Ankush Achwani

Computer Engineering, University of Massachusetts Amherst
aachwani@umass.edu · ankushachwani@gmail.com
ankushachwani.com · github.com/ankushachwani · linkedin.com/in/ankushachwani

Research interests

Making machine learning and other large-scale, real-world systems secure and trustworthy. My work so far covers post-quantum cryptography for 5G and embedded devices, attacks on and privacy of small quantized models, and embedded ML for health sensing.

Education

University of Massachusetts Amherst 2023 to May 2027 (expected)
B.S. in Computer Engineering, Commonwealth Honors College. GPA 3.89 / 4.0.

Honors

- Chancellor's Award, University of Massachusetts Amherst.
- Dean's List, Fall 2023 to present.

Research

Post-quantum signatures for STIR/SHAKEN in 5G
Post-quantum signatures are too large for SIP call setup, so simply replacing ECDSA in caller-ID authentication makes calls fail or slow down. This work develops a post-quantum design that matched today's ECDSA performance in testing on real SIP stacks, where the alternatives fall short.

Cryptonite: neural-network inference on the ESP32 RSA accelerator
Group course project
Runs ten int8 keyword-spotting networks as big-integer multiplies on a real ESP32. Data-path changes cut summed inference from 171 s to 44 s (3.93x), which is still 0.33x the speed of an optimized CPU kernel.

Polynomial products for post-quantum cryptography on the ESP32 RSA unit
2026 · code and data

- Packed ML-KEM, ML-DSA and Falcon polynomial products into the chip's 2048-bit multiplier, with every output checked bit for bit.
- The optimized path is 4.0 to 4.6x faster than the naive packed path, but a tuned NTT still wins five of six products.
- Whole operations take 0.91 to 1.38x PQClean's time, close to the limit set by how much of each operation is polynomial products.

Bit-flip attacks on microcontroller-scale keyword spotting
2026 · code and data

- Ran progressive bit search on DS-CNN-S and TC-ResNet8 at int8 and two 4-bit settings, with three seeds each, a random-flip baseline and a 30-flip cap.
- DS-CNN-S fell to 15% accuracy in a mean of 5.3 to 8.0 targeted flips. TC-ResNet8 never reached 15% within the cap, and random flips broke neither model.
- Architecture mattered more than bit-width. Results are from a white-box software simulation, not real fault injection.

Does 4-bit quantization change membership-inference leakage in keyword spotting?

2026 · code and data

- Attacked five small models at three bit-widths. Loss-attack AUC stays at 0.513 to 0.533, with no detectable difference between bit-widths.
- AUC tracks each model's train-test accuracy gap (Spearman 0.91). Membership is assumed from the standard split, and the attacks are simple threshold attacks, not LiRA.

Gradient inversion against a federated MNIST model

Spring 2026 · code

Trained a model with federated averaging, then attacked it. iDLG recovered the label on 40 of 40 images but rarely the image, with a median SSIM of 0.05.

Needle-less hypoglycemia detection wristband

Expected April 2027

An affordable wristband that alerts a phone to low blood sugar without needles. No results yet; evaluation will be subject-independent.

Teaching

All at the University of Massachusetts Amherst.

Course Coordinator, ECE 690STC Foundations of Generative Models Fall 2026

Canvas administration, quizzes and grading.

Teaching Assistant, ECE 371 Security Engineering Fall 2026

Teaching Assistant, ECE 214 Probability and Statistics; ECE 579 Math Tools for Data Science and ML Summer 2026

Supported 72 students across both courses through office hours, grading and Zoom check-in meetings.

Experience

Cofounder and CTO, StageLink 2026 to present

Booking and show-running software for live music, with artist and venue sides on one system. The artist app is live with access by waitlist; the venue app is built and not yet released. stagelink.dev

Software Engineering and AI Systems Intern, Queer Music Agency Summer 2026

Built an internal operations platform from scratch to replace spreadsheet and CRM workflows, covering calendar, email, messaging, tasks and artist rosters, with AI-assisted mail clustering and artist matching. Hosted on AWS.

Software projects

Cyphelo

2026 · cyphelo.com

Self-hosted personal cloud with 35 tagged releases. A Go agent serves files from the user's own drive over a Cloudflare Tunnel, with end-to-end encrypted folders designed so the agent never holds the plaintext or the key (AES-256-GCM, Argon2id). Includes AI photo search, face clustering and OCR, with web and Apple clients.

CourseWatch

2026 · coursewatch.online

Emails UMass students when a class seat opens or a waitlist appears on SPIRE, polling every minute. Serverless on AWS: Lambda, EventBridge, DynamoDB, S3 and API Gateway, with a Python backend.

mincontext

2026 · code

Finds the minimal set of files a coding task needs in a repository, using path scoring, an import graph and an LLM pruning step. Available as a web app and an MCP server on npm.

Newsora

2025 · website

Flutter news app for iOS and Android with offline reading, translation into 12+ languages and an AI assistant for questions about any article, powered by Cohere. A custom aggregator runs on AWS Lambda, S3 and EventBridge, with Supabase for accounts and sync.

Other builds

- **Deepfake audio detection** ECE 601, Spring 2026
  On ASVspoof 2019 LA, an MLP with L2 weight decay reached 99.11% accuracy and a 1.53% EER, against 7.36% for an MFCC-GMM baseline. These are in-dataset results from a 20% hold-out of the training partition, so they don't cover unseen attacks.
- **Clariti** 2025
  Task dashboard for college students. Pulls deadlines from Canvas, Gmail, Google Calendar, Discord, Slack and Notion, then ranks them with Cohere. Next.js and Prisma. Web app
- **UMass University Programming Council website** 2025
  Official club site with event listings, ticket reservations and an editor for non-technical staff. React and Express on AWS.
- **DIY DJ Deck** ECE 304
  Real-time audio firmware on an STM32F303RE, with 4-tap reverb and a PWM-controlled 2-pole Sallen-Key low-pass filter using optocouplers.
- **ESP32-CAM face detection**
  Edge versus cloud comparison, with Flask and OpenCV on the cloud side.

Leadership and service

Director of Finance, UMass University Programming Council May 2025 to March 2026

Managed a $750K budget with signature authority over financial documents and contracts, negotiated annual budgets with student governments, and helped organize large-scale campus concerts.

Late Night Event Coordinator, UMass University Programming Council July 2024 to May 2025

Ran weekly movie nights and monthly campus-wide events on $31K in event budgets, working with 10+ vendors, 5 campus departments and 60+ student volunteers.

Production Event Coordinator, UMass University Programming Council February to May 2024

Managed event inventory and equipment rentals for student organizations.

Project Lead, MassAI Spring 2025

Led two student teams of 4 to 6 members building applied AI projects with computer vision and LLM APIs.

Selected coursework

Security: Introduction to Security Engineering; Security Engineering (graduate-level); Reverse Engineering and Exploit Development (in progress).

ML: Machine Learning for Engineers; Advanced On-Device Deep Learning (in progress).

Systems and embedded: Introduction to Embedded Systems; Systems Programming; Hardware Organization and Digital Design; Junior Design Project; Senior Design Project I (in progress).

Math and theory: Probability and Statistics; Continuous-Time Signals and Systems; Introduction to Computation; Analytical Tools for ECE.

Other: Honors Research (in progress).

Skills

Languages: Python, C/C++, Go, JavaScript/TypeScript, Swift, Dart, SQL, MATLAB.

ML and security: PyTorch, TensorFlow, scikit-learn, OpenCV, PQClean, mbedTLS, libsodium.

Embedded: ESP32, STM32.

Systems and web: AWS serverless, Next.js, React, Flask, Express, Flutter, Supabase, Postgres, Cloudflare Tunnel, Vercel, LaTeX.

Certifications and other

- AWS Certified Cloud Practitioner, July 2025.
- Interests: football, music, traveling, event planning.
- Spoken languages: English, Hindi, Kannada, Sindhi.