



Scan for the paper



Scan to connect

## How We Turned a Keyboard Into a LoRa Transmitter

### Team

Shayan Majumder<sup>1</sup>, Emmanouil M Tentzeris<sup>2</sup>, George Goussetis<sup>1</sup>, Stylianos D. Asimonis<sup>3</sup> and Spyridon N. Daskalakis<sup>1</sup>

### Affiliations

<sup>1</sup> Heriot-Watt University, Edinburgh, UK, <sup>2</sup> Georgia Institute of Technology, Atlanta, USA and <sup>3</sup> University of Patras, Greece

Every modern electronic device contains a microcontroller. Inspired by our previous NoLoRa work, in this work we show that a commercial keyboard's microcontroller leaks RF signals through its PCB traces. We intercept these emissions from tens of meters away to recover keystrokes, passwords, and credentials. No hardware modifications. No implanted radio chip. This approach can potentially extend to other microcontroller-based devices.



### Motivation

Keyboards are everywhere, offices, ATMs, secure facilities. All share the same design: a MCU that potentially can broadcast what you type. This can be captured by existing LoRa gateways already deployed citywide.

### How it Works

The keyboard's 16 MHz microcontroller's data lines generates harmonics. The 27<sup>th</sup> lands near 433 MHz, LoRa's band. PCB traces radiate it.

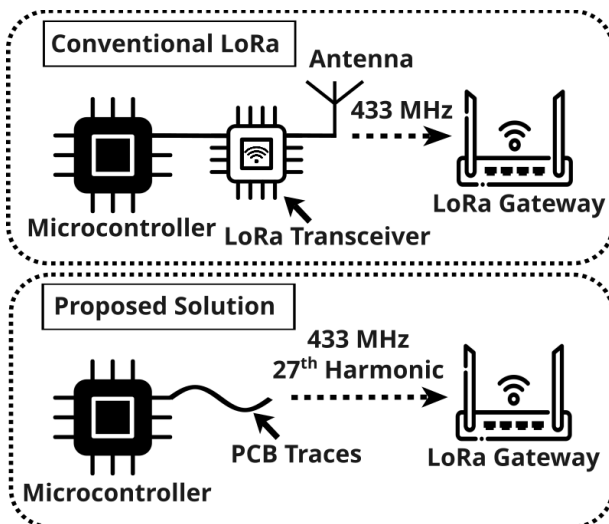
### Contributions

- Keystroke interception via unintended 433 MHz harmonic emission
- Works on unmodified commercial keyboards
- No implanted hardware — pure side-channel
- Receiver range: 10+ m indoors, through walls

### Results

Injected valid LoRa frames via unmodified keyboard PCB. Packet RX 10-25 m indoors, adjacent rooms. <5% PER within 10 m. PCB traces only; no antenna.

### System Architecture

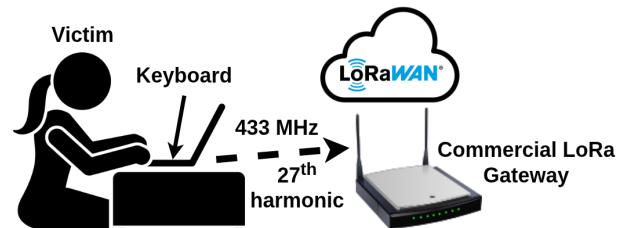


Conventional LoRa needs a transceiver IC. Ours needs none. The keyboard's SPI/I<sup>2</sup>S lines radiate at 433 MHz via the 27<sup>th</sup> harmonic of the 16 MHz clock. No extra hardware. No PCB changes. The 27<sup>th</sup> harmonic falls inside the LoRa band and remains ~35 dB above LoRa's -130 dBm noise floor. Any commercial LoRa gateway can receive it.

### Hacking a commercial Keyboard

We demonstrated LoRa on an unmodified commercial keyboard via side-channel exploitation, enabling remote password exfiltration without hardware modification or dedicated radio chips, with just a simple firmware update.

Video: <https://youtu.be/46ryFLtGbOE>



Paper: NoLoRa: Ultra-Low-Power LoRa Transmissions Without Active Radios for Battery-Free Devices