PakTech Today | Pakistan's Premier Technology Magazine
Vol. 01, Issue 14 • ISSN: 3136-2729

TECHNOLOGY FEATURE Industrial News / Technology Report / Research Communication

When Your Computer Talks Too Much: Acoustic Cryptanalysis and the Sound of Leaking Keys

A smartphone on a coffee table, a hand resting on a laptop's palm rest, even a USB charger, all can silently betray your private encryption keys. The most elegant cyberattacks don't touch the network. They travel through air.

By **Mubashra** | University of Agriculture Faisalabad (UAF) | Published: August, 2026
mubashramajid725@gmail.com | Position: Student Researcher

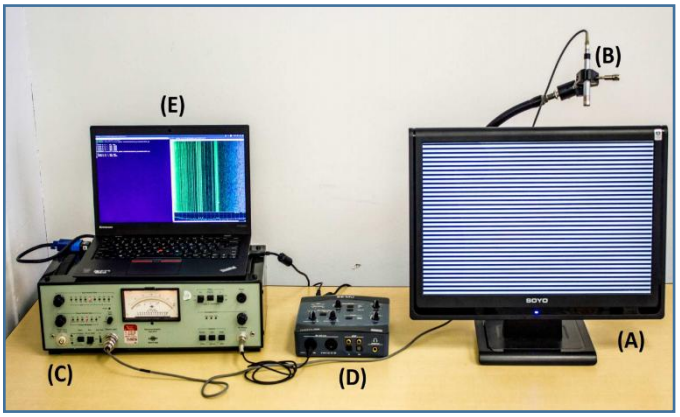
Introduction

We have spent decades building digital walls. Firewalls, encrypted VPNs, multi-factor authentication, layer after layer of protection against threats that come through cables and networks. And yet, some of the most devastating attacks on modern cryptography do not travel through a wire at all. They travel through the air. They come as sound.

Acoustic cryptanalysis is the art of recovering cryptographic keys by listening to the unintentional noises a computer makes while encrypting or decrypting data. This is not science fiction. It is a proven, practical technique that has extracted real RSA keys from real laptops using nothing more than a smartphone microphone.

The idea belongs to a broader family called side-channel attacks. A side-channel attack does not break the mathematics of encryption. Instead, it exploits the messy physical reality of computing: processors heat up, power consumption fluctuates, operations take different amounts of time – and yes, they make sounds. Acoustic cryptanalysis turns the machine's own voice into a witness against you.

> ***"In 2013, researchers extracted a full 4096-bit RSA private key from a laptop using a microphone 30 cm away. No malware. No network access. Just sound."***



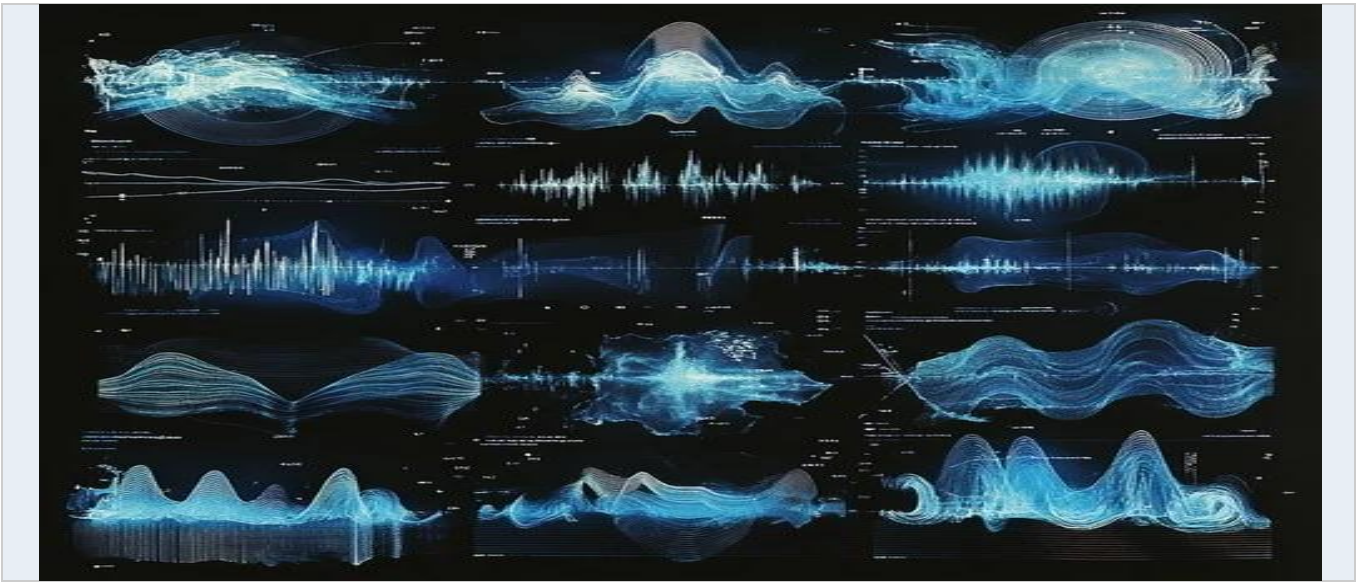
Vol. 01, Issue 14 • ISSN: 3136-2729

Technology Overview: The Physics of a Chatty Computer

To understand the attack, we have to look inside a laptop during a cryptographic operation. When a CPU performs RSA or AES decryption, it executes millions of logical operations per second. Each operation draws electrical current from the power supply. That current does not flow silently.

Capacitors, voltage regulators and inductors on the motherboard vibrate at frequencies that depend on the current load. These vibrations produce **acoustic emissions** – sound waves that radiate into the air and through the machine's chassis. The critical insight is that these sounds are not random. They are **data-dependent**. A decryption with one private key sounds measurably different from a decryption with another key. Capture those differences with enough precision, and you can work backwards to recover the key itself.

The frequencies involved span from infrasound (below 20 Hz) to ultrasound (above 20 kHz), but the most useful signal often lives in the same range as human speech – a few hundred hertz to a few kilohertz. That means the leak blends into the background noise of any office, coffee shop, or hotel lobby. It never announces itself. It just drips information, constantly, every time the machine does cryptographic work.



Waveform visualization

Key Findings & Impact

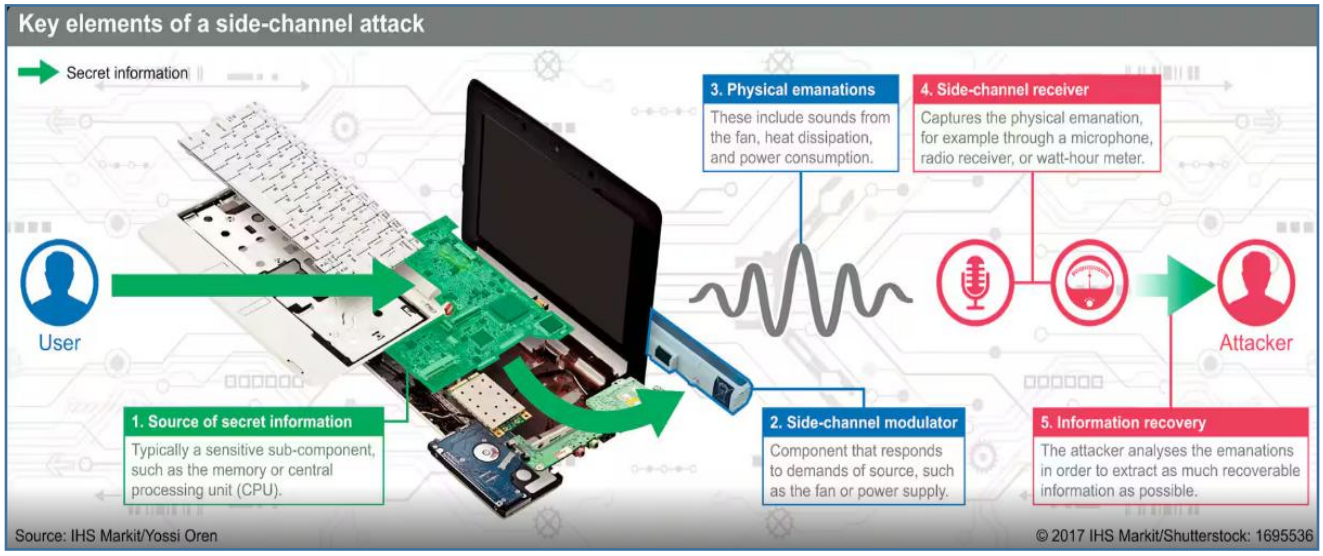
The attack scenario is almost embarrassingly straightforward: put a microphone close to a laptop, record the sounds it makes when decrypted particular ciphertexts, and then process these recordings by a machine learning algorithm. The machine learning algorithm infers the acoustic leakage from bits in the private key.

The 2004 breakthrough: Adi Shamir (the "S" in RSA) and Eran Tromer demonstrated that the sound emanating from a typical PC when it is decrypting an RSA ciphertext reveals a partial key. The inventor of RSA also showed how to defeat his creation with a microphone.

The 2013 horror: The same researchers, with Daniel Genkin, were able to recover the full 4096-bit RSA key of a laptop with a microphone 30 cm away. It took an hour to listen. No physical tampering. No malware. Pure sound.

The smartphone twist: They also demonstrated that the built-in microphone of a typical smartphone on the same table was enough. A rogue app on the laptop of the person sitting in a cafe opposite you could then potentially snatch your keys, while you sip your latte.

Weirder variations: A hand on the laptop palm rest can feel the vibrations - no microphone needed. A cable (power or audio) plugged into the laptop can transmit the sound via the ground wire. Computing is physics, and physics is leaky.



Attack Flowchart

Who should worry? For the typical home user, this is currently a low risk, the attack requires proximity, time and post-processing. However, for a news reporter needing to protect their sources, a CEO in a M&A deal, a government official dealing with sensitive information, or an intelligence agency, this is a credible threat.

What's Next – Protecting Against the Singing Machine

The first reaction is: “Why don't you use an anechoic chamber." That doesn’t work. Sensitive computing takes place in open offices, at airports, in hotels - places we can't control. Microphones in the ceiling, smart speakers, our colleagues' phones, even microphones in cameras can become audio sensors.

Software can't fully solve this problem. Cryptographic libraries are now quite adept at thwarting timing and power attacks, but sound is a hardware problem. Transistors must switch. Current must flow. Components must vibrate. You can't patch away physics.

So what can we do?

Constant-time algorithms: Program cryptography so that all branches of the code take the same time and consume the same electrical power - regardless of the key. If the machine makes identical sounds for all keys, there is no signal to find. Libsodium and Google’s BoringSSL do this.

RSA blinding: Randomise the input to decryption; de-randomise the output. An attacker only sees noise (random) corresponding to the randomisation.

TEMPEST shielding: Metallic boxes that stop acoustic and electromagnetic leaks. Unfeasible for consumer laptops, but a must in secure government offices.

Operational hygiene: Disable your microphone on confidential computers. Don't leave your phone sitting around when handling sensitive data. Learn to think about security in the physical, not only the virtual, world.

> ***"The best encryption in the world is useless if your private key is broadcast on air."***

About the Author

Mubashra is a sixth semester BS Computer Science student at the University of Agriculture Faisalabad (UAF), with a deep interest in cybersecurity, side channel attacks, and unconventional computing. She can be reached at mubashramajid725@gmail.com.

Keywords: Acoustic Cryptanalysis; Side-Channel Attack; RSA; Cybersecurity; Hardware Security; Pakistan Tech

References

[1] Shamir, A., & Tromer, E. (2004). Acoustic cryptanalysis: On nosy people and noisy machines. *Weizmann Institute of Science Technical Report*.

[2] Genkin, D., Shamir, A., & Tromer, E. (2014). RSA key extraction via low-bandwidth acoustic cryptanalysis. *Advances in Cryptology – CRYPTO 2014*, Lecture Notes in Computer Science, Springer.

[3] Genkin, D., Pipman, I., & Tromer, E. (2015). Getting to the bottom of side channels. *Journal of Cryptographic Engineering*, 5(2).

[4] Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3rd ed.). Wiley.

[5] NSA/CSS. (2020). *TEMPEST and Emanations Security Standards*. National Security Agency Publication Series.