são necessários. Recomendamos utilizar os quatro sensores disponíveis sempre que possível, pois o chip dispõe de portas suficientes e os microcontroladores selecionados suportam este número de entradas analógicas.

É importante destacar que o condicionamento de sinais é um processo delicado e a qualidade do sinal obtido depende de vários fatores, como a qualidade do sensor, a qualidade do circuito de condicionamento e a conformidade das entradas com as especificações técnicas. Sinais fora das especificações podem resultar em perda de dados ou danos ao circuito de condicionamento. Estas entradas são particularmente sensíveis a sinais negativos, com margens de erro muito restritas. Portanto, é crucial ajustar cuidadosamente a fonte negativa do circuito da etapa anterior.

Caso um usuário deseje explorar métodos além dos baseados em emanações acústicas, recomendamos o uso de blindagens eletromagnéticas em todas as etapas do processo, dada a sensibilidade a frequências elevadas. Além disso, circuitos de condicionamento individuais para cada sensor, equipados com filtros passa-banda, podem ser adicionados, dedicando cada entrada a uma faixa específica de frequências. A necessidade de blindagem e os limites do circuito projetado de condicionamento serão discutidos em detalhes na

⁶ A amplitude da onda de saída pode ser ajustada pelas tensões de alimentação do amplificador, tomadas as devidas precauções para evitar a sobretensão e ajustar a nova referência de onda, que depende da relação entre R1 e R2.

seção de resultados.

4.2 SOFTWARES UTILIZADOS

Para a realização deste trabalho, foi utilizado um computador com as seguintes especificações: processador Intel i5-9600KF com 6 núcleos a 4,6 GHz, 32 GB de memória RAM e sistema operacional baseado em Debian Sid, arquitetura x86_64, executando os kernels Linux 6.6.6 a 6.9.10. A interface gráfica empregada foi KDE Plasma 5, com gerenciador de janelas KWin. Foram utilizados nele diferentes softwares, cada um com um propósito específico, conforme descrito abaixo:

Visual Studio Code (VSCode)

O Visual Studio Code foi utilizado como ambiente de desenvolvimento integrado (IDE) para a escrita e organização do código fonte do projeto. Inicialmente, extensões para programar tanto os Arduinos quanto o ESP32 estavam disponíveis no VSCode. Contudo, a extensão para o Arduino foi descontinuada durante o projeto, exigindo a migração dos trabalhos com Arduinos para o Arduino IDE.

KiCad

O software KiCad foi empregado para o projeto e simulação dos circuitos utilizados no condicionamento dos sinais, como o ilustrado na figura 1. Suas funcionalidades permitiram a criação de esquemáticos detalhados e simulação do comportamento do circuito amplificador. Por meio de seus simuladores SPICE puderam ser feitos ajustes precisos no circuito antes da prototipagem, garantindo maior eficiência no desenvolvimento⁷.

Arduino IDE

O Arduino IDE foi utilizado para programação, configuração e testes de microcontroladores Arduino empregados no projeto após a descontinuidade da extensão para o VSCode.

⁷ Os códigos para as simulações do comportamento dos circuitos estão no anexo E

5 RESULTADOS E DISCUSSÃO

5.1 DOS SENSORES

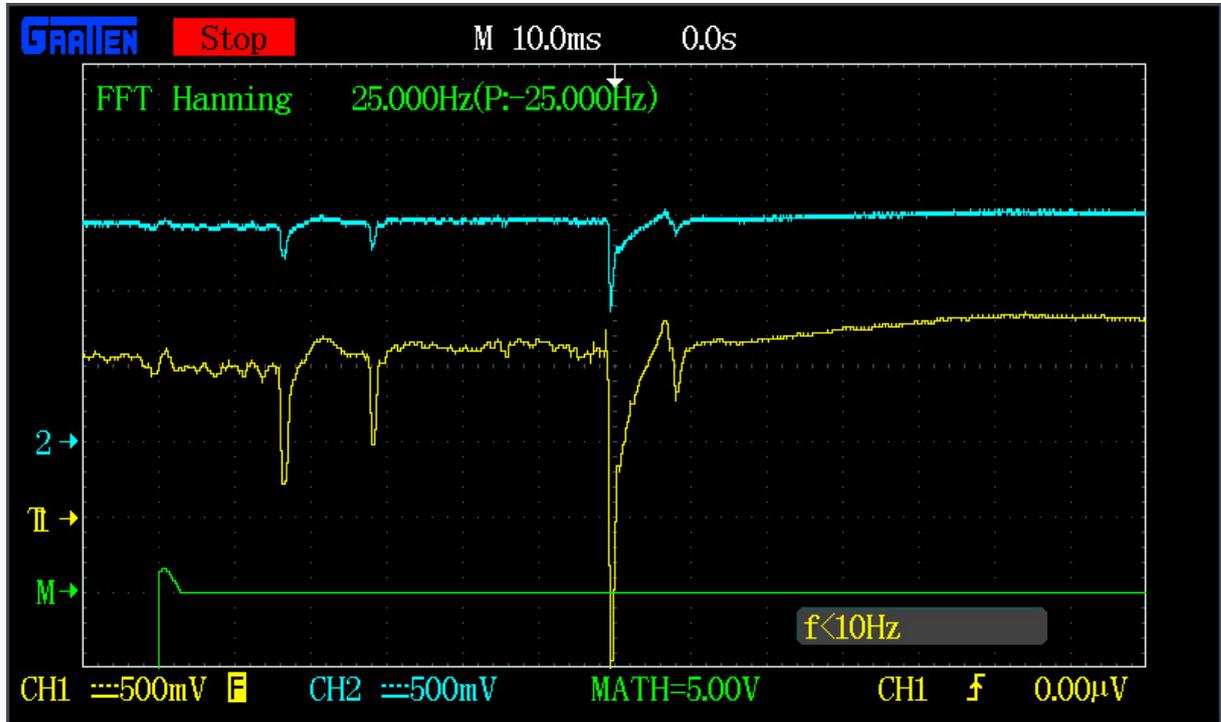


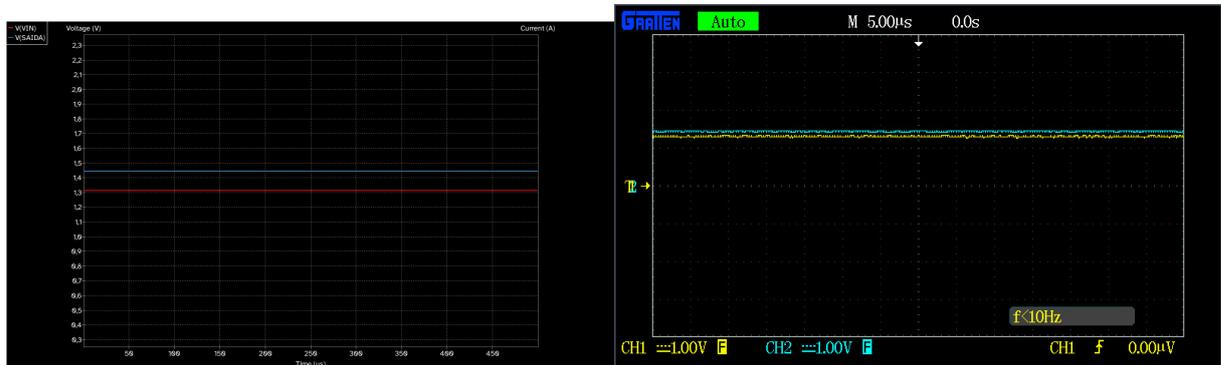
Figura 3 – Sinal capturado[1] (Sinal do sensor em malha fechada.) e condicionado[2]. Observamos a atenuação do pico de tensão enquanto a forma da onda é preservada. Esta atenuação é necessária para a proteção dos microcontroladores.

A qualidade dos sinais coletados depende significativamente da ancoragem dos sensores. Apesar de serem acessíveis e disponíveis, os sensores em formato de pastilha apresentam desafios para acoplamento confiável às superfícies. Acoplamento este que após revisão da bibliografia se mostrou pivotal, visto que o sinal é gerado por excitações mecânicas da ordem de micrômetros a ângstrons¹, qualquer elasticidade existente em fitas dupla-face comprometerá a leitura. Sugere-se a utilização de poliuretano rígido com suporte e mola de rigidez adequada² para manter o contato confiável entre o sensor e a superfície alvo ou um material de rigidez menos exagerada de geometria especializada para esta aplicação específica, muito provavelmente na forma de quasi-esfera, de forma a manter o sensor em contato com a superfície pode ser uma solução para manter a viabilidade de sensores não-especializados.

¹ (Gautschi, 2002) inclusive cita um dos usos destes mesmo sensores por conta de sua capacidade de deslocamento linear de forma determinística nestas ordens de magnitude como atuadores para calibração de dispositivos que necessitem de extrema precisão, um dos exemplos citados sendo microscópios atômicos

² Necessária uma constante elástica na ordem de 5 kN/m para manter a frequência natural baixa o suficiente para não entrar em ressonância com as frequências de interesse.

5.2 DOS CIRCUITOS



(a) Comportamento DC do circuito simulado (b) Ensaio DC do protótipo do circuito

Figura 4 – Comportamento DC do circuito amplificador. A tensão de saída ensaiada está em conformidade com os valores projetados. Notam-se serrilhados atribuídos a ruídos de alta frequência, mesmo com o filtro ativo do osciloscópio configurado. Esses ruídos apresentam baixa amplitude e não interferem nas amplitudes e frequências de interesse. Para uma análise mais detalhada sobre os ruídos, consultar a Seção 5.3.

O circuito amplificador projetado mostrou-se eficiente para aplicações nas faixas audíveis de frequência. A saturação do amplificador operacional foi suficiente para proteger os microcontroladores contra sobretensão. O consumo energético foi satisfatório, com cada amplificador consumindo menos de 20 mW durante a operação^C. Com ajustes nos circuitos para centralizar a referência no intervalo de entrada, é possível alimentá-los diretamente pelas portas de tensão dos microcontroladores, que variam de 500 a 1500 mW. A amplificação foi suficiente para aquisição de sinais de amplitude de levemente acima de 5 volts e os traduzir com fidelidade aceitável para a amplitude de menos de 1,5 volts imposta pelo projeto.

Circuitos mais complexos e sem as restrições autoimpostas podem beneficiar-se de proteção extra por meios de diodos schottky e zenner para mais uma camada de proteção contra sobretensões positiva e negativa; pode-se também utilizar um número maior de sensores e geometrias variadas aliados a filtros passa-banda de modo a cada conjunto analisar uma faixa específica de frequências com maior especialização.

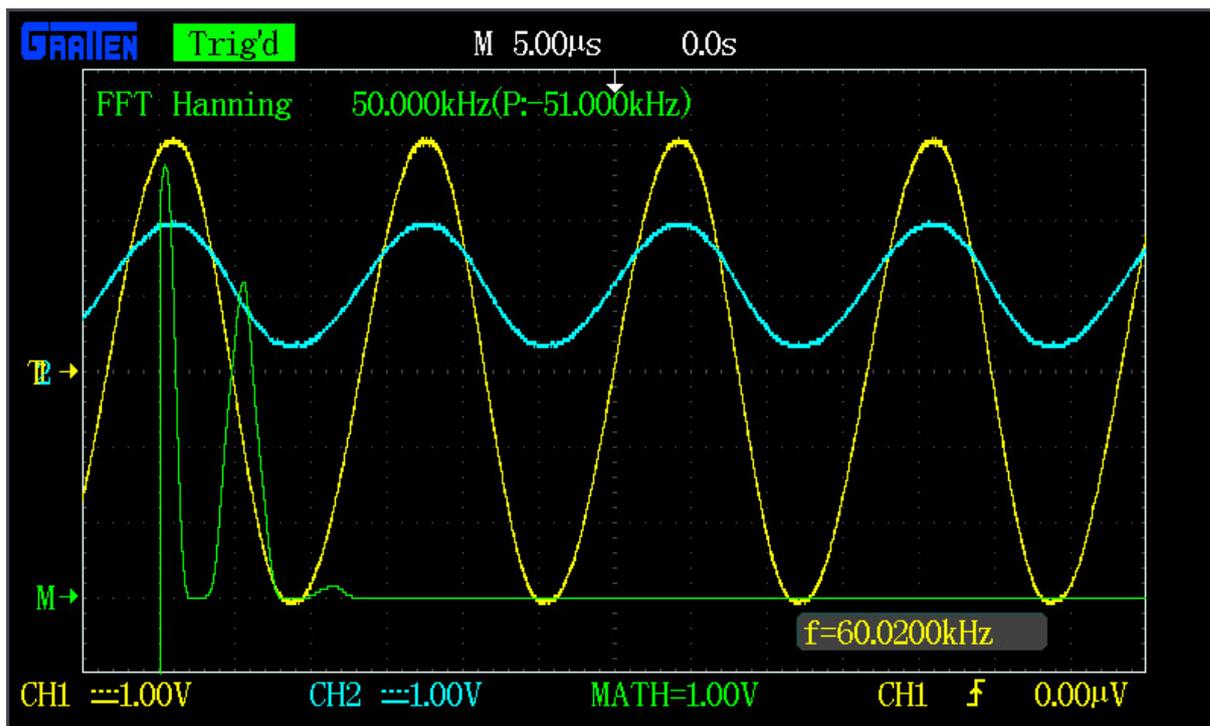


Figura 5 – Resposta do circuito amplificador para uma entrada senoidal de 60 kHz com $6 V_{pp}$. Observa-se que esta frequência está próxima ao limite de operação do circuito pela iminência de distorções nos picos da saída, em azul.

5.3 DOS RUÍDOS

Os ensaios revelaram a presença de ruídos, observados como serrilhados nas ondas capturadas. Na Figura 7, uma FFT (em verde) ilustra a análise da saída do circuito em repouso. A ordem da amplitude dos ruídos é da ordem de unidades de mV, mas estão presentes em todas as faixas de frequência. Estes ruídos foram considerados insignificantes para as ordens de grandeza definidas pelos objetivos do projeto.

Caso trabalhos futuros trabalhem em ordens maiores de frequências onde o sinal de interesse muito provavelmente seria dramaticamente atenuado, recomendamos o uso de blindagens tanto no cabeamento quanto nos circuitos e nas fontes. Destacamos que filtros capacitivos ou indutivos muito provavelmente interferirão no comportamento do circuito.

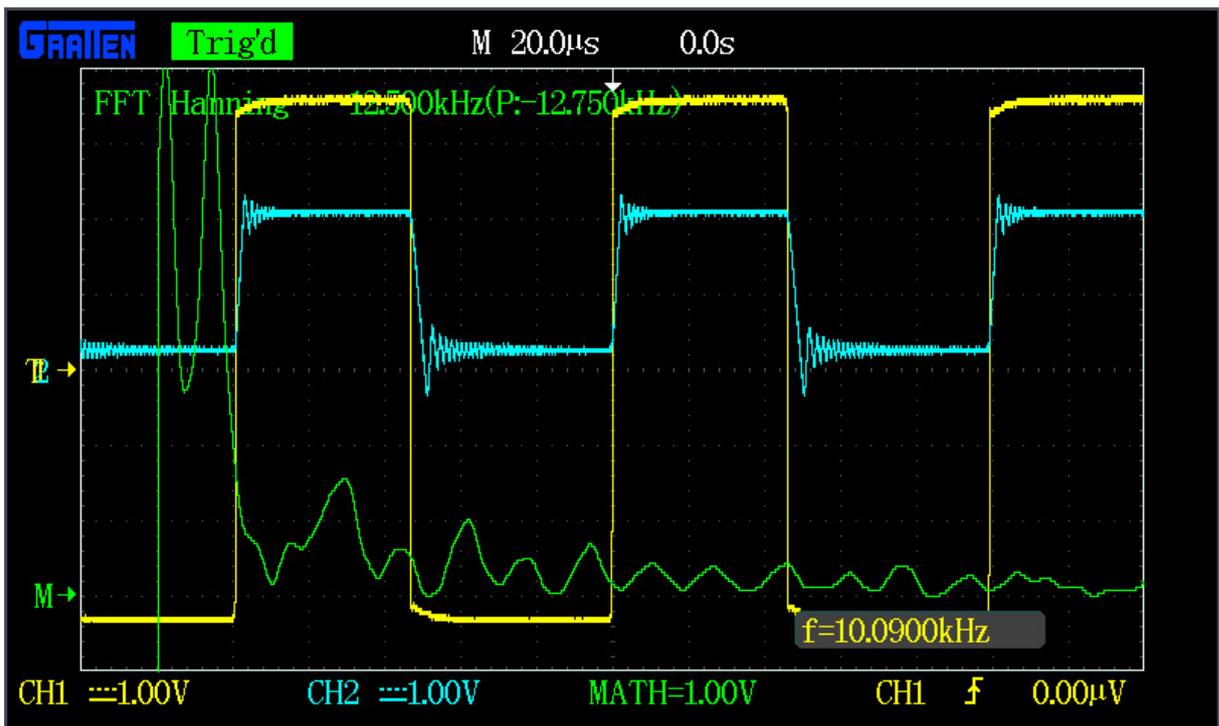


Figura 6 – Resposta do circuito amplificador para uma entrada quadrada de 10 kHz com 5 V_{pp} . Nota-se que dos 7 V_{pp} de entrada, temos ligeiramente acima de 2 V_{pp} na saída. Pode-se também observar o comportamento transitório do circuito amplificador.

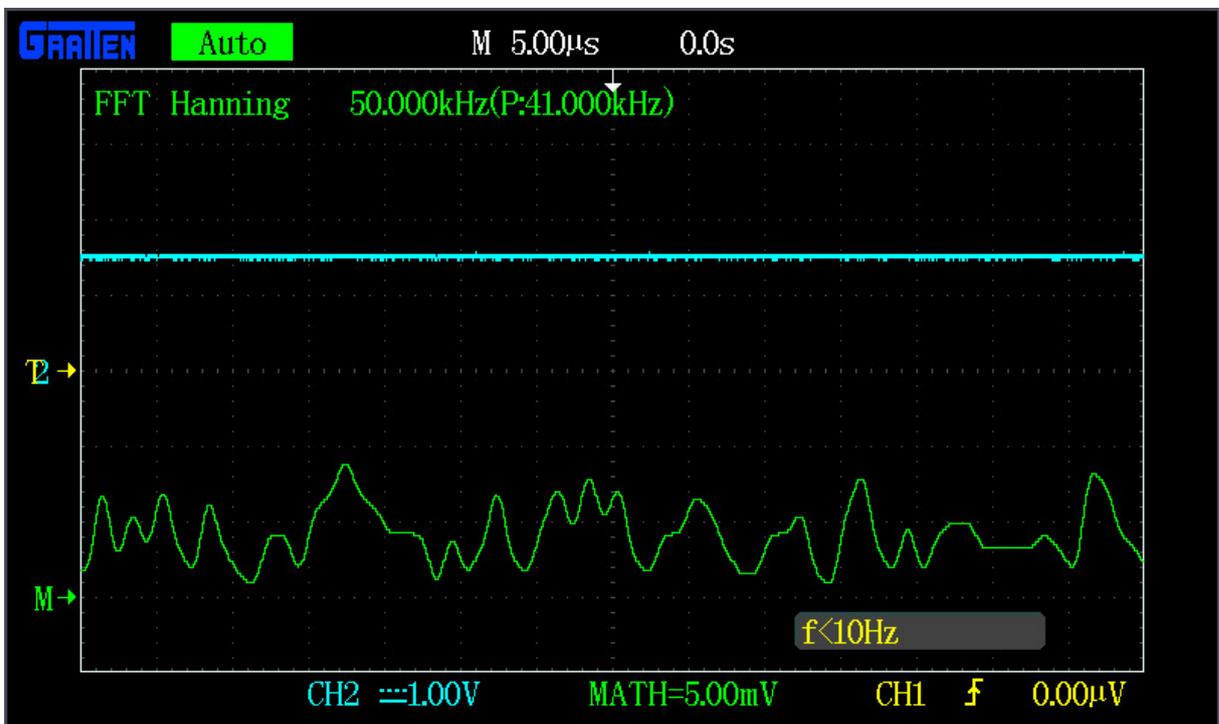


Figura 7 – Ensaio do ruído de fundo. Da FFT (em verde) nota-se a inexorabilidade do ruído em todas as faixas de frequência e a amplitude diminuta do mesmo. A pequena amplitude não é relevante para as faixas de trabalho analisadas.

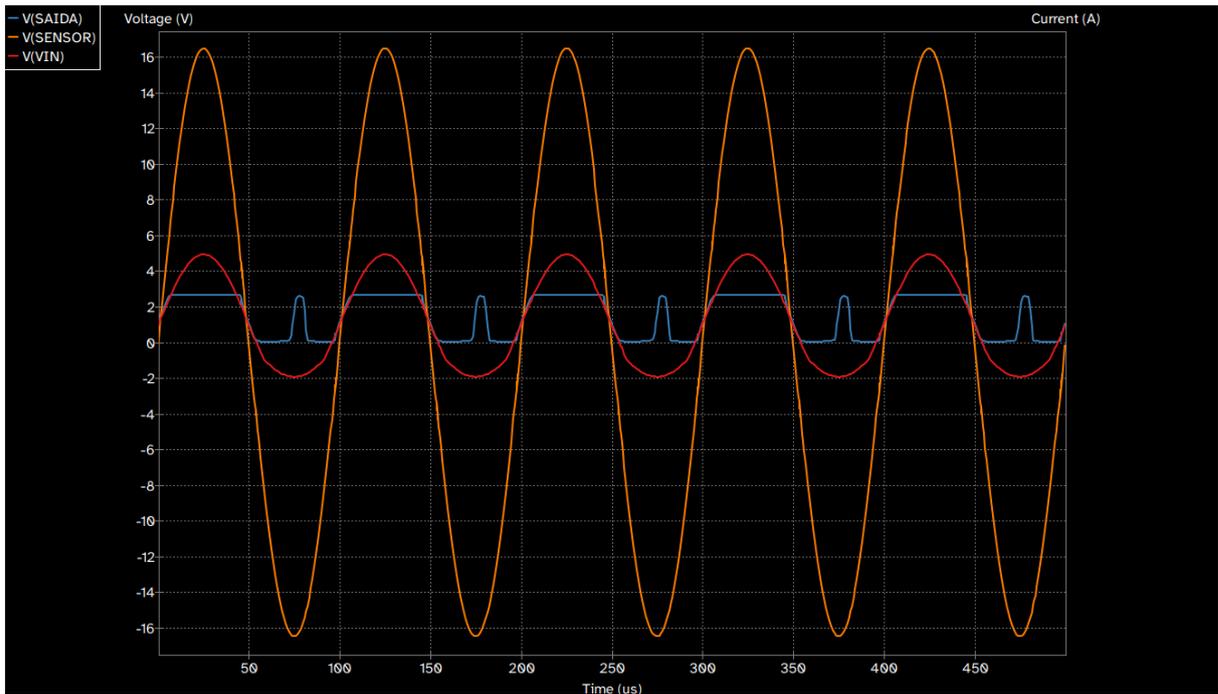


Figura 8 – Simulação de limites de amplitude do Circuito. Observamos que teóricamente a saturação é suficiente para proteger o controlador e em tensões de entradas abaixo de -16V, abaixo do ponto de falha do AmpOp, a saída ainda é compatível com a entrada do microcontrolador, mas gera-se leituras errôneas. Estas amplitudes não são esperadas em aplicações reais.

6 CONCLUSÃO

O circuito amplificador projetado demonstrou viabilidade para a aplicação proposta, atendendo às limitações definidas e apresentando consumo energético abaixo de 17 mW por amplificador. Embora o sensor escolhido apresente desafios para ancoragem, sua disponibilidade, seu desempenho e baixo custo atenderam os objetivos propostos. Os dispositivos se mostraram capazes de realizar as transformadas matemáticas em tempo de execução, mas a eficiência energética e a capacidade de processamento dos microcontroladores utilizados ainda precisam ser avaliadas. A argumentação teórica requer validação prática. Ainda assim, a proposta apresenta potencial para aplicações práticas, podendo servir como ferramenta para pesquisadores e entusiastas em criptoanálise, especialmente no contexto de ataques laterais. Se comprovada eficaz, a teoria proposta tem o potencial de abrir um novo campo de estudo na criptoanálise: a criptoanálise mecânica.

REFERÊNCIAS BIBLIOGRÁFICAS

ARDUINO AG. **Arduino Mega ADK Rev3**. [S. l.]. Acesso em 01-11-2024. Disponível em: <https://docs.arduino.cc/retired/boards/arduino-mega-adk-rev3/>.

ARDUINO AG. **Arduino Uno Rev3 with Long Pins**. [S. l.]. Acesso em 01-11-2024. Disponível em: <https://docs.arduino.cc/retired/boards/arduino-uno-rev3-with-long-pins/>.

ARNAU VIVES, A. (ed.). **Piezoelectric Transducers and Applications**. [S. l.]: Springer, 2004.

BACKES, Michael; DÜRMUTH, Markus; GERLING, Sebastian; PINKAL, Manfred; SPORLEDER, Caroline. Acoustic Side-Channel Attacks on Printers. *In: USENIX Security Symposium*. [S. l.: s. n.], 2010. Acesso em 01-11-2024. Disponível em: <https://api.semanticscholar.org/CorpusID:17532291>.

CHENG, P.; BAGCI, I. E.; ROEDIG, U.; YAN, J. SonarSnoop: active acoustic side-channel attacks. **International Journal of Information Security**, 2019.

ESPRESSIF SYSTEMS. **ESP32 Datasheet**. [S. l.]. Acesso em 01-11-2024. Disponível em: https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf.

GAMAARACHCHI, Hasindu; GANEGODA, Harsha. **Power Analysis Based Side Channel Attack**. [S. l.: s. n.], 2018. arXiv: [1801.00932](https://arxiv.org/abs/1801.00932) [cs.CR]. Disponível em: <https://arxiv.org/abs/1801.00932>.

GAUTSCHI, G. **Piezoelectric Sensorics**. [S. l.]: Springer, 2002.

GENKIN, Daniel; SHAMIR, Adi; TROMER, Eran. RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis. *In: PROCEEDINGS of the CRYPTO 2014, Part I*. [S. l.]: Springer, 2014. v. 8616. (Lecture Notes in Computer Science), p. 444–461.

JIAO, P.; EGBE, K.-J. I.; XIE, Y.; MATIN NAZAR, A.; ALAVI, A. H. Piezoelectric Sensing Techniques in Structural Health Monitoring: A State-of-the-Art Review. **Sensors**, v. 20, n. 13, p. 3730, 2020.

KOEUNE, F.; STANDAERT, F. X. A Tutorial on Physical Security and Side-Channel Attacks. *In: ALDINI, A.; GORRIERI, R.; MARTINELLI, F. (ed.). Foundations of Security Analysis and Design III*. [S. l.]: Springer, Berlin, Heidelberg, 2005. v. 3655. (Lecture Notes in Computer Science). Disponível em: https://doi.org/10.1007/11554578_3.

LIDE, David R. (ed.). **CRC Handbook of Chemistry and Physics**. 85th. [S. l.]: CRC Press, jun. 2004.

MAIN, Iain G. **Vibrations and Waves in Physics**. 3rd. Cambridge, UK: Cambridge University Press, 1993. ISBN 0521441862.

PANDA, Swati; HAJRA, Sugato; MISTEWICZ, Krystian; IN-NA, Pichaya; SAHU, Manisha; RAJAITHA, P. Mary; KIM, Hoe Joon. Piezoelectric energy harvesting systems for biomedical applications. **Nano Energy**, v. 100, p. 107514, 2022. ISSN 2211-2855.

RAU, Mark Gregory. **Vibration and Acoustic Measurements of Guitars with Applications to Luthiery Synthesis and Audio Effects**. 2023. Tese (Doutorado) – Stanford University. Acesso em 21-10-2024. Disponível em: <https://purl.stanford.edu/kx813bh3027>.

RAYLEIGH, Lord. On Waves Propagated along the Plane Surface of an Elastic Solid. **Proceedings of the London Mathematical Society**, s1-17, n. 1, p. 4–11, 1885.

SONG, Dawn Xiaodong; WAGNER, David; TIAN, Xuqing. Timing analysis of keystrokes and timing attacks on SSH. *In*: PROCEEDINGS of the 10th Conference on USENIX Security Symposium - Volume 10. Washington, D.C.: USENIX Association, 2001. (SSYM'01).

TEXAS INSTRUMENTS. **TL072-EP, TL074-EP: Low-Noise JFET-Input Operational Amplifier**. SLOS747F. Dallas, out. 2011. Acesso em 01-11-2024. Disponível em: <https://www.ti.com/lit/ds/symlink/tl074-ep.pdf?ts=1730919018034>.

APÊNDICE A – Croquis da Superfície de um Alvo Hipotético

O croquis da superfície de um alvo hipotético descrito em 3 “desmontado” e com a face angulada duplicada para efeitos de análise de caminhos alternativos é apresentado na Figura 9:

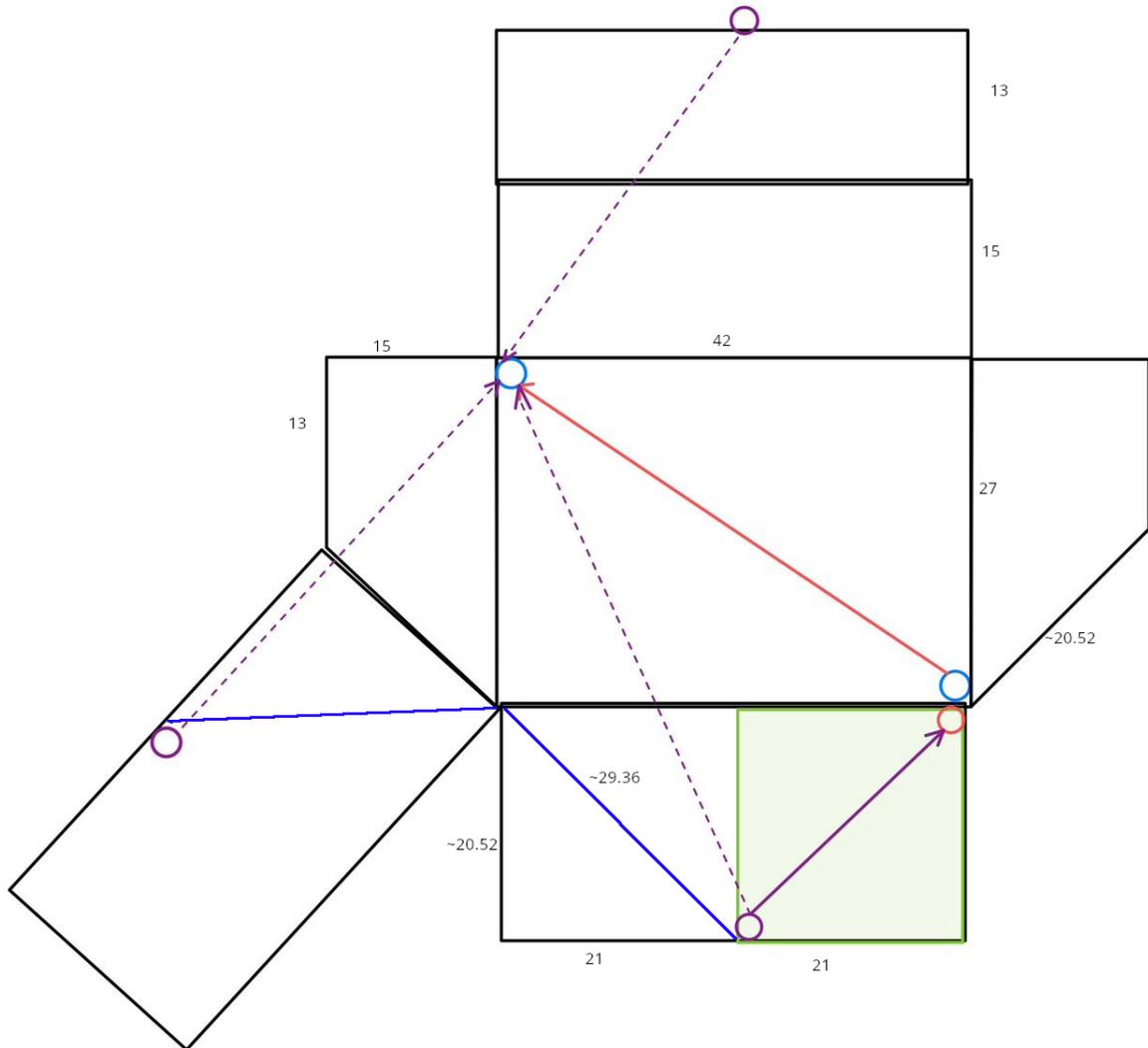


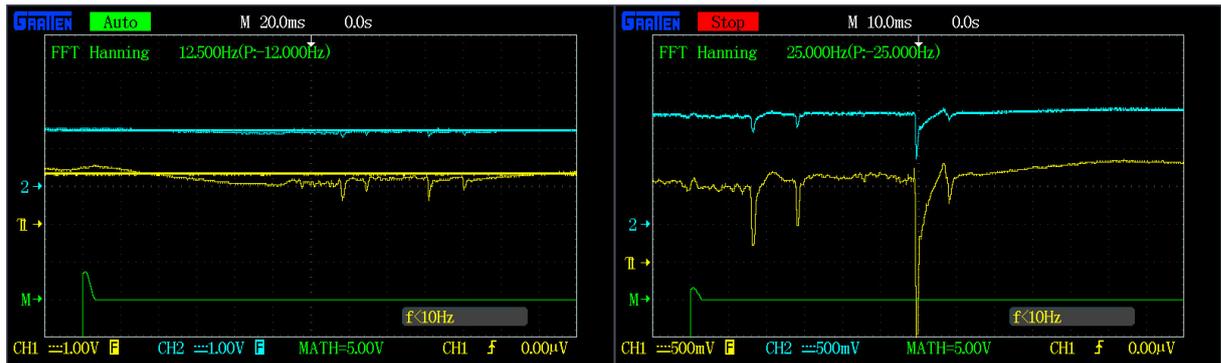
Figura 9 – Croquis com auxílios visuais para a análise realizada em 2.1

Tabela 4 – Croquis - Legenda

Cor	Elemento	Significado
Azul	Retas	Retas idênticas
Azul	Círculo	Posição dos sensores
Vermelho e Roxo	Círculos	As duas posições de atuação
Vermelho	Seta	Caminho da onda da primeira posição de atuação
Roxo	Setas	Sólida: caminho para o sensor mais próximo Tracejada: três caminhos para o outro sensor
Verde	Área	Área considerada para pontos de atuação

APÊNDICE B – Uso do osciloscópio nos ensaios

Os ensaios de amplificação e captura de sinais foram realizados com osciloscópio modelo GA-1102CAL disponível no laboratório de eletrônica da Faculdade de Computação. Para capturar ondas transientes, foi inicialmente utilizada a função de persistência de ondas na tela e posteriormente consideramos a função de captura de eventos únicos mais ápta à vizualização dos dados.



(a) Captura de evento com persistência

(b) Captura de eventos únicos

Figura 10 – Comparativo entre métodos de captura de eventos

Este método de captura se mostrou mais eficiente para a visualização dos eventos. A função de persistência de ondas na tela, apesar de útil para a visualização de ondas periódicas, não se mostrou eficiente para a captura de eventos únicos, como os gerados pelos sensores piezoelétricos.

APÊNDICE C – Simulação do consumo energético para quatro circuitos de condicionamento

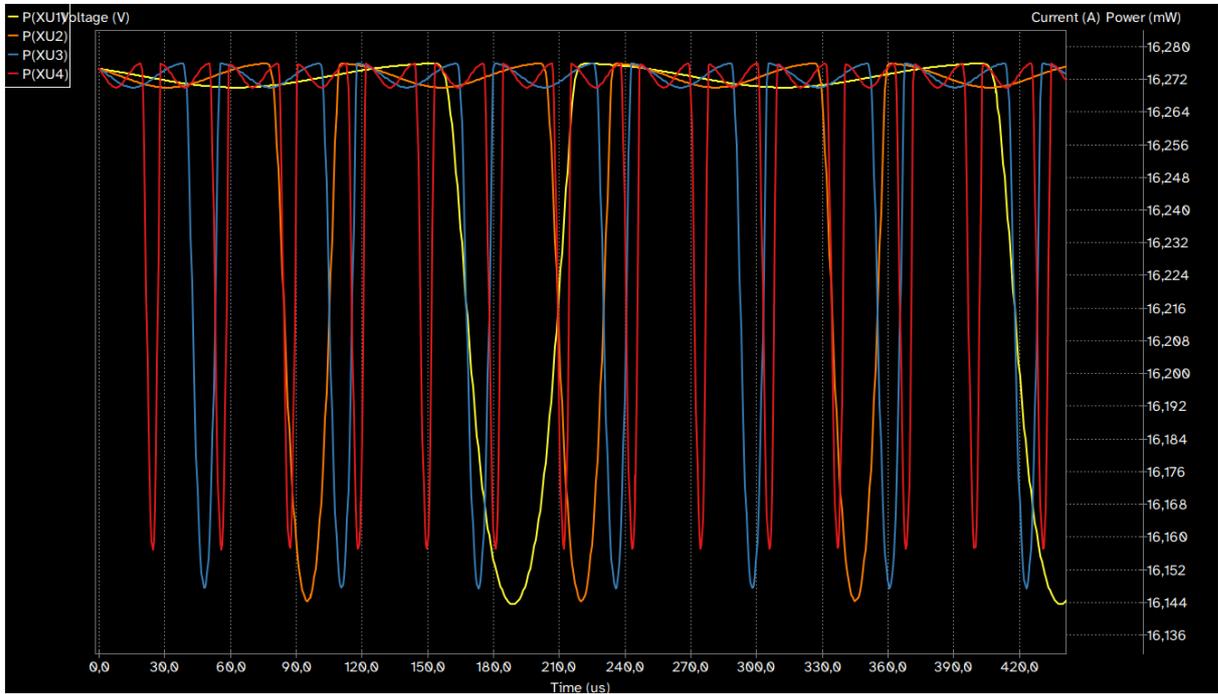


Figura 11 – Consumo energético para quatro circuitos de condicionamento simulados em Kicad, com frequências de 4, 8, 16 e 32kHz e amplitude de 5V. Observa-se que o consumo é praticamente linear, com variação em décimos de mW, indicando estabilidade energética do circuito em diferentes condições de frequência.

APÊNDICE D – Ensaios do protótipo

Este Apêndice apresenta leituras dos ensaios realizados com o protótipo do circuito amplificador, disponibilizados em formato interativo no PDF. Para garantir a visualização correta, recomenda-se o uso de um leitor de documentos com suporte a conteúdo dinâmico.

Durante os testes, observou-se que alguns leitores de PDF podem não exibir corretamente os elementos interativos, resultando em perda de funcionalidade ou visualização incompleta. Caso isso ocorra, sugerimos utilizar um dos seguintes leitores compatíveis:

1. Okular (versão 21.08.2 ou superior, para Linux e Windows);
2. Adobe Acrobat Reader (versão 2021 ou superior, para Windows e macOS).

Se não for possível utilizar um leitor compatível, uma versão estática dos dados pode ser solicitada ao autor, ou o conteúdo pode ser visualizado em um ambiente com suporte ao software mencionado.

CH1: entrada

CH2: saída

APÊNDICE E – Códigos de prototipagem

Código para a simulação de apenas um circuito amplificador:

```
.title KiCad schematic
.include "/caminho/para/TL081.301"
.save all
.probe all
.probe p(V++1)
.probe p(R2)
.probe p(XU1)
.probe p(R3)
.probe p(R1)
.probe p(Rg1)
.probe p(Rg2)
.probe p(V--1)
.probe p(Vin1)
.tran 1u 500u
V++1 Net-_U1-V+_ 0 DC 4.2
R2 Net-_U1-V+_ VIN 20k
XU1 VIN Net-_U1--_ Net-_U1-V+_ unconnected-_U1-V--Pad4_ SAIDA TL081
R3 SENSOR VIN 20k
R1 VIN 0 9.1k
Rg1 SAIDA Net-_U1--_ 100k
Rg2 Net-_U1--_ 0 1Meg
V--1 0 unconnected-_U1-V--Pad4_ DC 1.5
Vin1 SENSOR 0 DC 0 SIN( 0 3 10k 0 0 0 ) AC 0
.end
```

Código para a simulação do circuito quádruplo:

```
.title KiCad schematic
.include "/caminho/para/TL081.301"
.save all
.probe all
.probe p(R10)
.probe p(R12)
.probe p(R11)
.probe p(Rg7)
.probe p(Rg8)
.probe p(XU4)
```

```

.probe p(R4)
.probe p(R5)
.probe p(Rg2)
.probe p(XU1)
.probe p(V--1)
.probe p(V13)
.probe p(V++1)
.probe p(V1)
.probe p(R1)
.probe p(R3)
.probe p(R2)
.probe p(Rg3)
.probe p(Rg4)
.probe p(XU2)
.probe p(V10)
.probe p(R8)
.probe p(R7)
.probe p(R9)
.probe p(Rg6)
.probe p(XU3)
.probe p(Rg5)
.probe p(Rg1)
.probe p(R6)
.probe p(V4)
.options reltol=0.01 abstol=.1f vntol=10u

.tran .5u 1m
R10 Net-_U4+_ 0 9.1k
R12 Net-_U4+_ Net-_U1-V+_ 20k
R11 in4 Net-_U4+_ 20k
Rg7 0 Net-_U4--_ 1000k
Rg8 Net-_U4--_ out4 100k
XU4 Net-_U4+_ Net-_U4--_ Net-_U1-V+_ Net-_U1-V-_ out4 TL081
R4 Net-_U1+_ Net-_U1-V+_ 20k
R5 Net-_U1+_ 0 9.1k
Rg2 Net-_U1--_ out1 100k
XU1 Net-_U1+_ Net-_U1--_ Net-_U1-V+_ Net-_U1-V-_ out1 TL081
V--1 0 Net-_U1-V-_ DC 1.5
V13 in4 0 DC 0 SIN( 0 5 32k 0 0 0 ) AC 1

```

```

V++1 Net-_U1-V+_ 0 DC 4.2
V1 in2 0 DC 0 SIN( 0 5 8k 0 0 0 ) AC 1
R1 Net-_U2+_ 0 9.1k
R3 Net-_U2+_ Net-_U1-V+_ 20k
R2 in2 Net-_U2+_ 20k
Rg3 0 Net-_U2--_ 1000k
Rg4 Net-_U2--_ out2 100k
XU2 Net-_U2+_ Net-_U2--_ Net-_U1-V+_ Net-_U1-V-_ out2 TL081
V10 in3 0 DC 0 SIN( 0 5 16k 0 0 0 ) AC 1
R8 in3 Net-_U3+_ 20k
R7 Net-_U3+_ 0 9.1k
R9 Net-_U3+_ Net-_U1-V+_ 20k
Rg6 Net-_U3--_ out3 100k
XU3 Net-_U3+_ Net-_U3--_ Net-_U1-V+_ Net-_U1-V-_ out3 TL081
Rg5 0 Net-_U3--_ 1000k
Rg1 0 Net-_U1--_ 1000k
R6 in1 Net-_U1+_ 20k
V4 in1 0 DC 0 SIN( 0 20 4k 0 0 0 ) AC 1
.end

```

Estes códigos em SPICE foram gerados automaticamente pelo compilador de circuitos do KiCad, e foram utilizados para simular o comportamento do circuito amplificador projetado.

ANEXO A – Modelo de AmpOp em SPICE

O modelo utilizado foi:

```
* TL081 OPERATIONAL AMPLIFIER "MACROMODEL" SUBCIRCUIT
* CREATED USING PARTS RELEASE 4.01 ON 06/16/89 AT 13:08
* (REV N/A)      SUPPLY VOLTAGE: +/-15V
* CONNECTIONS:  NON-INVERTING INPUT
*                | INVERTING INPUT
*                | | POSITIVE POWER SUPPLY
*                | | | NEGATIVE POWER SUPPLY
*                | | | | OUTPUT
*                | | | | |
.SUBCKT TL081    1 2 3 4 5
*
C1  11 12 3.498E-12
C2   6  7 15.00E-12
DC   5 53 DX
DE  54  5 DX
DLP 90 91 DX
DLN 92 90 DX
DP   4  3 DX
EGND 99  0 POLY(2) (3,0) (4,0) 0 .5 .5
FB   7 99 POLY(5) VB VC VE VLP VLN 0 4.715E6 -5E6 5E6 5E6 -5E6
GA   6  0 11 12 282.8E-6
GCM  0  6 10 99 8.942E-9
ISS  3 10 DC 195.0E-6
HLIM 90  0 VLIM 1K
J1  11  2 10 JX
J2  12  1 10 JX
R2   6  9 100.0E3
RD1  4 11 3.536E3
RD2  4 12 3.536E3
R01  8  5 150
R02  7 99 150
RP   3  4 2.143E3
RSS 10 99 1.026E6
VB   9  0 DC 0
VC   3 53 DC 2.200
VE  54  4 DC 2.200
```

```
VLIM 7 8 DC 0
VLP 91 0 DC 25
VLN 0 92 DC 25
.MODEL DX D(IS=800.0E-18)
.MODEL JX PJF(IS=15.00E-12 BETA=270.1E-6 VTO=-1)
.ENDS
```

TEXAS INSTRUMENTS. TL081 Low-noise JFET-input operational amplifier. Disponível em: <https://www.ti.com/product/TL081>. Acesso em: 11 set. 2024.