CS7351 传感系统原理与设计
Principles and Design of Sensing Systems

Side-channel Sensing Attack (2)

陈东尧

上海交通大学

chendy@sjtu.edu.cn

2025年秋季

Schedule our Project Presentation

1月1日（周四）至3日（周六）放假调休，共3天。
1月4日（周日）上班，教学安排按第16周周五课表执行。

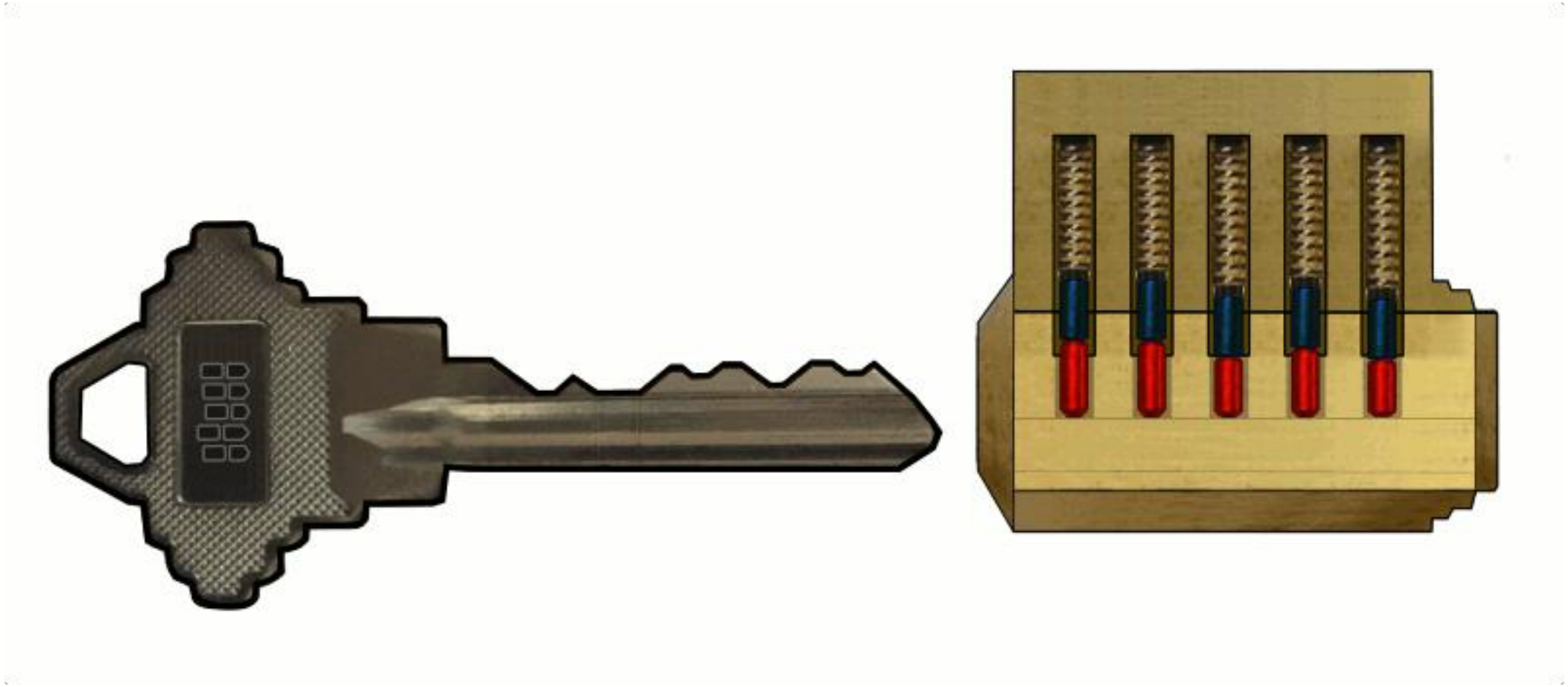
学 期 校 历

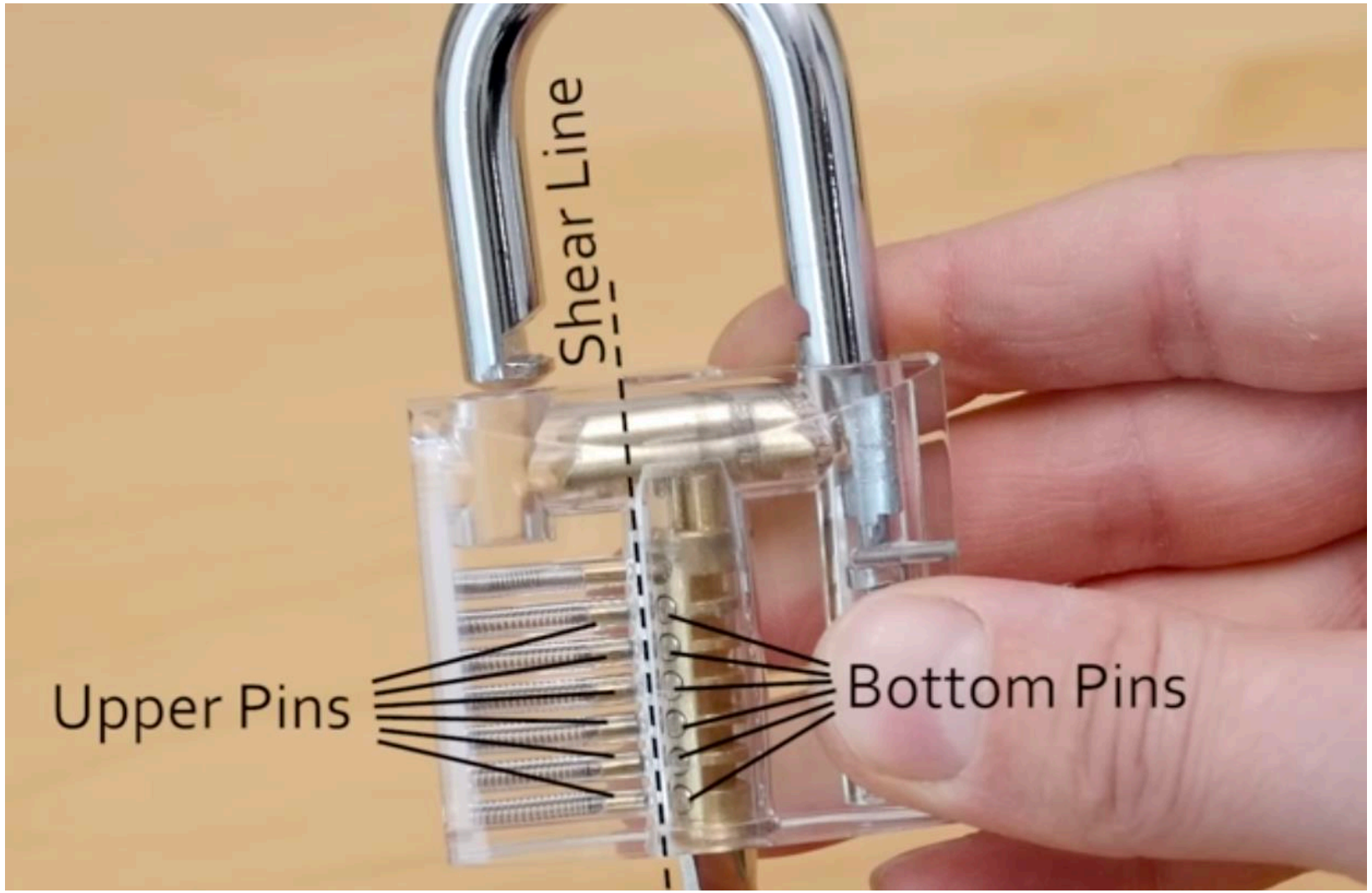
	12月			1月		
	14	15	16	16	17	18
	15	22	29		5	12
	16	23	30		6	13
	17	24	31		7	14
	18	25		1	8	15
	19	26		2	9	16
	20	27		3	10	17
	21	28		4	11	18

Building the Security Mindset

- Understanding the mechanism
- Define and detail an effective attack model
- Thorough evaluation

How to Pick a Lock!




Shear Line
Upper Pins
Bottom Pins

Outline

- Security for different sensing modalities
  - Attack on microphone (LightCommand)
  - Attack on IMU (Wallnut)
  - Eavesdropping on IMU (VeFi)
  - Secure I/O devices (DualStrike)
- For IoT Systems
  - Attack on Hall-effect Sensors and Power Grid (Hall spoofing)
  - Secure Connections between IoT devices (BLE Guardian and VAuth)

- **Impact: Attack model/targeted scenario**
- **Novelty: technical elements**
- **Thoughtfulness: Evaluation**

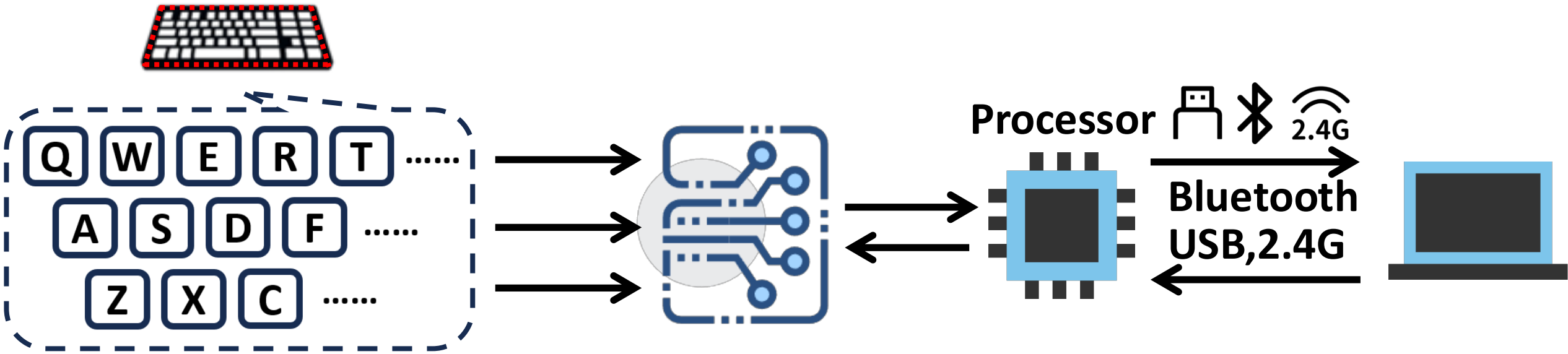
DualStrike

Accurate, Real-time
Eavesdropping and ***Injection*** of Keystrokes
on Commodity Keyboards

Xiaomeng Chen, Jike Wang, Zhenyu Chen, Qi Alfred Chen, Xinbing Wang, Dongyao Chen

Hall-effect keyboard vs *Mechanical keyboard*

- A keyboard consists of three main components: **switches**, a scanning circuit, and a communication port.



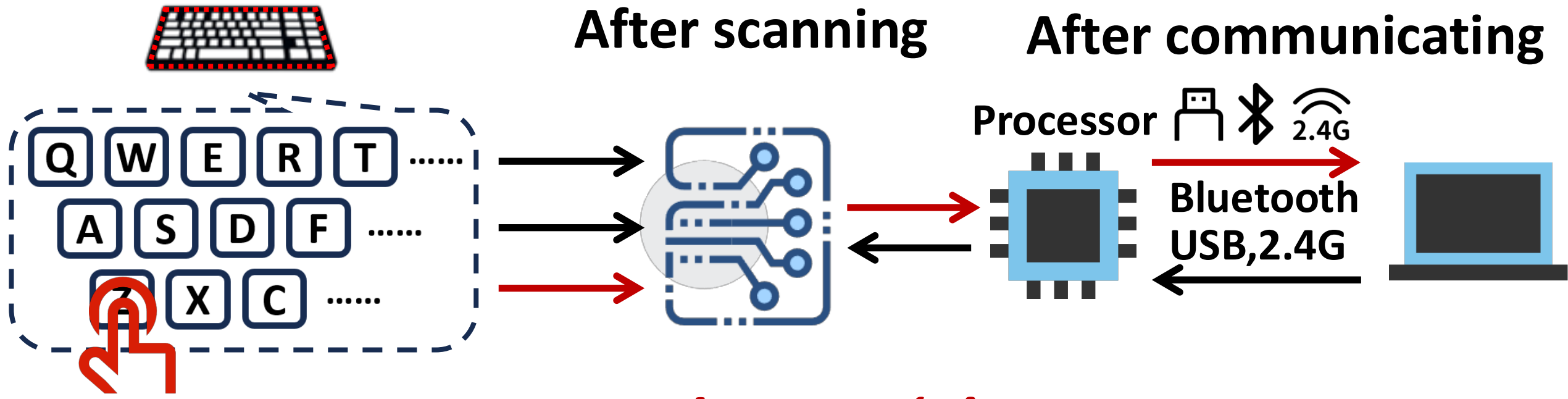
Switches On a Keyboard

Scanning Circuit

Communication Port

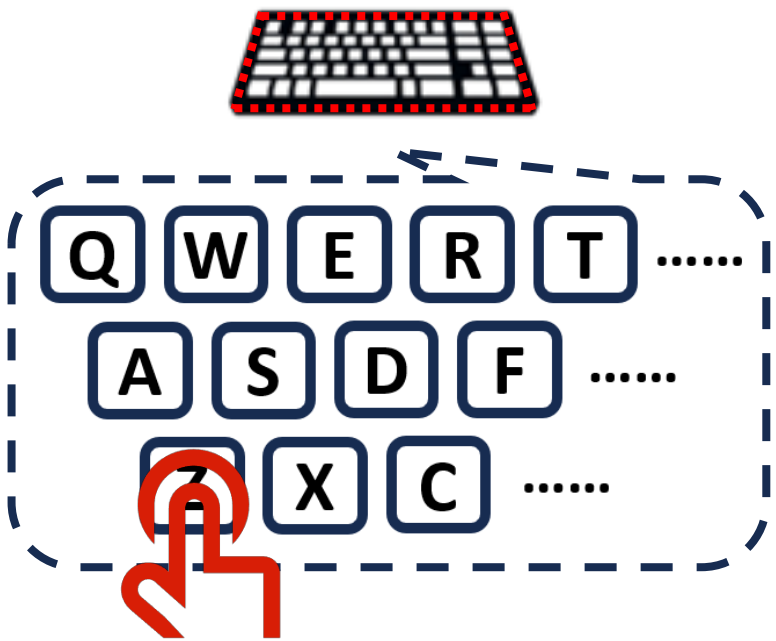
Hall-effect keyboard vs *Mechanical keyboard*

- A keyboard consists of three main components: **switches**, a scanning circuit, and a communication port.



Hall-effect keyboard vs *Mechanical keyboard*

- A keyboard consists of three main components: **switches**, a scanning circuit, and a communication port.



Z :I was Tapped

Mechanical vs Hall-effect

Key difference:

Keystroke sensing mechanism

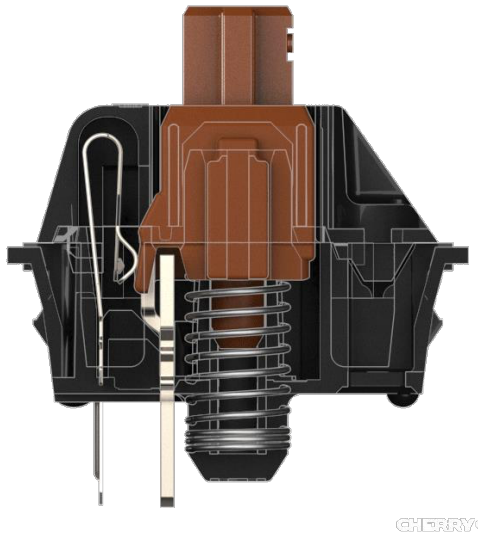
How is Z sensed?

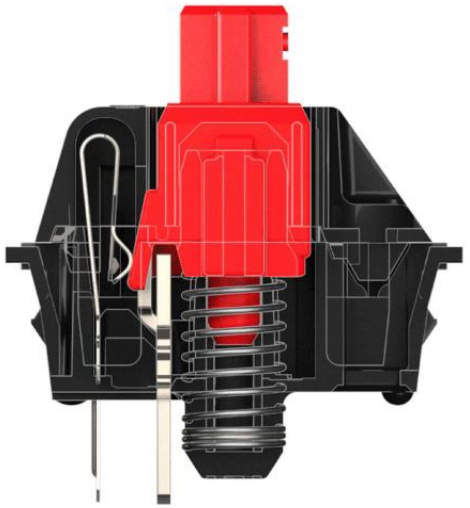
Hall-effect keyboard vs *Mechanical keyboard*

Mechanical Switch

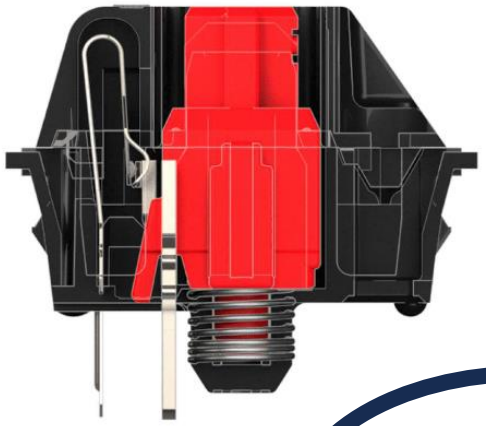
Contact-based!

Before pressing





After pressing

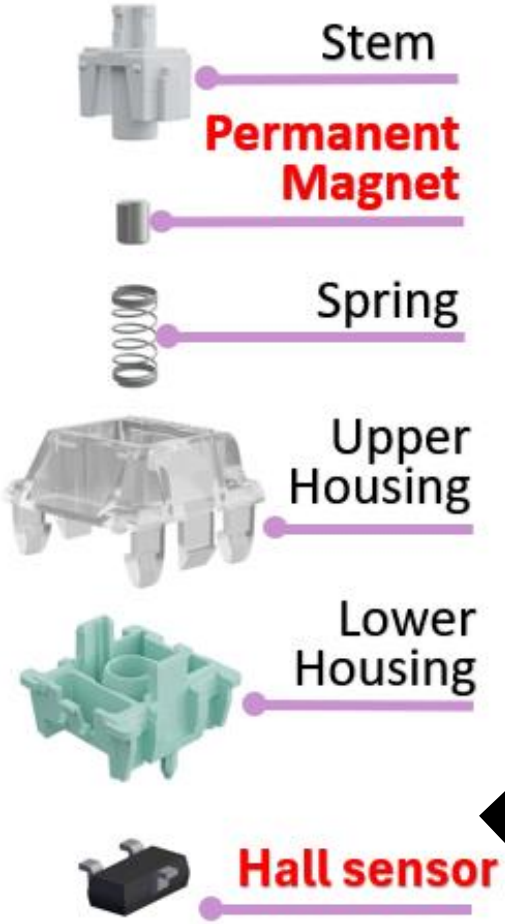


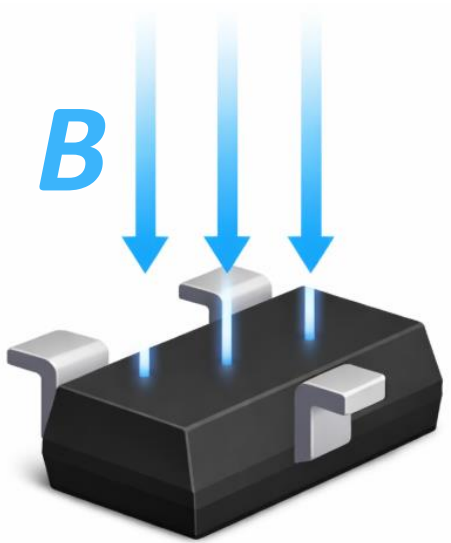
- Need fully pressed to register a keystroke

Keystroke detected!

Hall effect keyboard vs *Mechanical keyboard*

Hall effect Switch





Measure perpendicular magnetic field

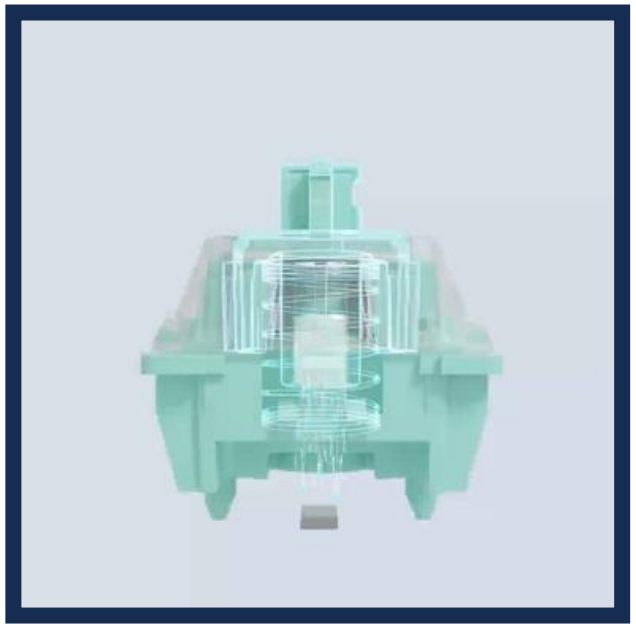
- Output a voltage

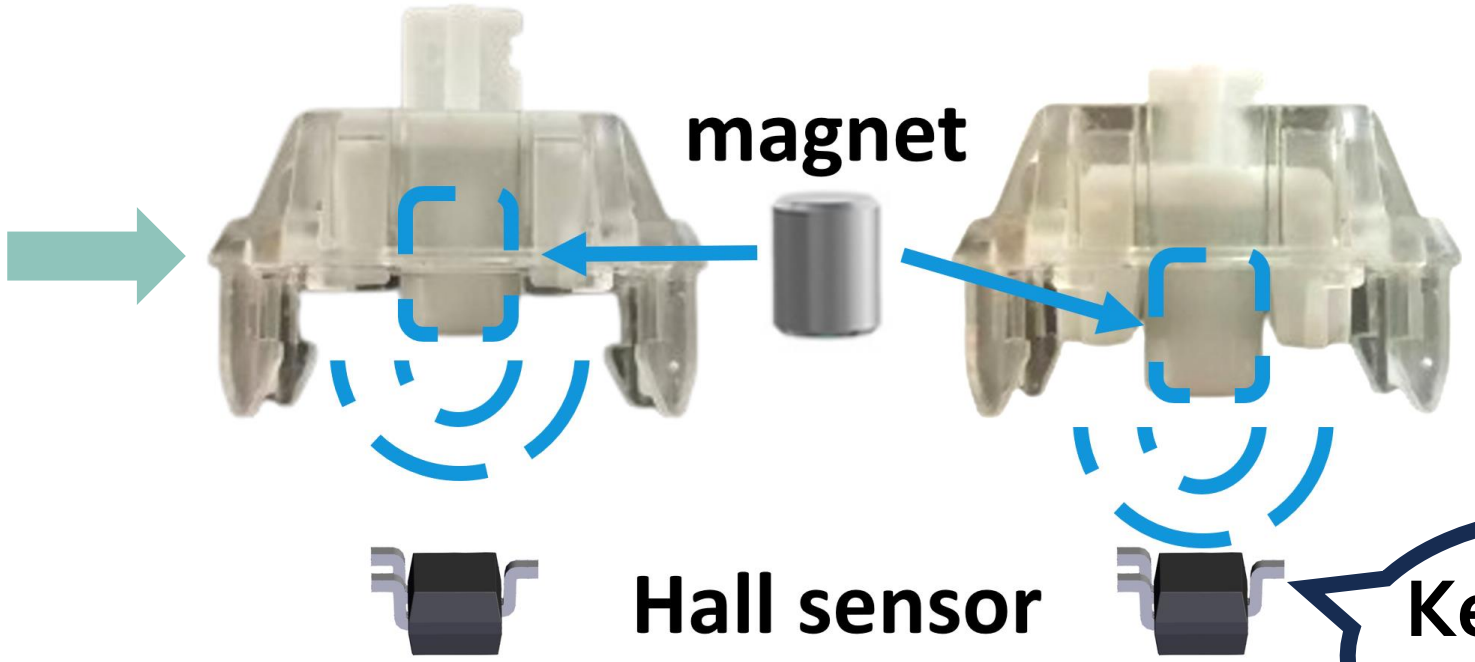
Vout ∝ B

Hall-effect keyboard vs *Mechanical keyboard*

Hall-effect Switch

Contactless!



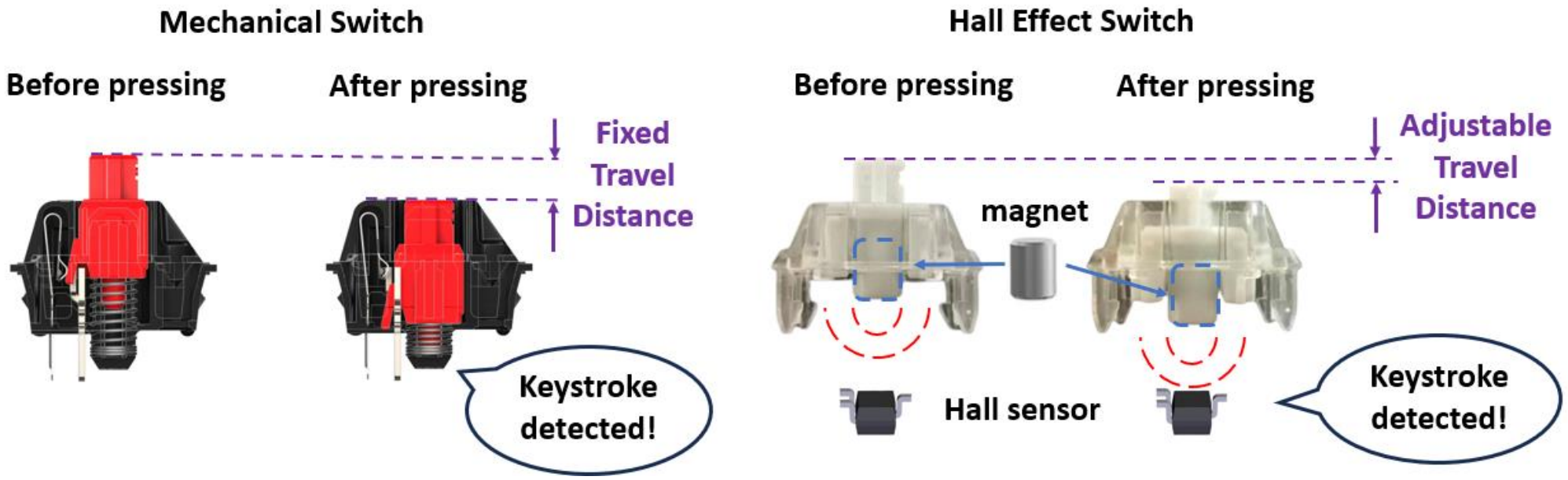


Hall-effect keyboard vs *Mechanical keyboard*

Customizable key travel: **0.1 mm and 4 mm, granularity of 0.1 mm** for SteelSeries Apex Pro Hall-effect keyboard

Quicker response time: favorable in high-performance keyboard applications

Longer lifespan: > 100 million click



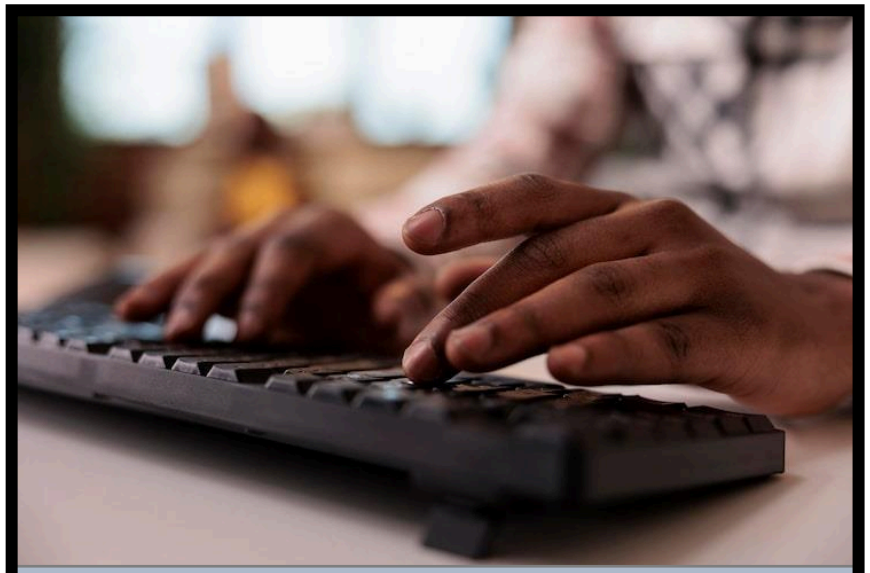
Hall-effect keyboard vs *Mechanical keyboard*

Customizable key travel: 0.1 mm and 4 mm, granularity of 0.1 mm
for SteelSeries Apex Pro Hall-effect keyboard

Quicker response time: favorable in high-performance keyboard applications

Longer lifespan: > 100 million click

Favored by



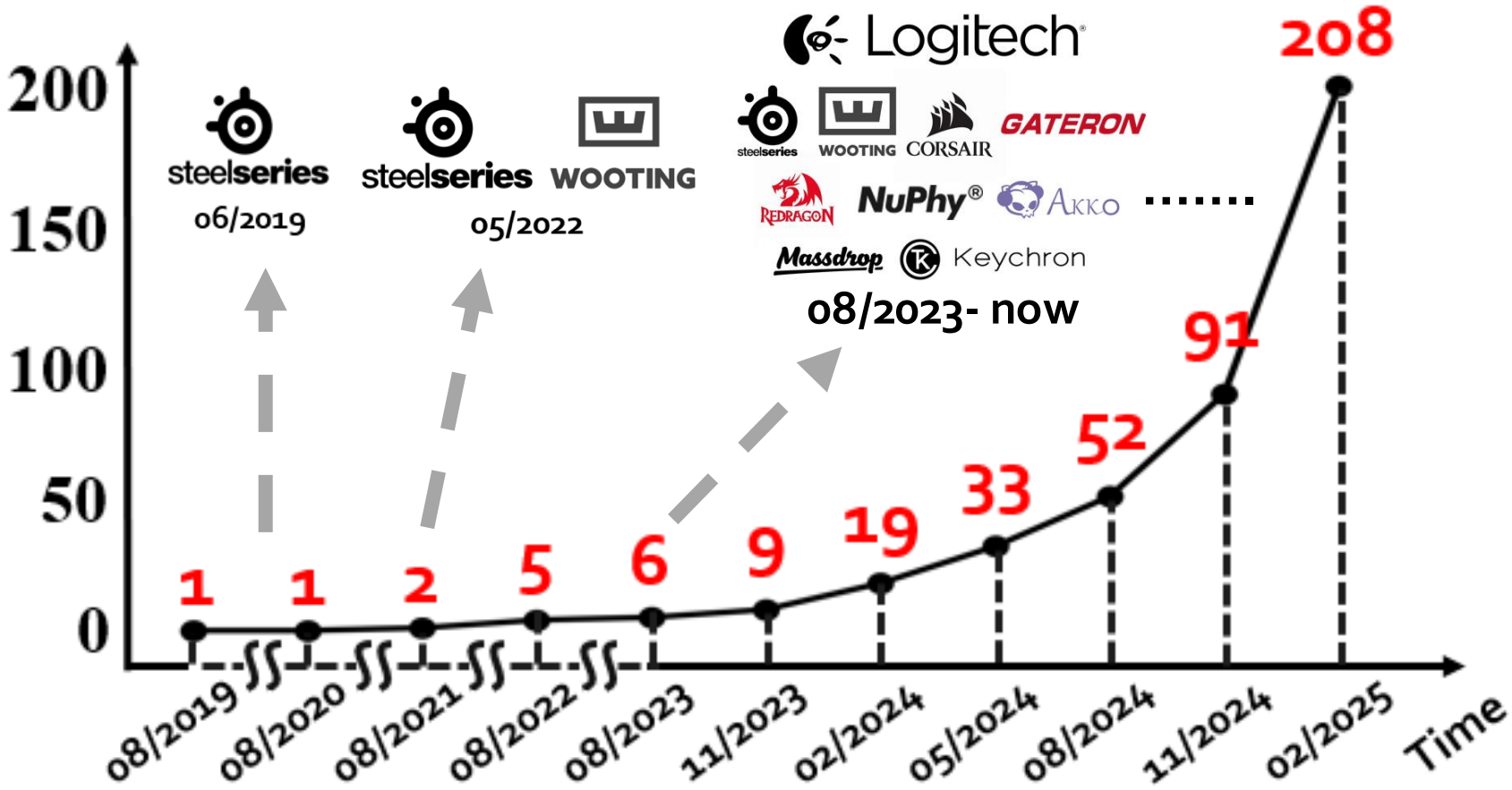
Everyday Keyboard Users

Esports Players

Fast-emerging Hall effect keyboard

- Hall-effect keyboard models recorded an average growth rate of **82.60% every three months.**
- Hall-effect keyboard market size exhibits a CAGR of **18.7% since 2024**.

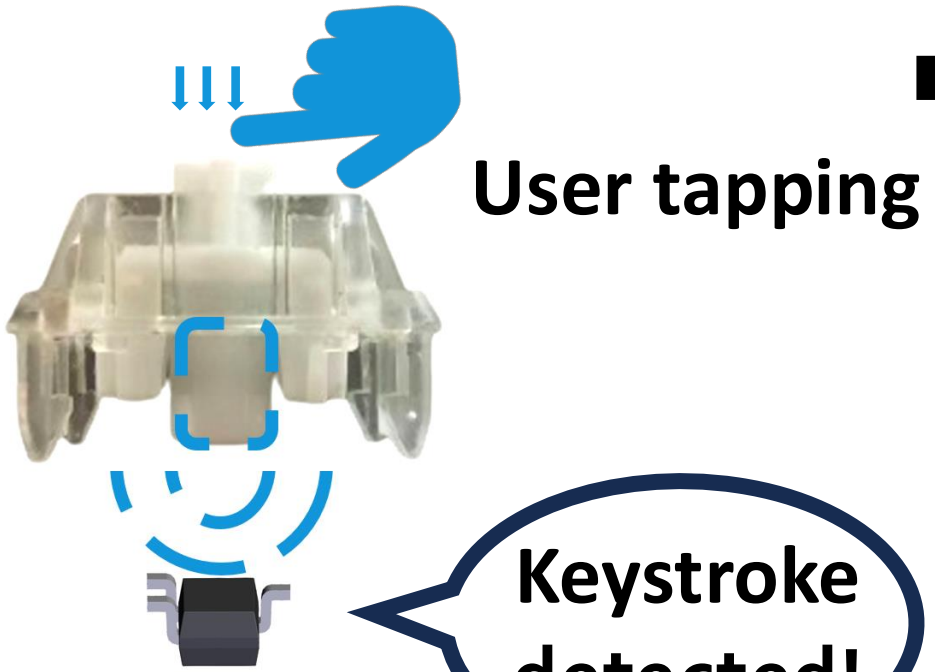
Num. of Hall-effect keyboard models



Hall-Effect Switch can be the Root Cause

Hall-effect Switch's

- ***high sensitivity***
- ***durability***
- ***reliability***



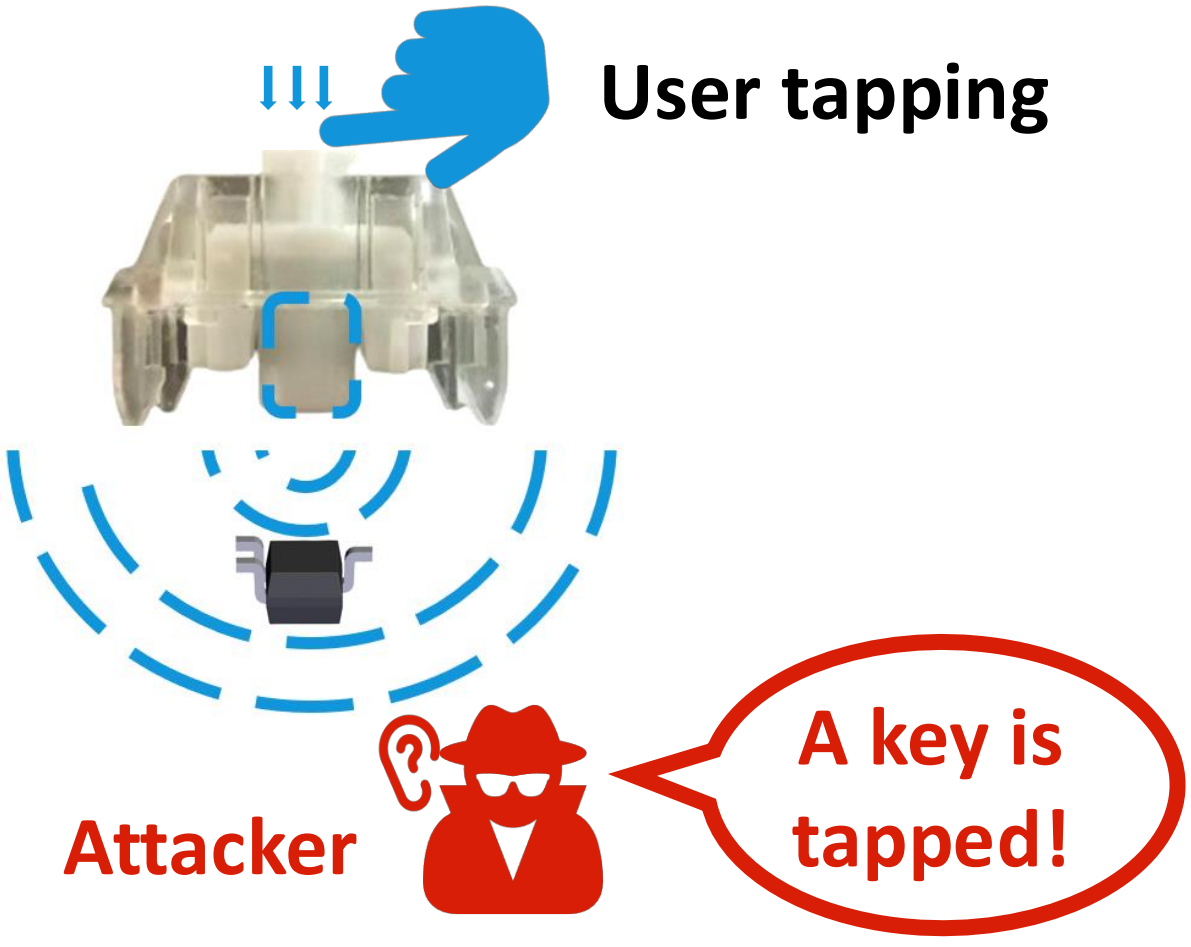
User tapping

- **Customizable key travel**
- **Quicker response time**
- **Longer lifespan**

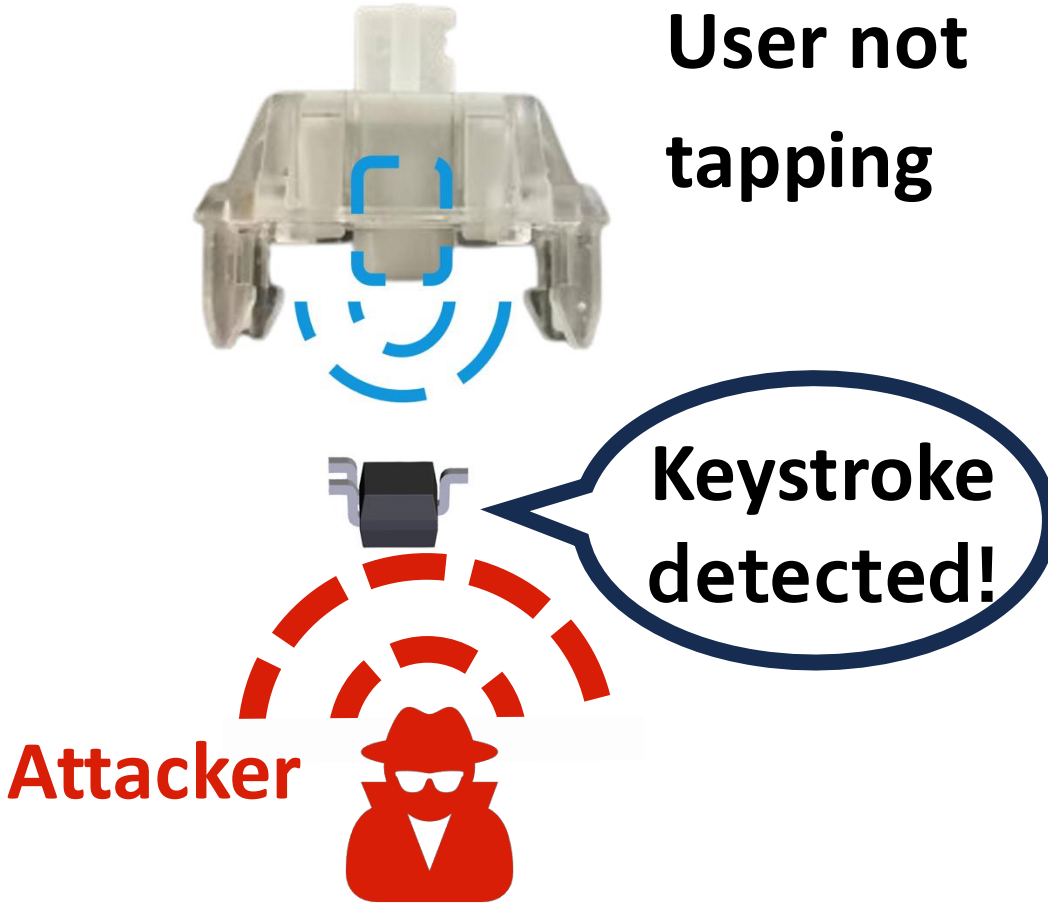
Hall-Effect Switch can be the Root Cause

- However, it can also be the root cause for:

Eavesdropping



Keystroke Injection



Existing Keyboard Attacks

Only Eavesdropping:

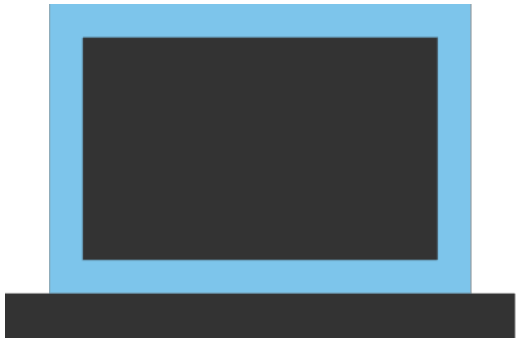
- leveraging side-channel signals such as **visual**, **acoustic**, and **electromagnetic** information to infer current keystrokes.

Only Keystroke injection:

- BadUSB attack: use of reprogrammed USB devices to mimic keyboards injecting malicious fake keystrokes

Now protected

- Authentication
- Windows + Kaspersky



Existing Keyboard Attacks

Only Keystroke injection:

- EMI injection: **GhostType** enables contactless keystroke via **electromagnetic interference (EMI).**

However, GhostType:

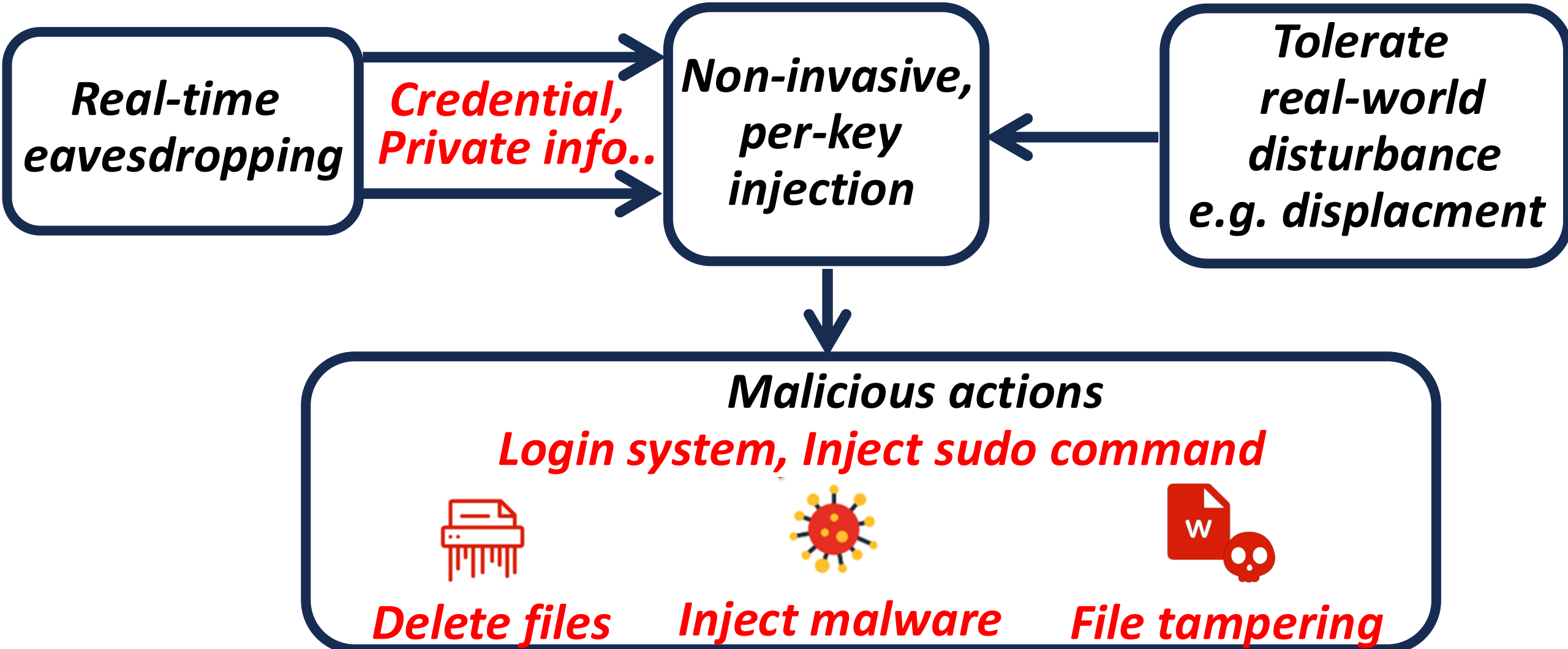
(i) Requires synchronization

(ii) EMI generation devices: signal generator, amplifier

(iii) Cannot achieve per-key injection

A practical attack on keyboard should be :

Eavesdropping + Keystroke injection



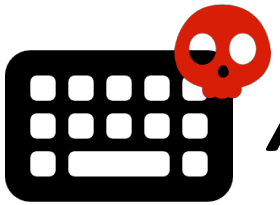
DualStrike:

The first attack scheme that can perform:
(i) keyboard listening and

(ii) non-invasive, per-key keystroke injection
on Hall-effect keyboards, and can also

(iii) mitigate real-world disruptions such as keyboard displacement

Attack model



Attack goal: *both eavesdrop and malicious input injection*

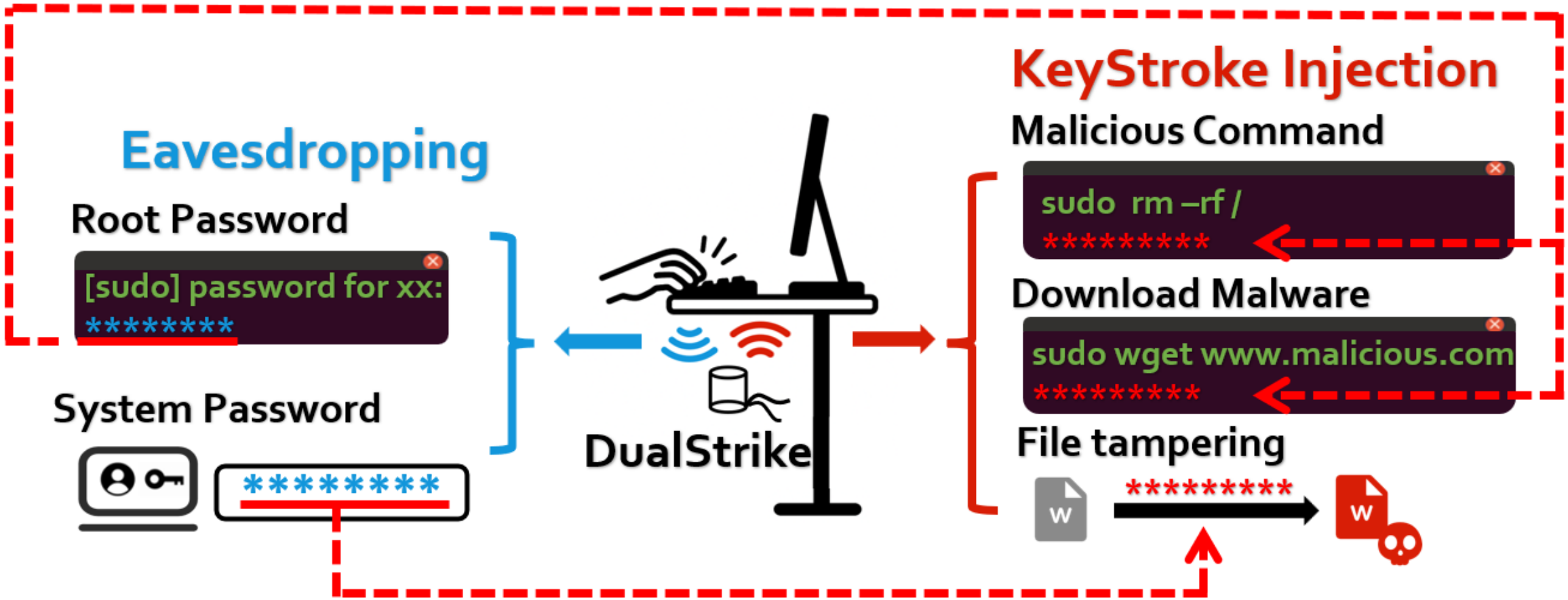
Prior Knowledge: *Known keyboard model and characteristics*

Non-contact & Invasive: *covert, no modification*

Stealthy deployment: *attack device beneath table*

Attack scenarios

- ***Eavesdropping*:** capture sensitive information, infer user liveness
- **Injection:** With sensitive context, attacker can implement several attack vectors



Questions: 

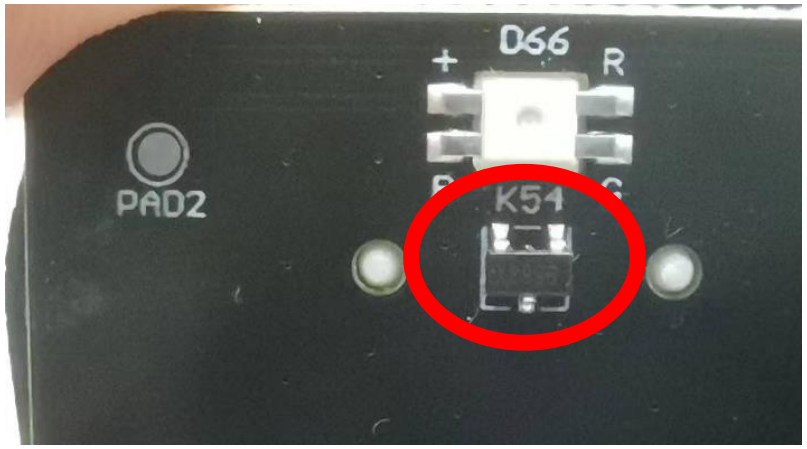
Although hall-effect switch can be the root cause, however:

1. ***How much magnetic field strength*** *is needed to trigger a keystroke?*

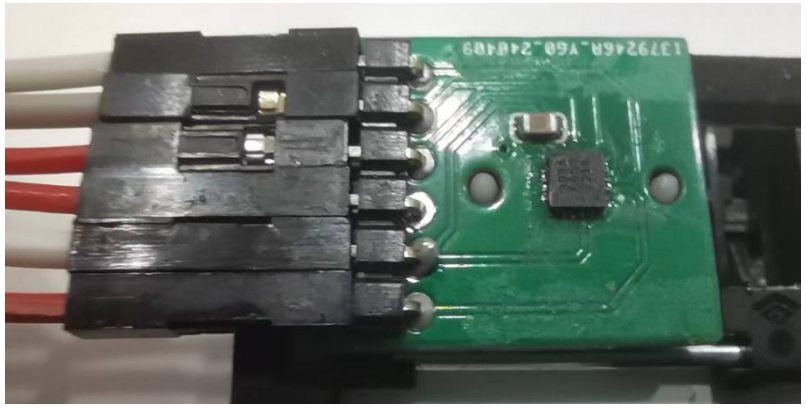
2. *Can* ***magnetometers*** *sense the movement of magnetic switches?*

2. *What is the internal* ***scanning mechanism*** *of hall-effect keyboard?*

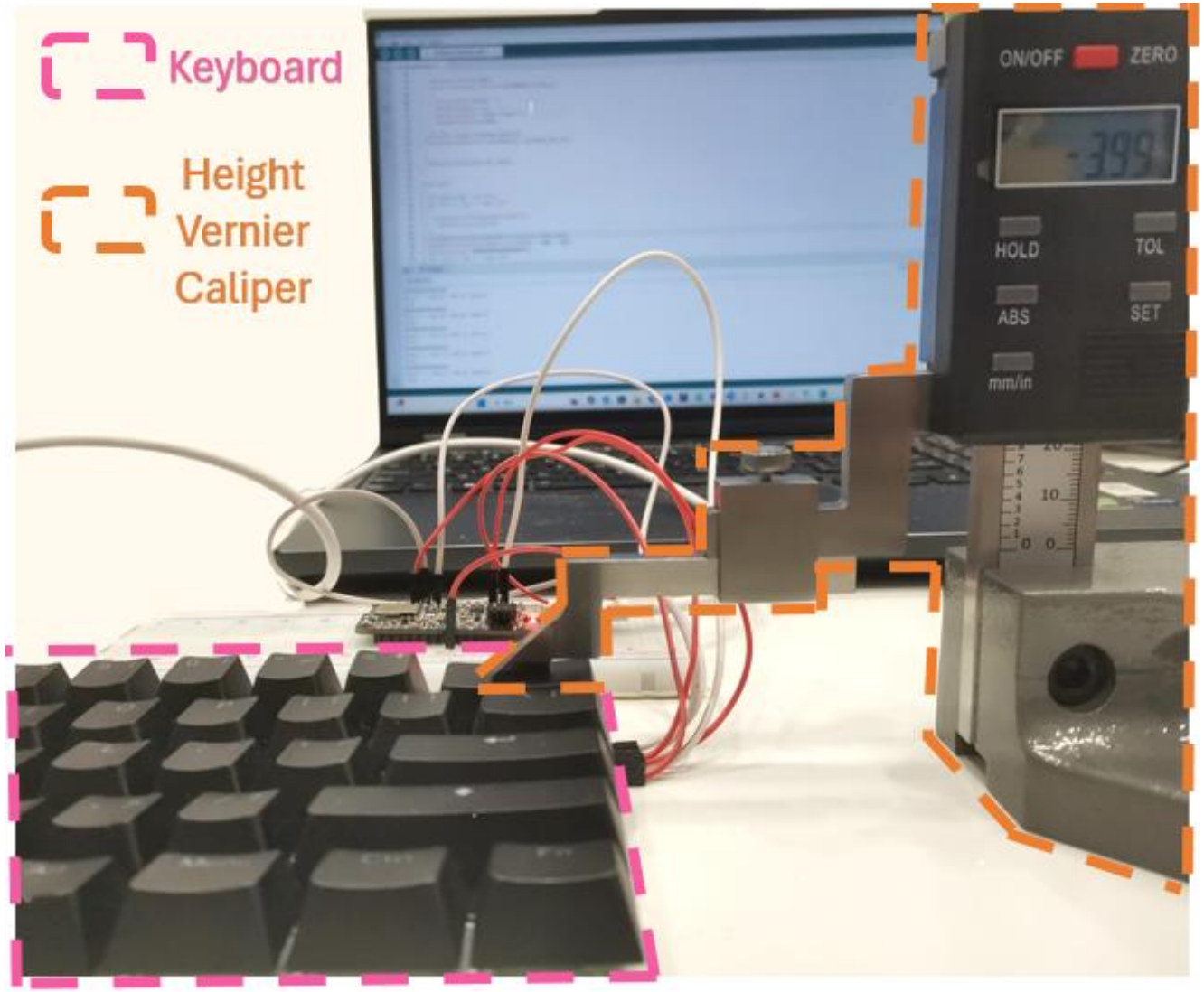
Characterizing Hall-effect Keyboards -- Hall-effect Switches



original proprietary sensor

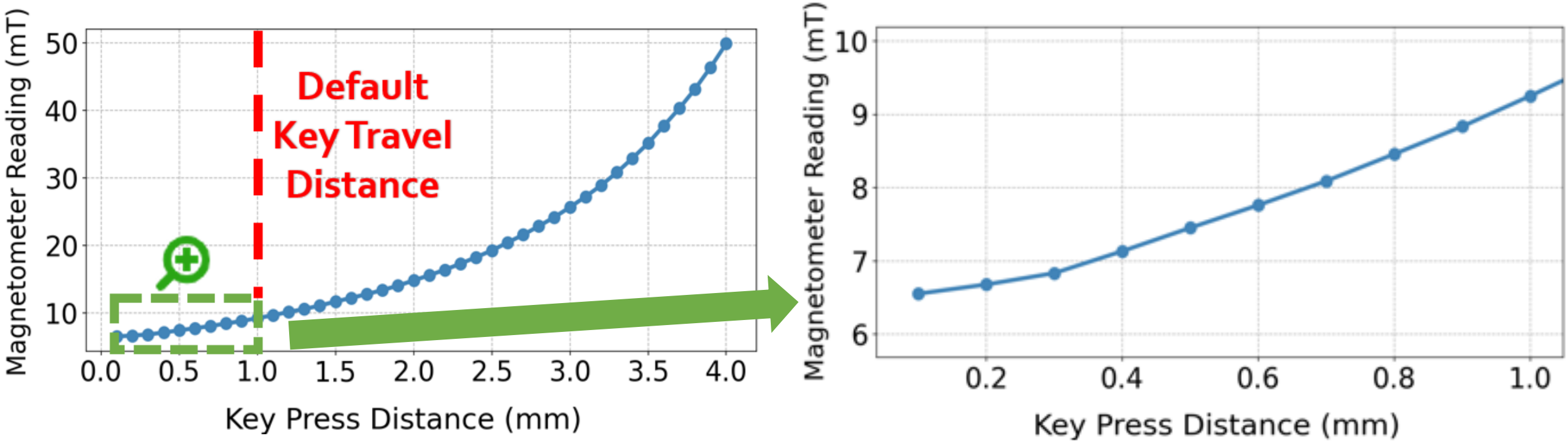


Replaced MLX90393 sensor



use vernier caliper emulate
travel distances from 0.1 to 4 mm

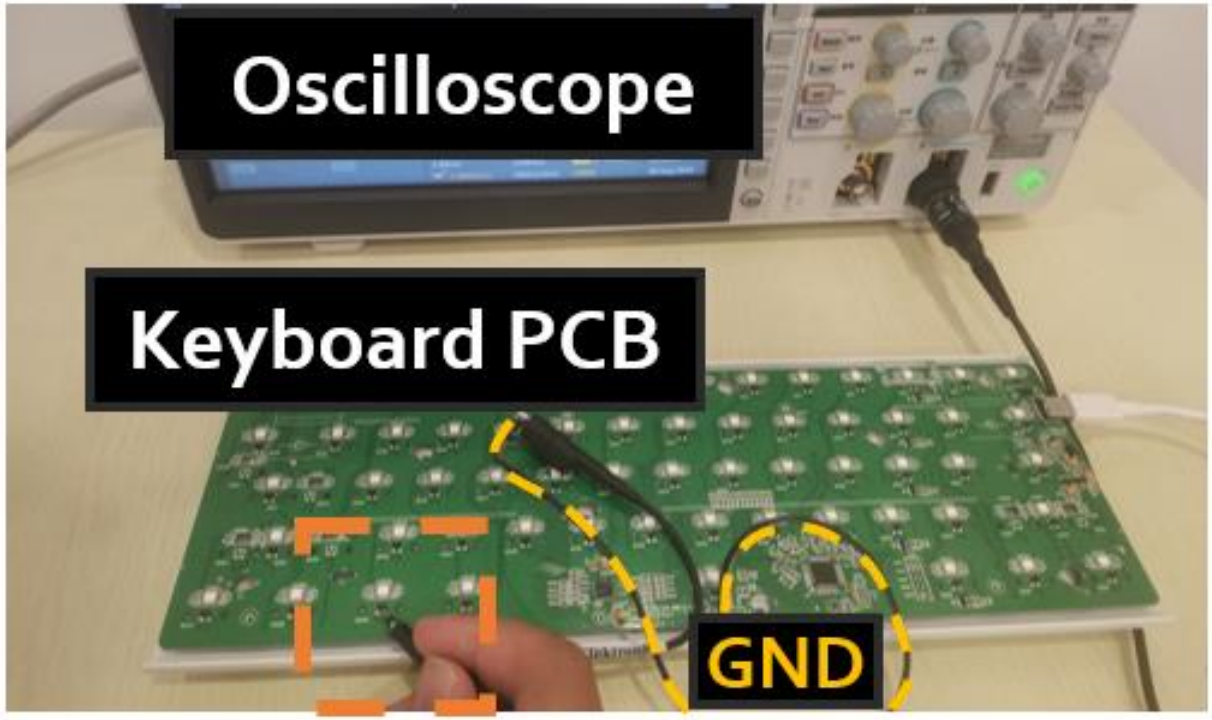
Characterizing Hall-effect Keyboards -- Hall-effect Switches

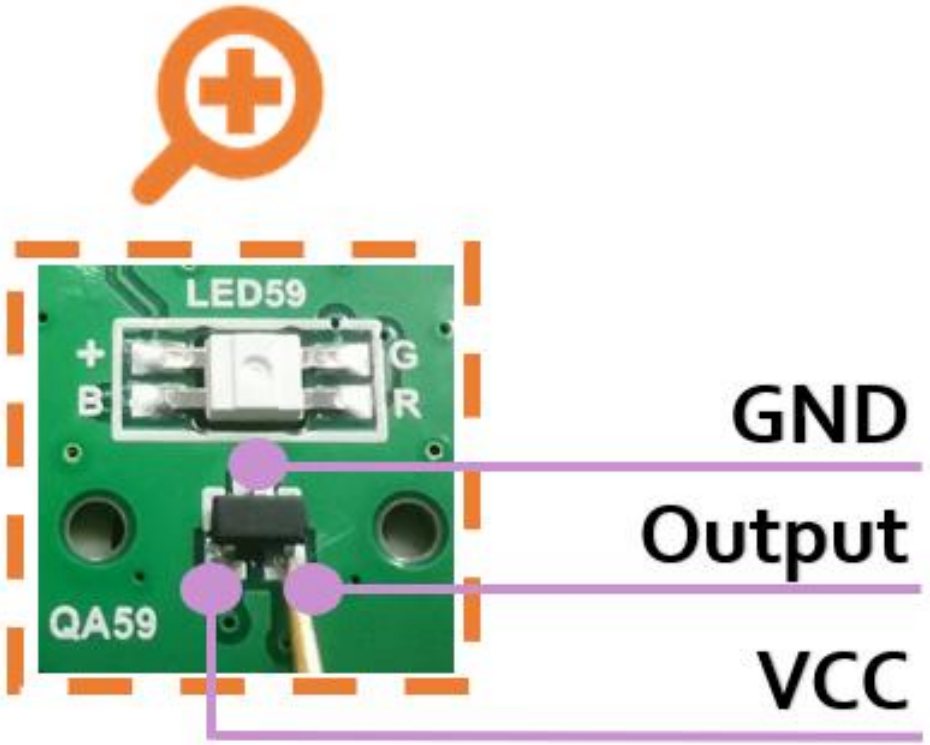


- ***<1mm**: preferred key travel distance*
- When < 1 mm, **only 9 mT** is needed to trigger a keystroke
- **Commodity magnetometers** can capture the variance of the magnetic field

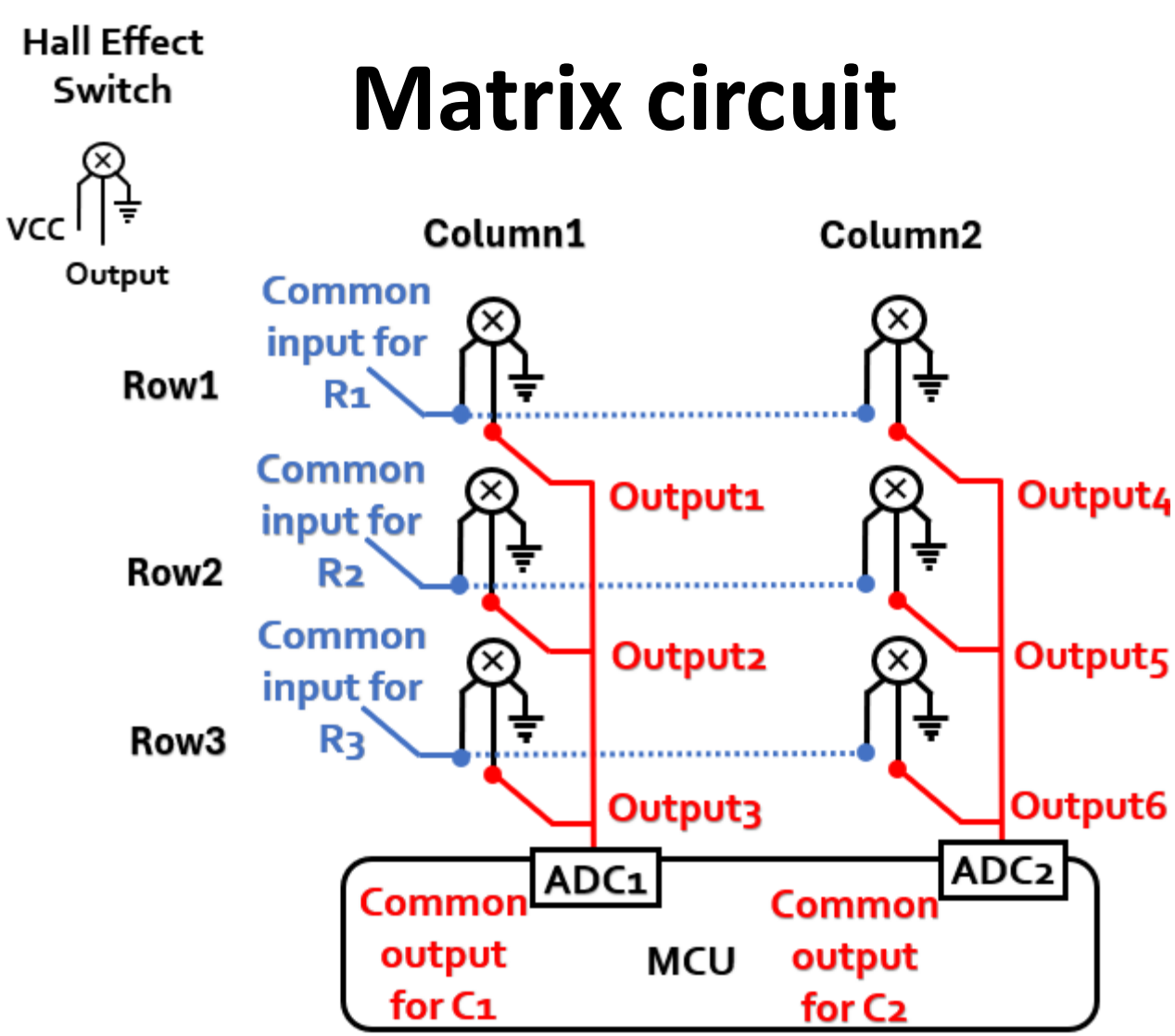
Characterizing hall-effect keyboards -- Scanning Circuit

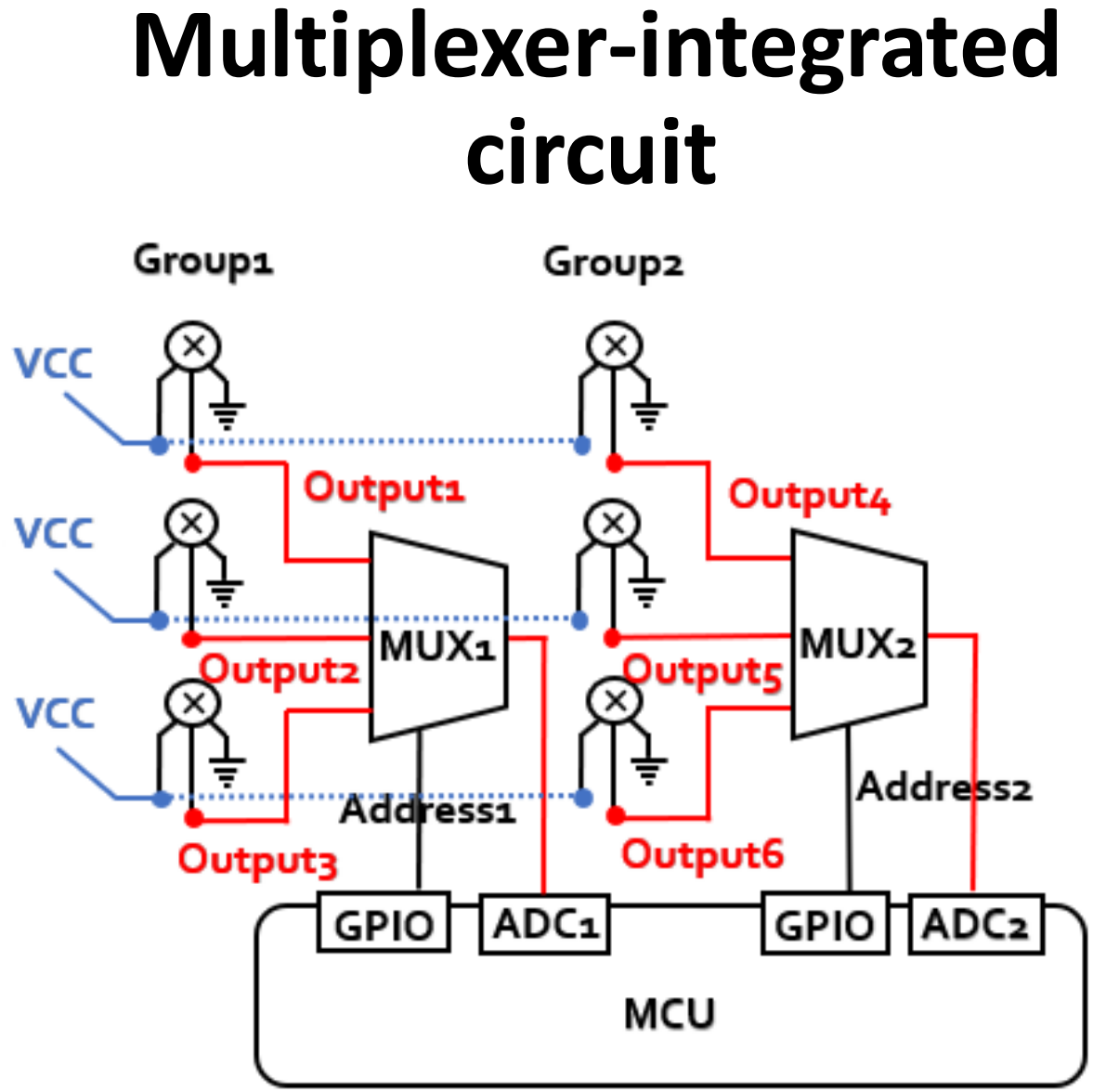
- We disassembled six popular off-the-shelf Hall-effect key boards and reverse-engineered their scanning circuits. Use oscilloscope to monitor signal.





Characterizing hall-effect keyboards -- Scanning Circuit





Characterizing hall-effect keyboards -- Scanning Circuit

Keyboard Type	Scanning Type	Cycle
Wooting 60 HE	MUX-integrated	375 μs
Steelseries Pro	Matrix	990 μs
Keydous NJ98-CP	MUX-integrated	5160 μs
k70 Pro Max	Matrix	900 μs
Reddragon M61	Matrix	1000 μs
DrunkDeer A75 Pro	Matrix	880 μs

- Hall-effect keyboards **have shorter scan cycles** compared to traditional keyboards (2.4 ms to 8.2 ms)

Design Challenges:

- ***Attack device:*** design powerful electromagnets with confined form factor

- ***High-frequency magnetic injection:***

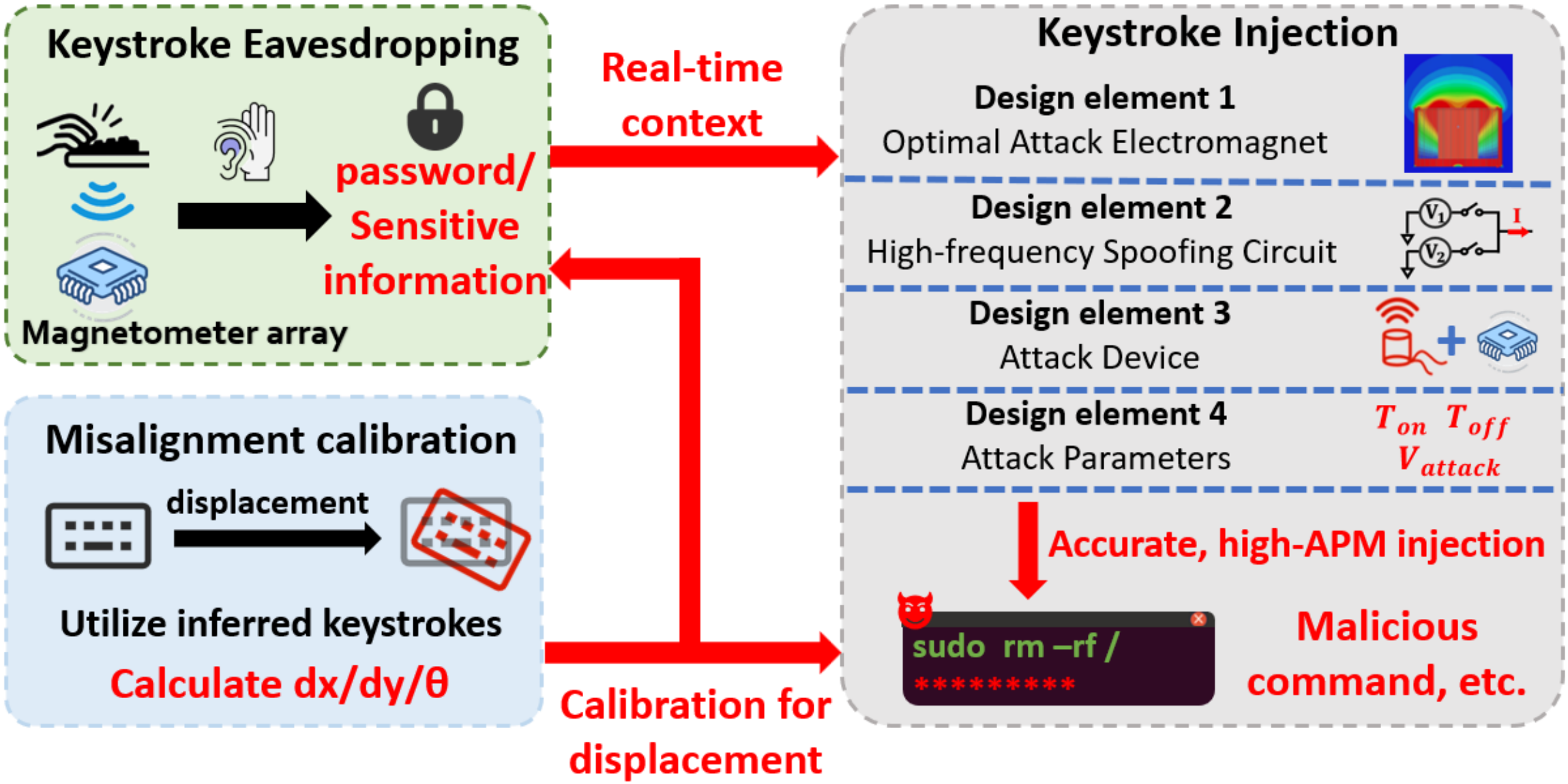
we use magnetometer as spoofing device. How to utilize hall-effect keyboard's rapid sensing to achieve High-frequency magnetic injection, regardless of Inductrive characteristics of electromagnets

- ***Alignment of attack device:***

users may adjust the keyboard's position based on personal habits.

How to successfully executing keystroke injection attacks despite misalignment

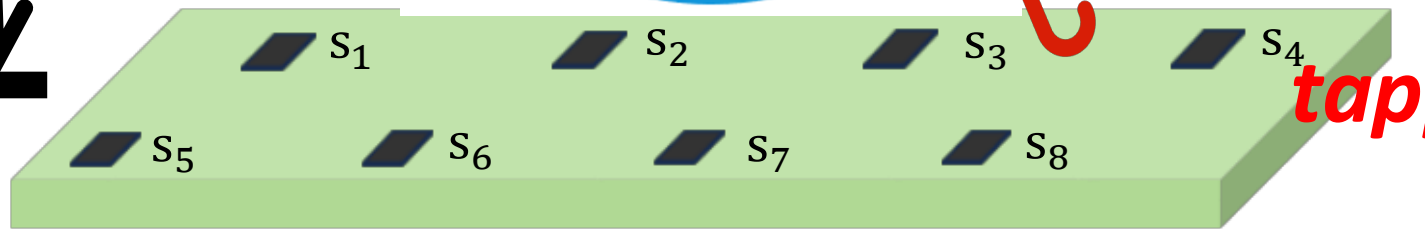
Design of DualStrike Attack Device --- System Overview



Design of DualStrike Attack Device --- Eavesdropping

Hall effect keyboard

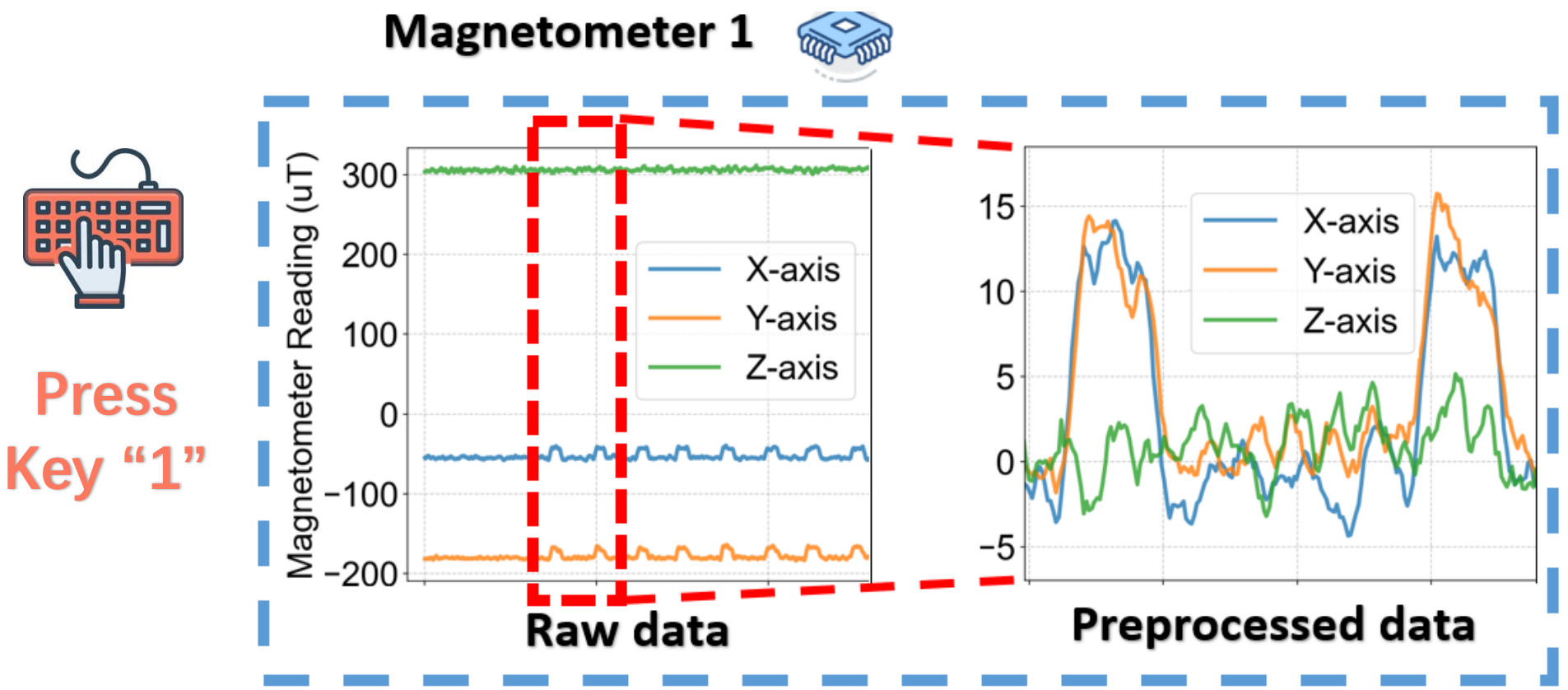
Common desk thickness



How to accurately catch *each tap* and *tapped key*?

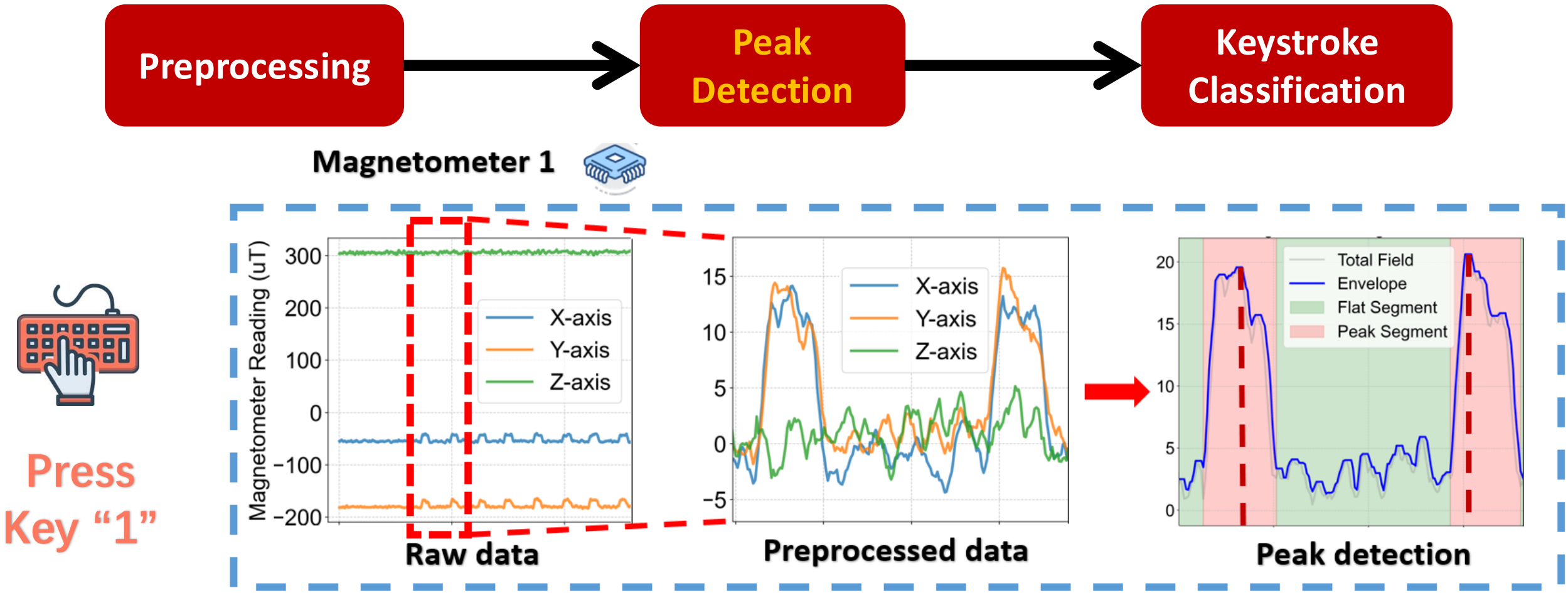
PCB--4*2 mlx90393 magnetometer array

Design of DualStrike Attack Device --- Eavesdropping



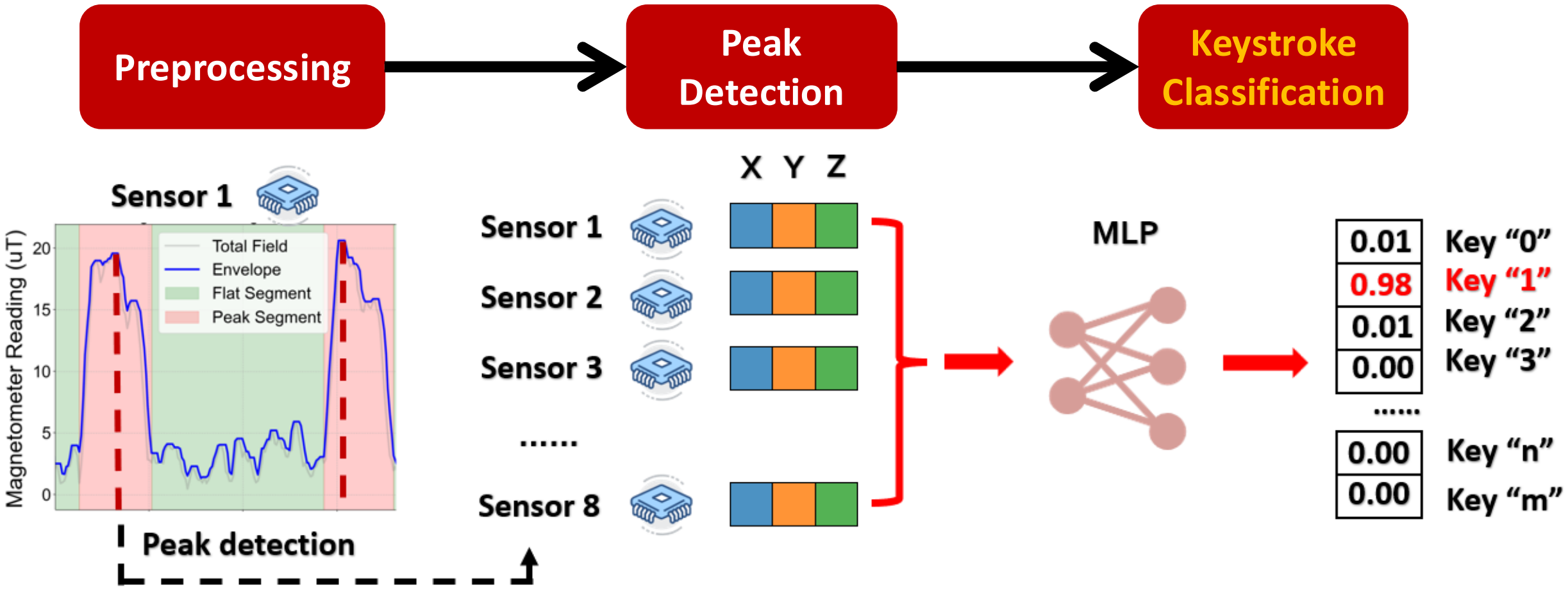
- Subtracted offset to eliminate environmental noise + Savitzky-Golay (SG) filter

Design of DualStrike Attack Device --- Eavesdropping



- Overall magnetic field strength of each sensor: $B_{overall} = \sqrt{mag_x^2 + mag_y^2 + mag_z^2}$
- Extract the local maximum and detect peak (**keystroke events**)

Design of DualStrike Attack Device --- Eavesdropping



- Input the reading of all magnetometers in peak time, and classify with a lightweight MLP model

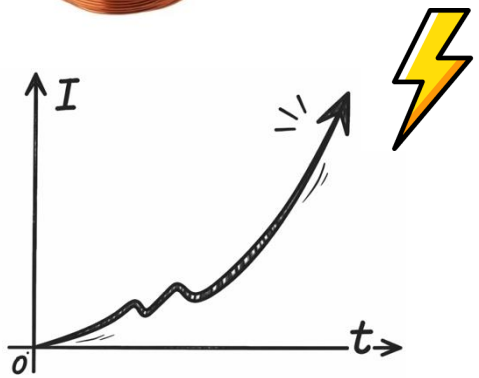
Design of DualStrike Attack Device --- Injection

Attack Unit(Electromagnet) Design

How to optimal Attack Electromagnet?

Attack unit driving circuit

How to achieve high-frequency spoofing circuit?



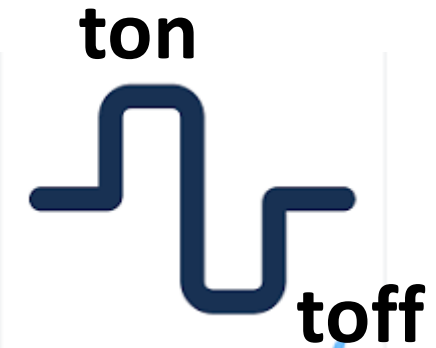
Whole Attack Device

How to integrate a universal attack device?

× N

Attack Parameter

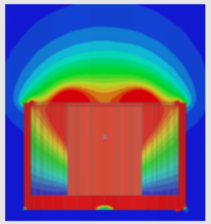
How to specific attack parameter for each keyboard?



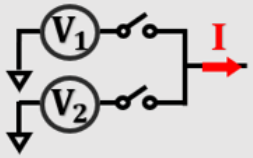
Design of DualStrike Attack Device --- Injection

Keystroke Injection

Design element 1
Optimal Attack Electromagnet



Design element 2
High-frequency Spoofing Circuit

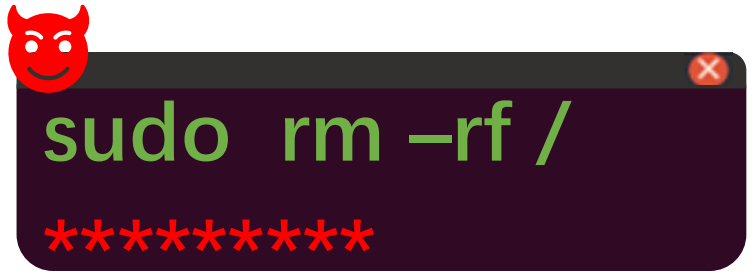


Design element 3
Attack Device

Design element 4
Attack Parameters

T_{on} T_{off}
V_{attack}

Accurate, high-APM injection



etc. inject 40 characters within 200 ms

faster than the human reaction time!

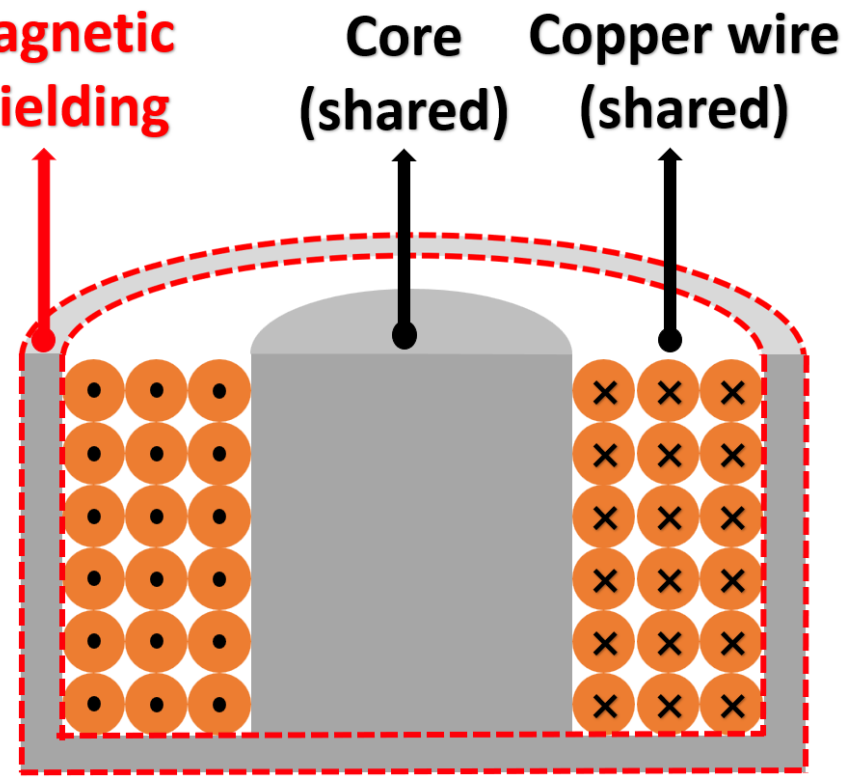
Injection (Design of Electromagnet)

What type: solenoid or suction?

Solenoid Electromagnet

Suction Electromagnet

Suction Electromagnet
With *extra shielding*



Injection (Design of Electromagnet)

What type: solenoid or suction?

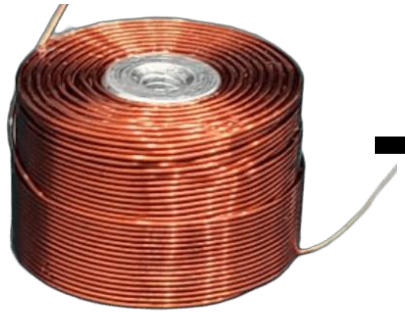
--- Finite element analysis (FEA) analysis

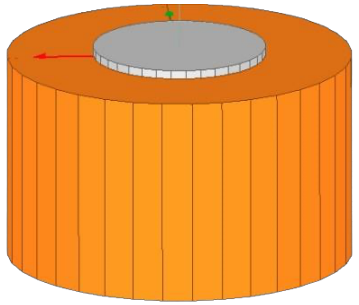
Physical model

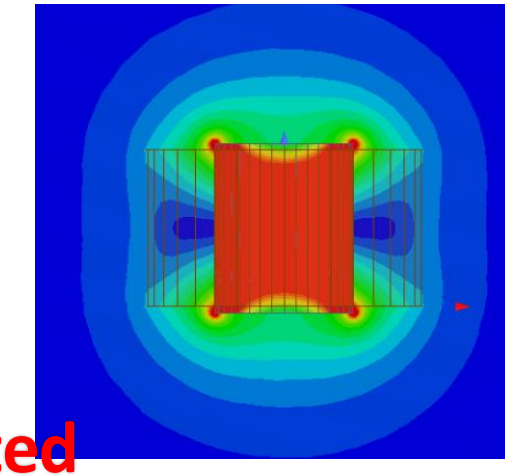
FEA model

Magnetic field contour

Solenoid Electromagnet

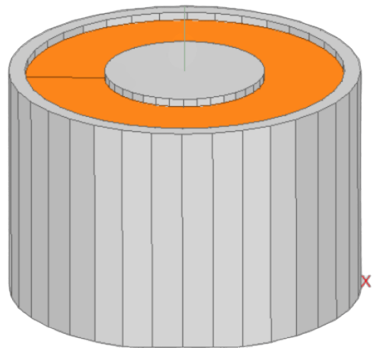


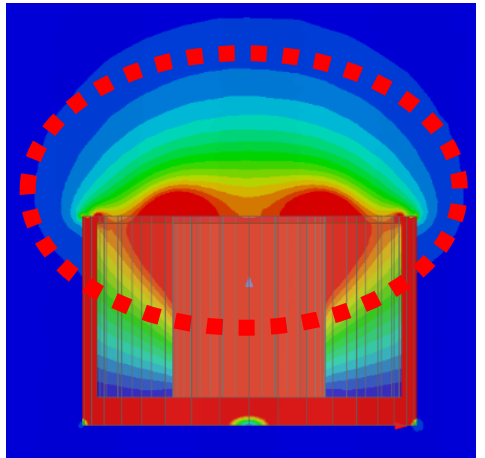




more concentrated field on one side

Suction Electromagnet



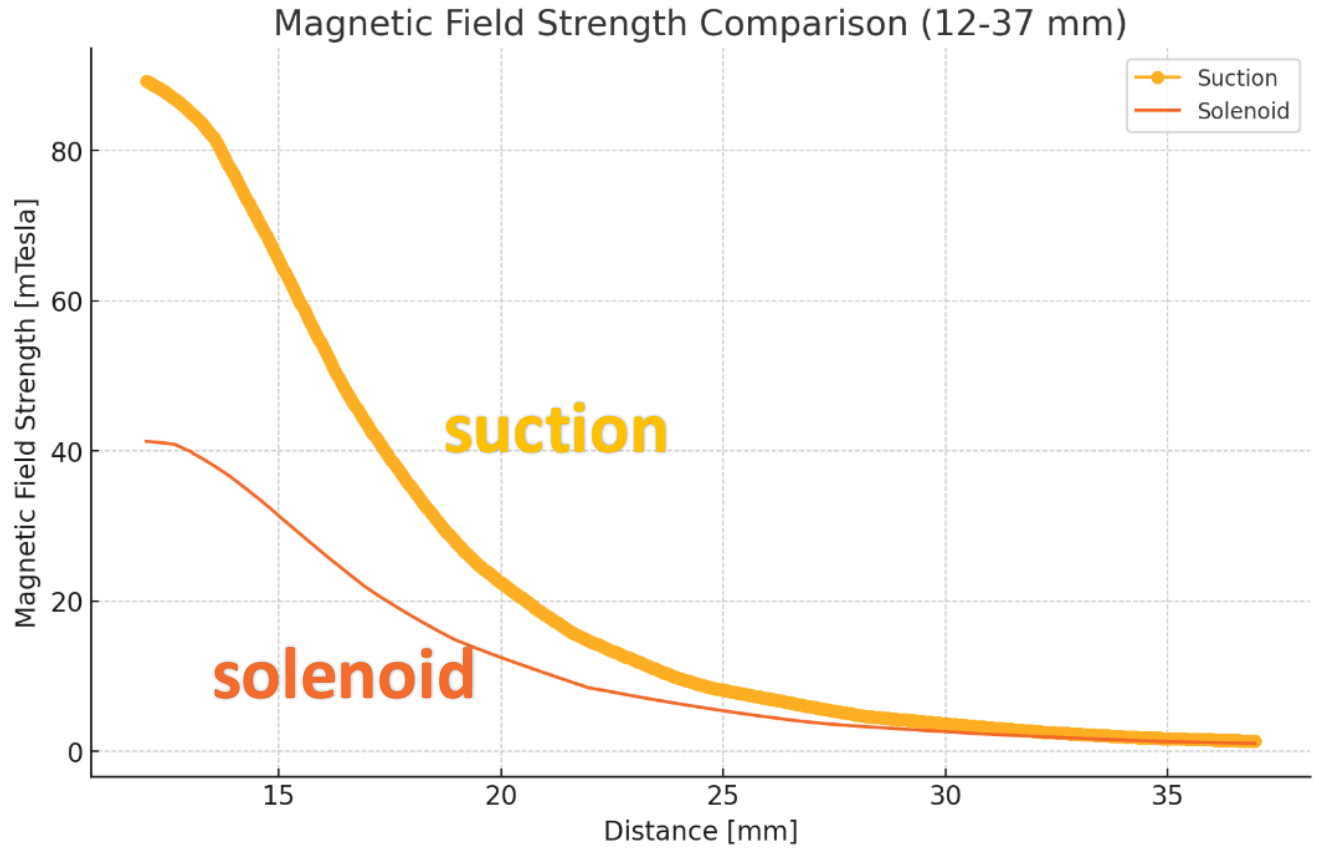


Injection (Design of Electromagnet)

What type: solenoid or suction?

--- Finite element analysis (FEA) analysis

Physical model



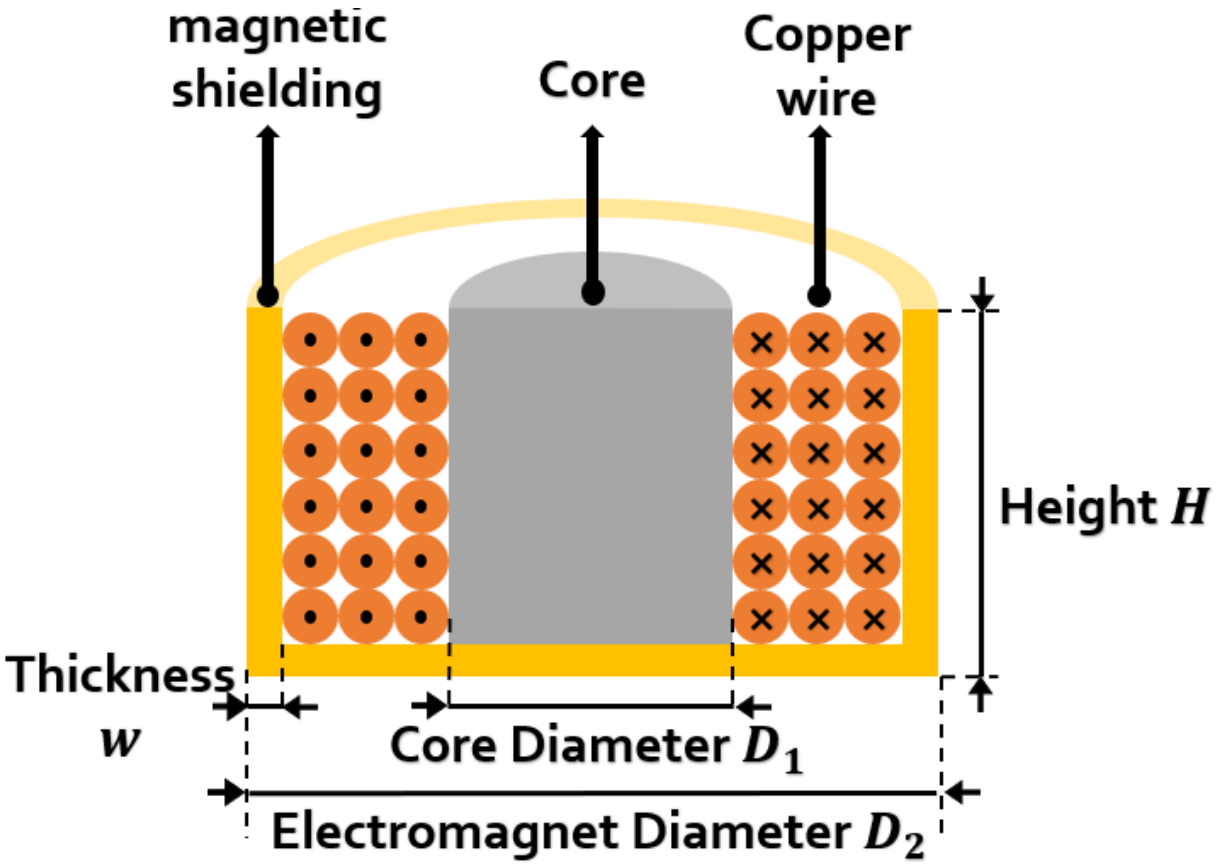
- Suction exhibits stronger magnetic field strength on

Injection (Design of Electromagnet)

type: **suction √**

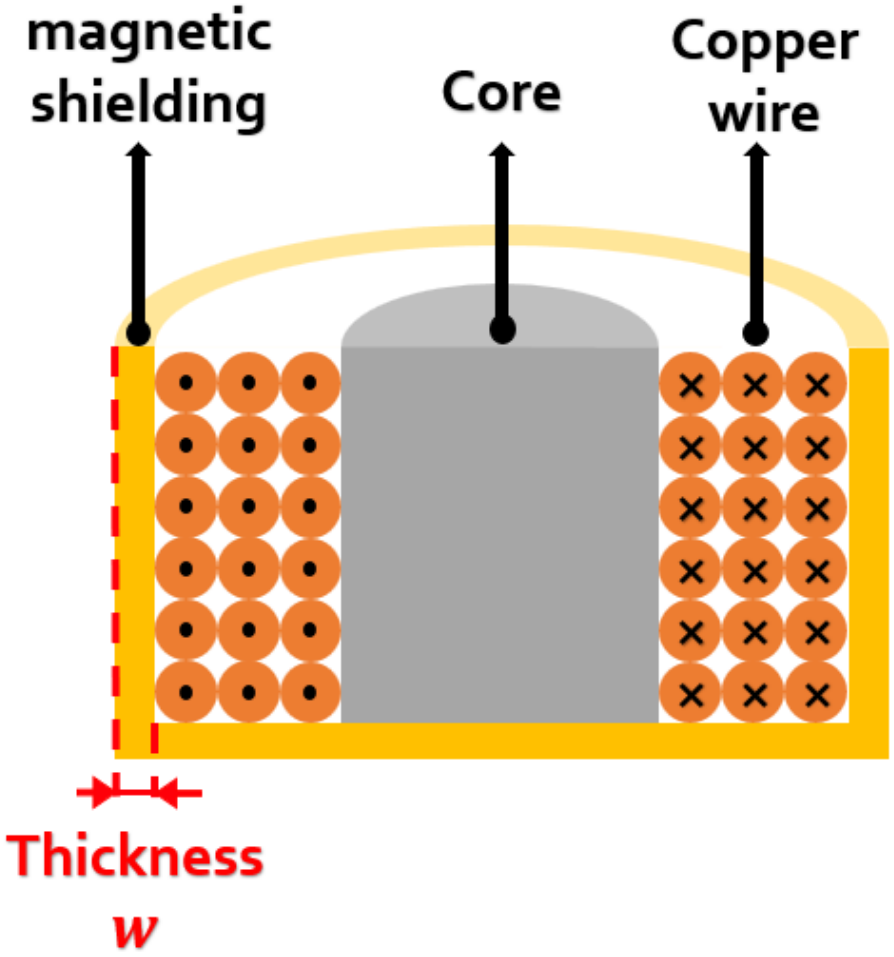
What size: shell thickness (W), height (H),
core diameter(D1), and overall diameter (D2) ?

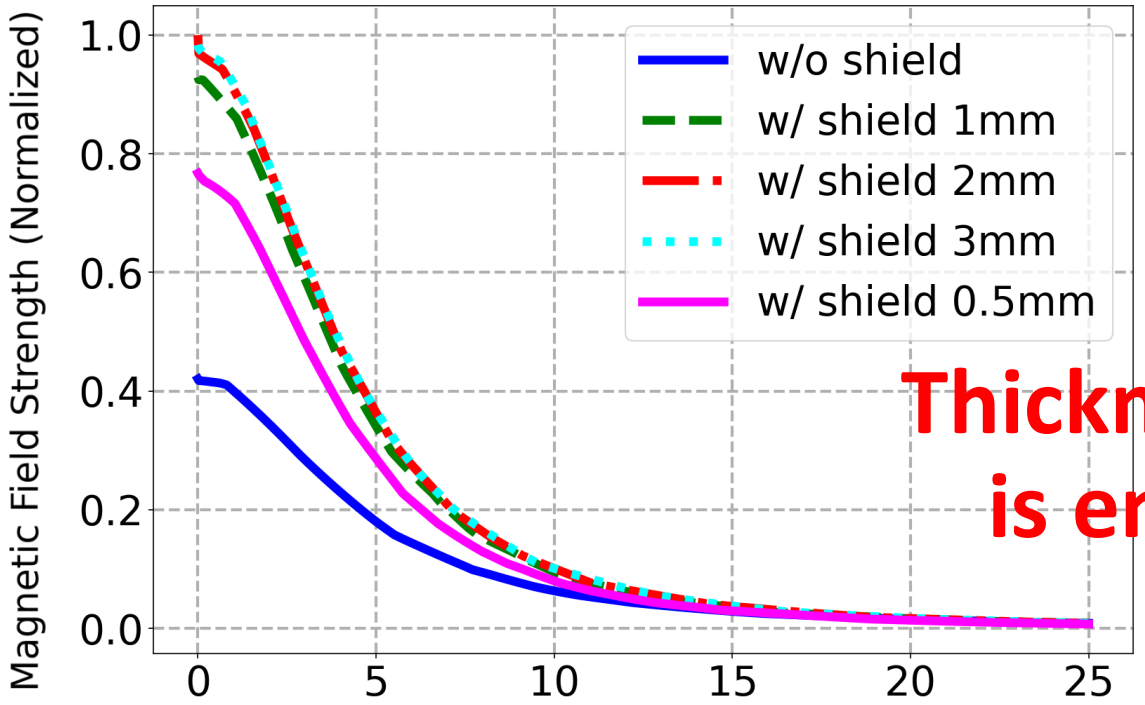
Suction Electromagnet



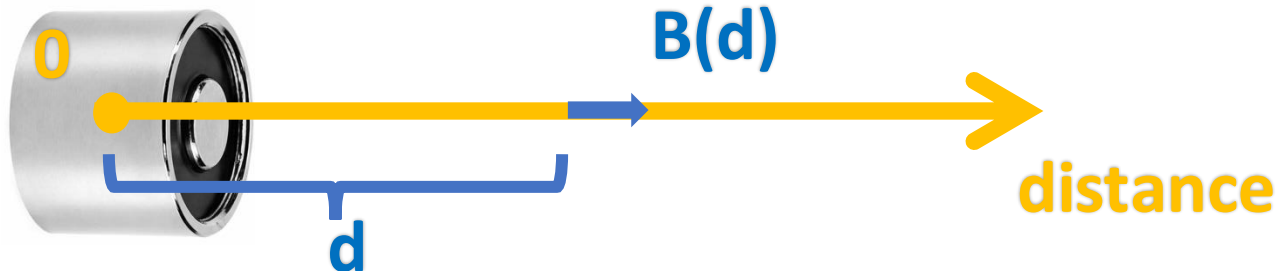
Injection (Design of Electromagnet)

What size: shell thickness (W)?



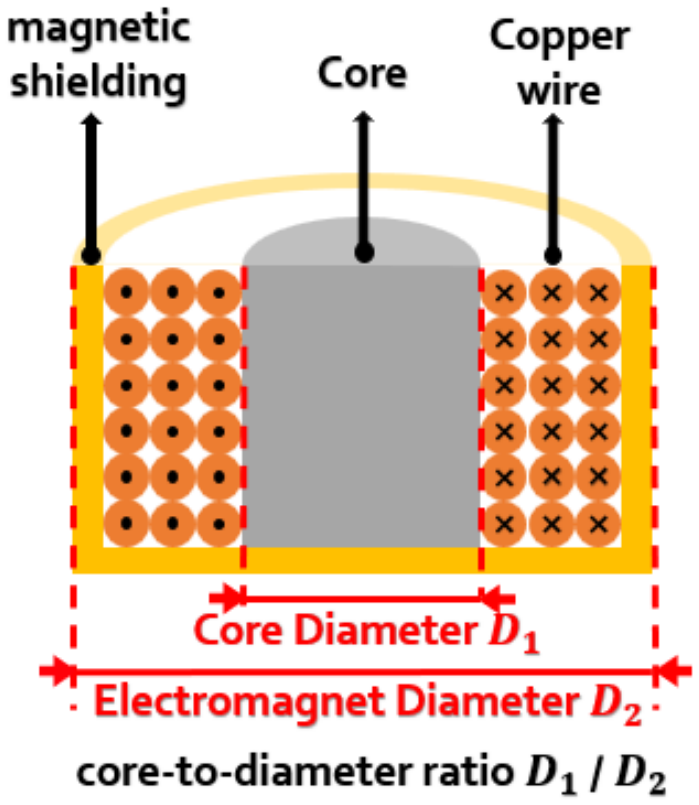


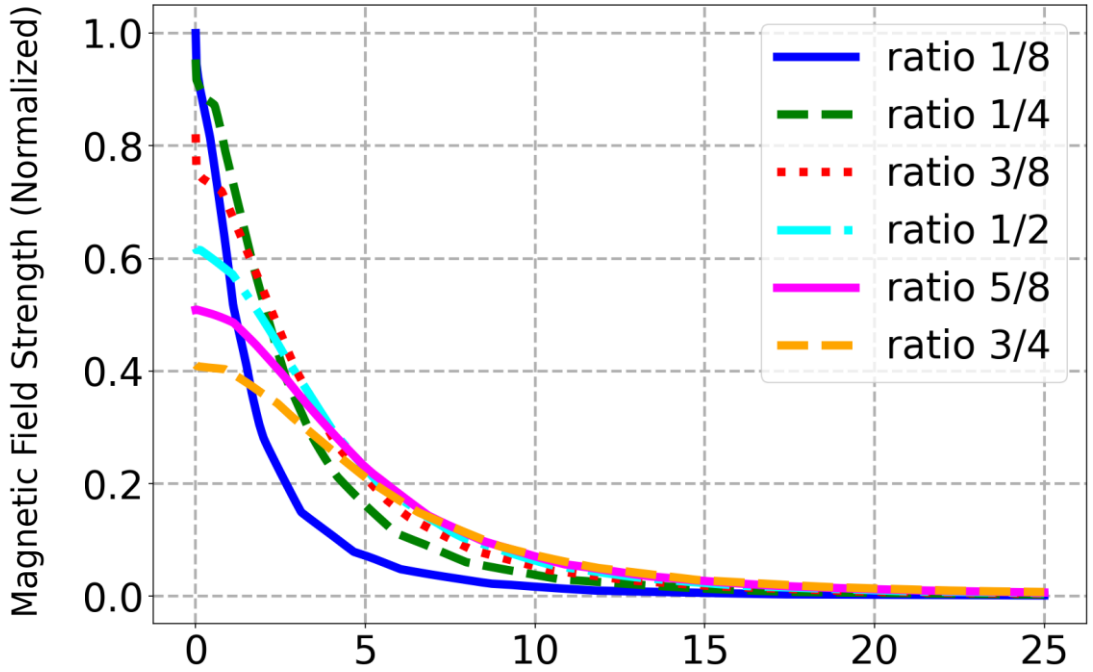
Thickness 1mm is enough



Injection (Design of Electromagnet)

What size: core diameter(D1), and overall diameter (D2) ?





Core ratio ½ is good

⬇

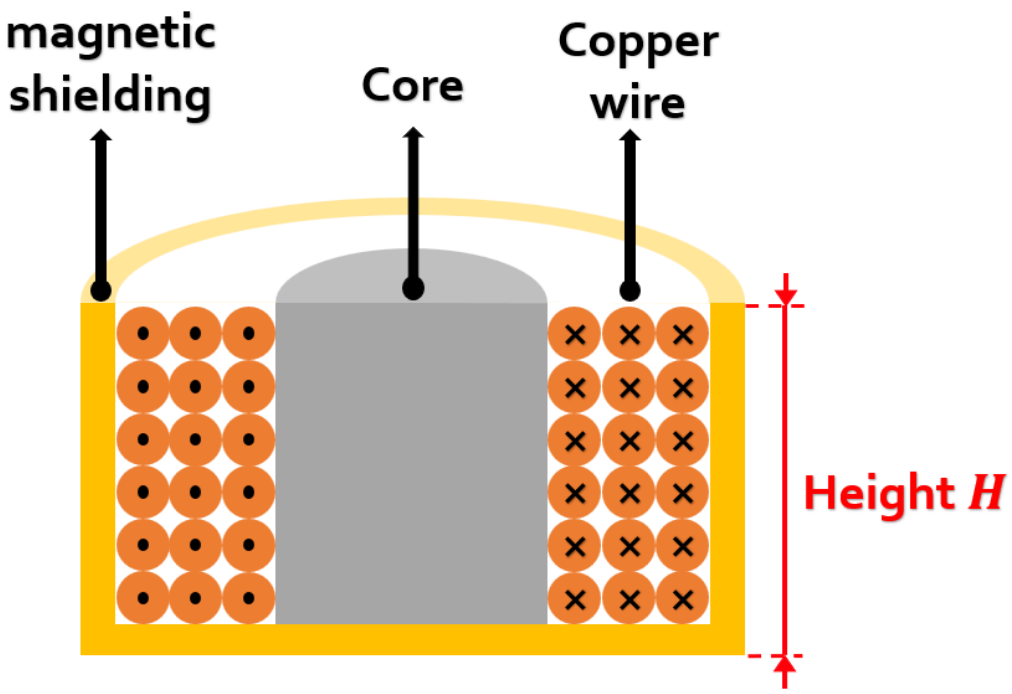
Key spacing is 19.05mm

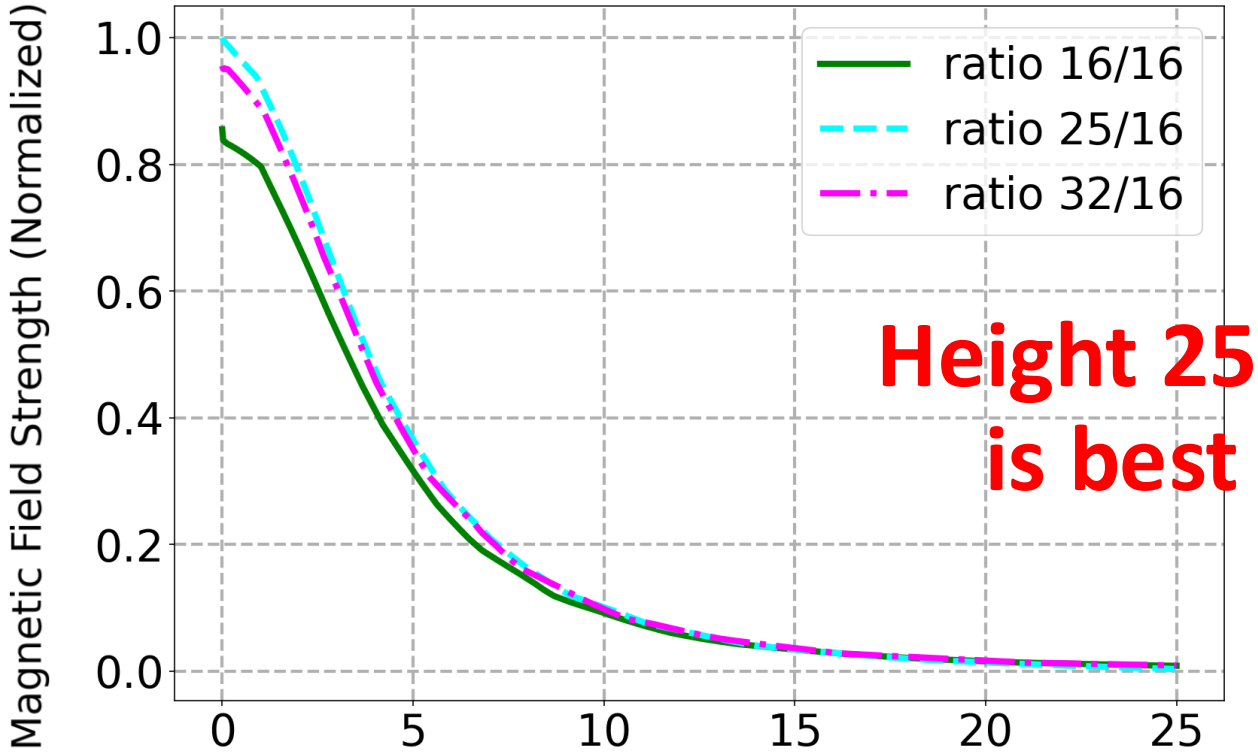
⬇

D1:8mm
D2:16mm

Injection (Design of Electromagnet)

What size: height (H) ?

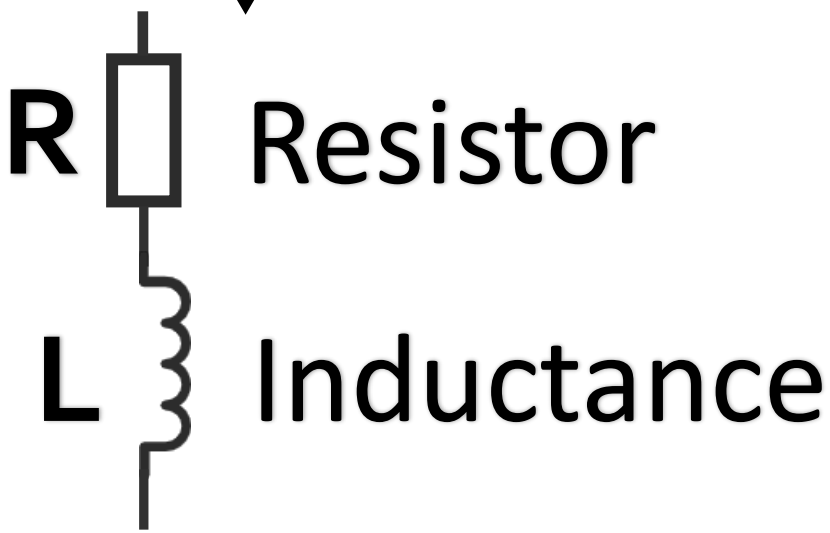


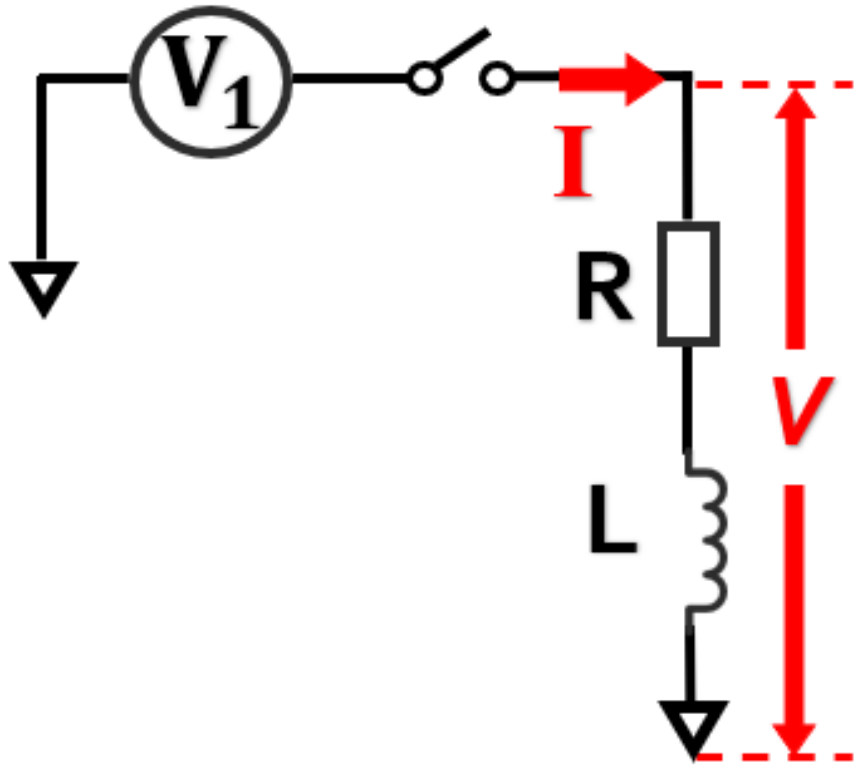


Height 25mm is best

Injection (High-frequency Magnetic Spoofing)

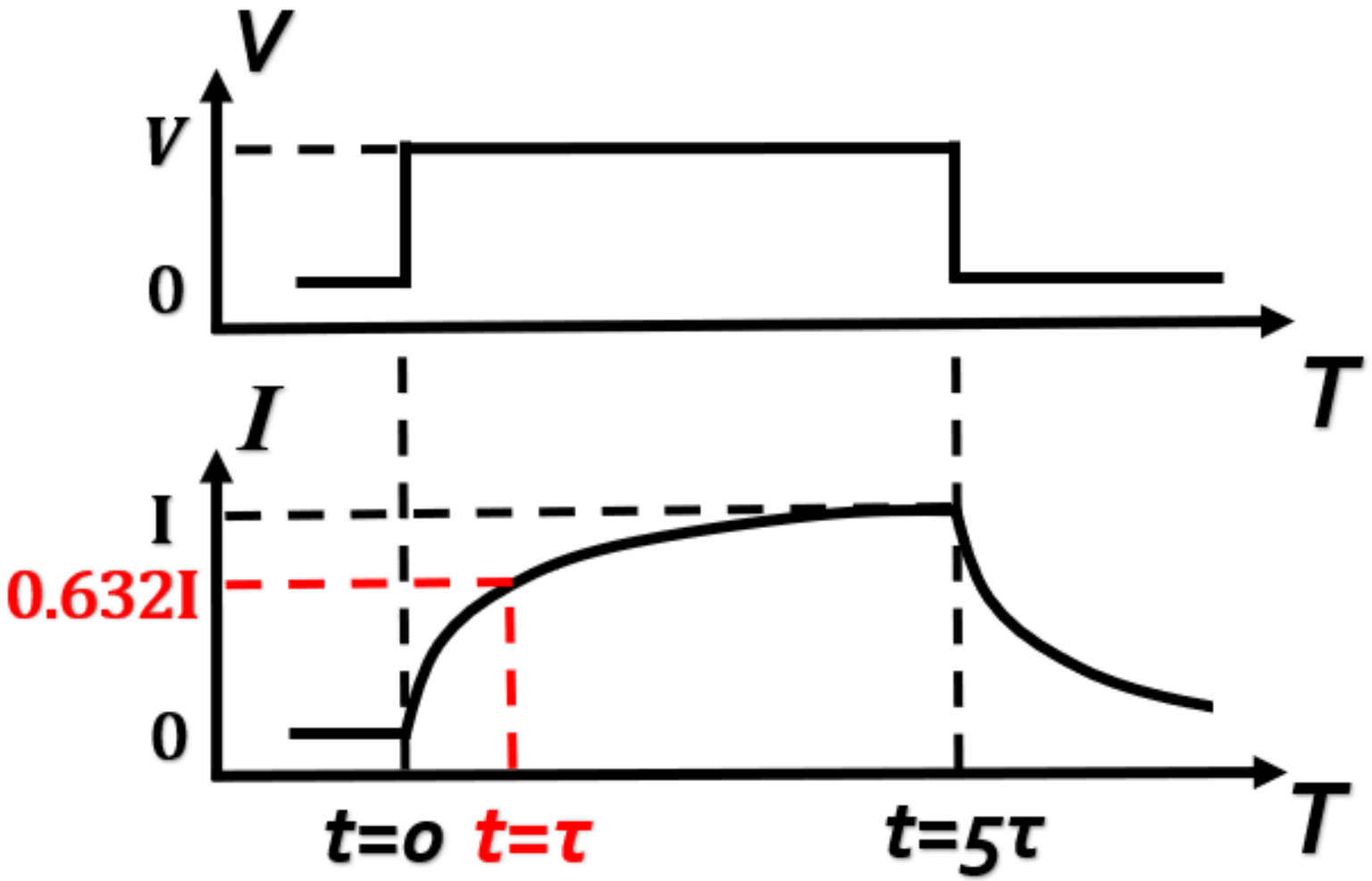
Electromagnet can be modelled as a RL model





Injection (High-frequency Magnetic Spoofing)

Electromagnet can be modelled as a RL model



$$I = \frac{v}{R}\left(1 - e^{-t/\tau}\right)$$

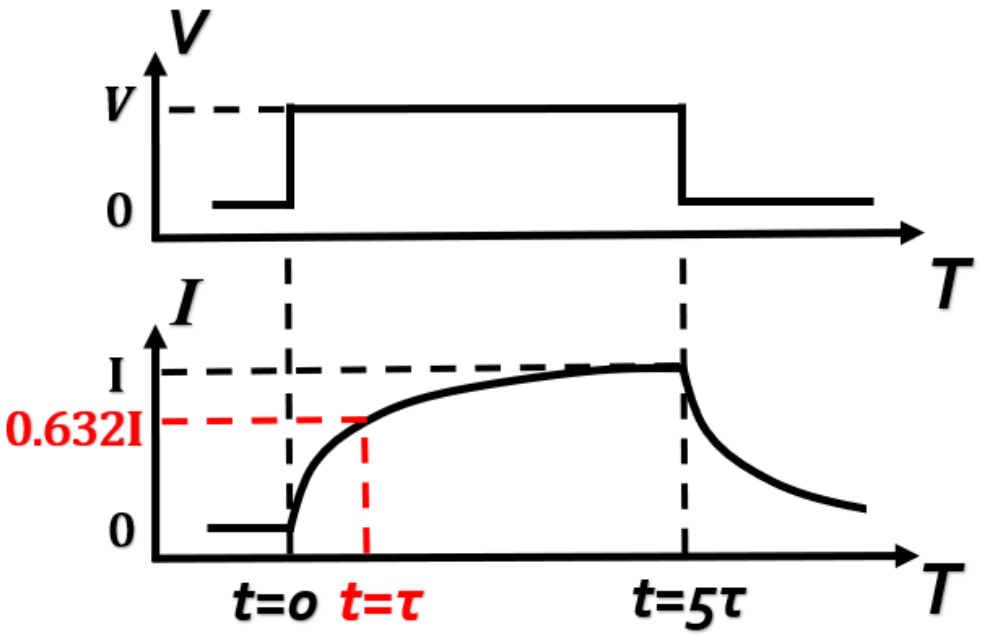
Time constant

τ = L / R

How fast circuit responds to input changes

Injection (High-frequency Magnetic Spoofing)

Electromagnet can be modelled as a RL model



$t=\tau \rightarrow I = 0.632 I_{max}$

$t=5\tau \rightarrow I \approx I_{max}$

For our optimal electromagnet

R=180Ω, L = 0.18H

→ *need 5ms to reach Imax!*

Keyboard Type	Scanning Type	Cycle
Wooting 60 HE	MUX-integrated	375 μs
Steelseries Pro	Matrix	990 μs
Keydous NJ98-CP	MUX-integrated	5160 μs
k70 Pro Max	Matrix	900 μs
Reddragon M61	Matrix	1000 μs
DrunkDeer A75 Pro	Matrix	880 μs

This is much larger than keyboard cycle time!

Injection (High-frequency Magnetic Spoofing)

How to speed up current preparing?

$t=\tau \rightarrow I = 0.632 I_{max}$

$t=5\tau \rightarrow I \approx I_{max}$

→ **the fastest current rise occurs during the initial τ period !**

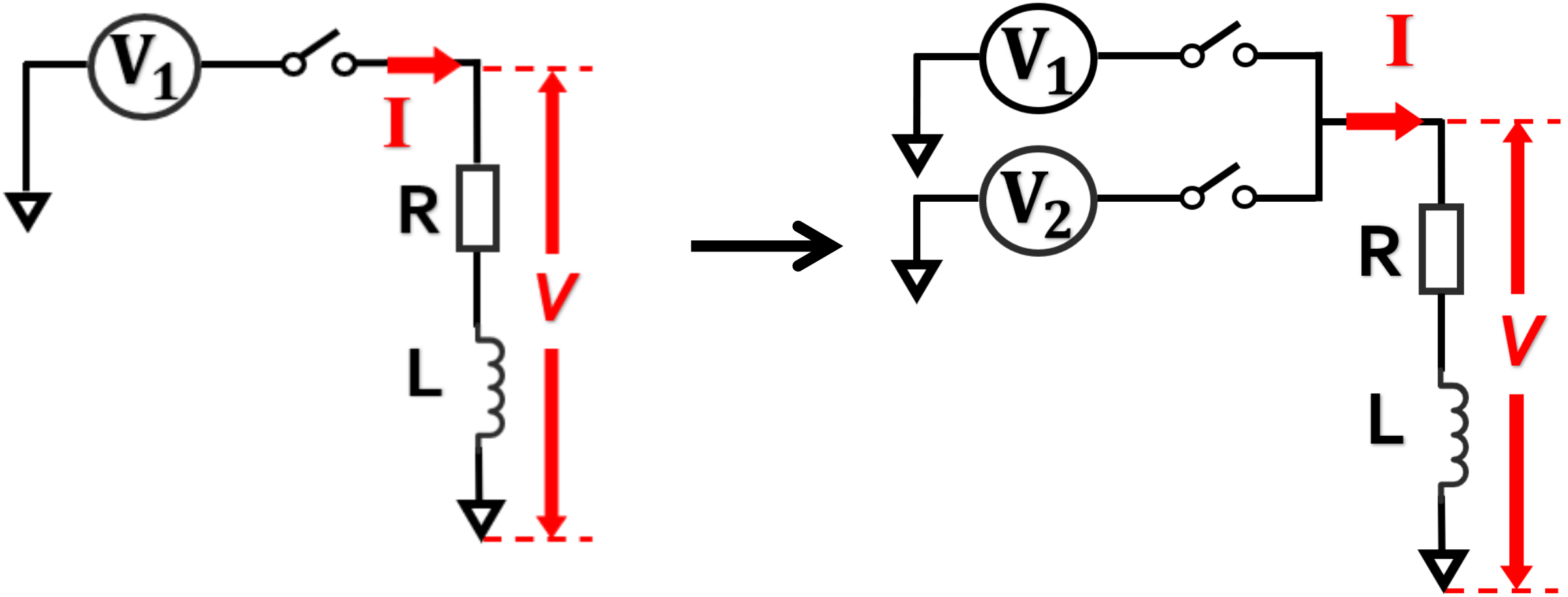
We can apply higher voltage in this phase, use this phase to reach Imax even faster

A Warm-up phase!

Injection (High-frequency Magnetic Spoofing)

How to speed up current preparing?

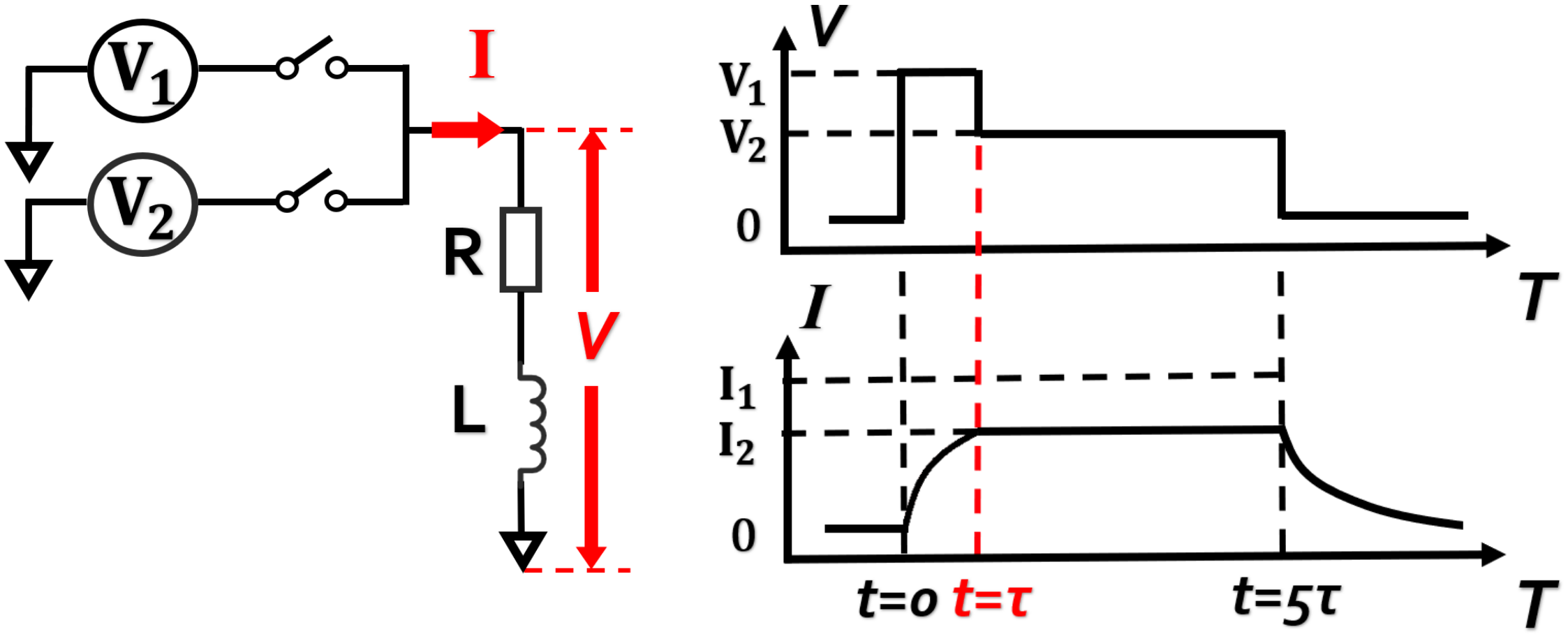
→ we use one more voltage



Injection (High-frequency Magnetic Spoofing)

How to speed up current preparing?

→ in warm-up phase, we apply higher voltage

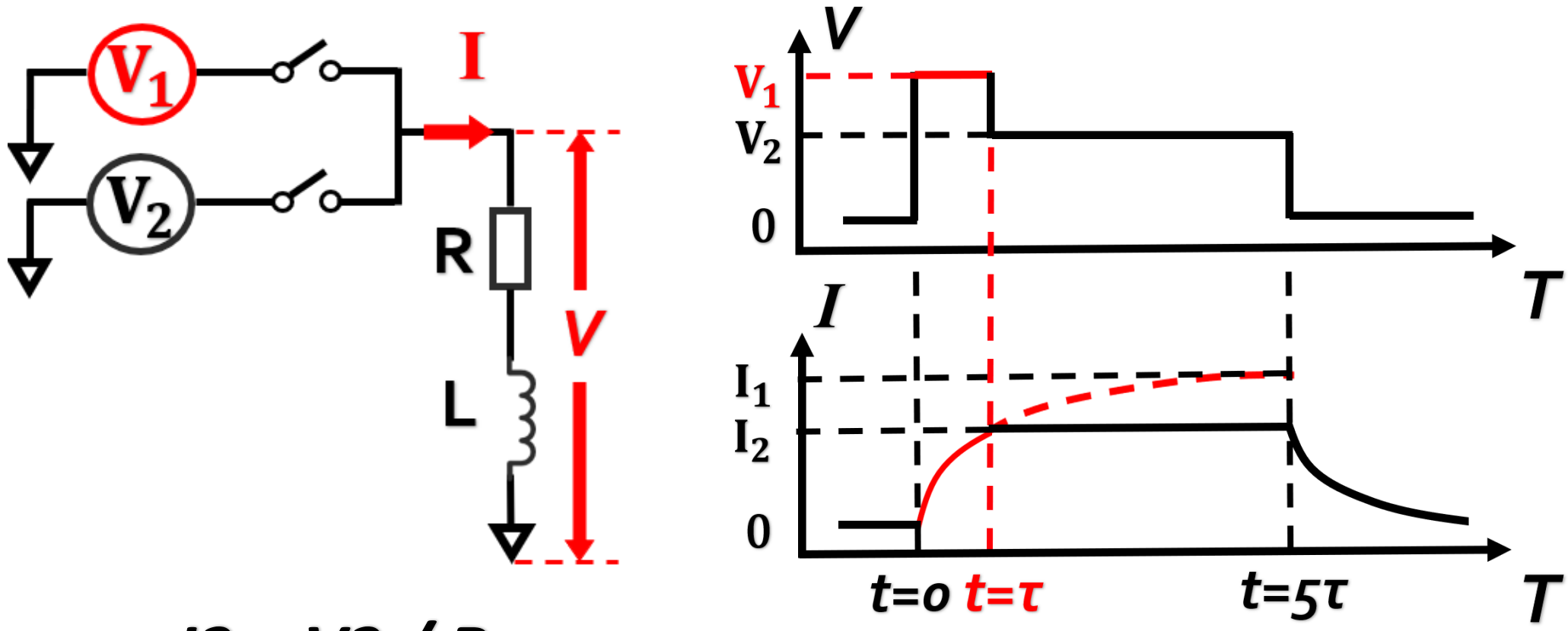


$$V = V1 * (u(t) - u(t-\tau)) + V2 * u(t-\tau)$$

Injection (High-frequency Magnetic Spoofing)

How to speed up current preparing?

→ in warm-up phase, we apply higher voltage



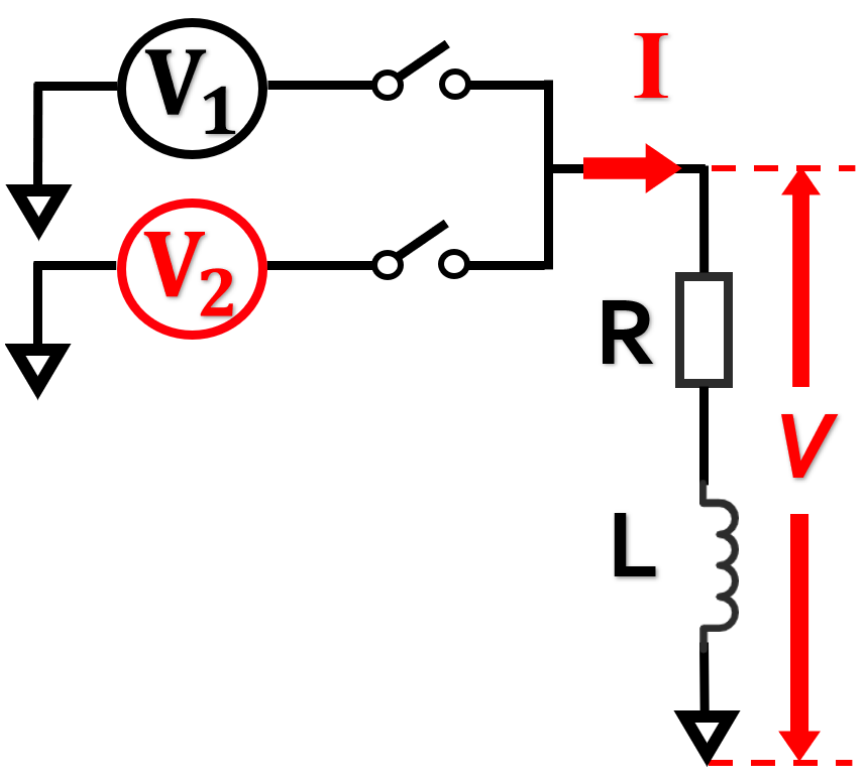
If Imax = I2 = V2 / R

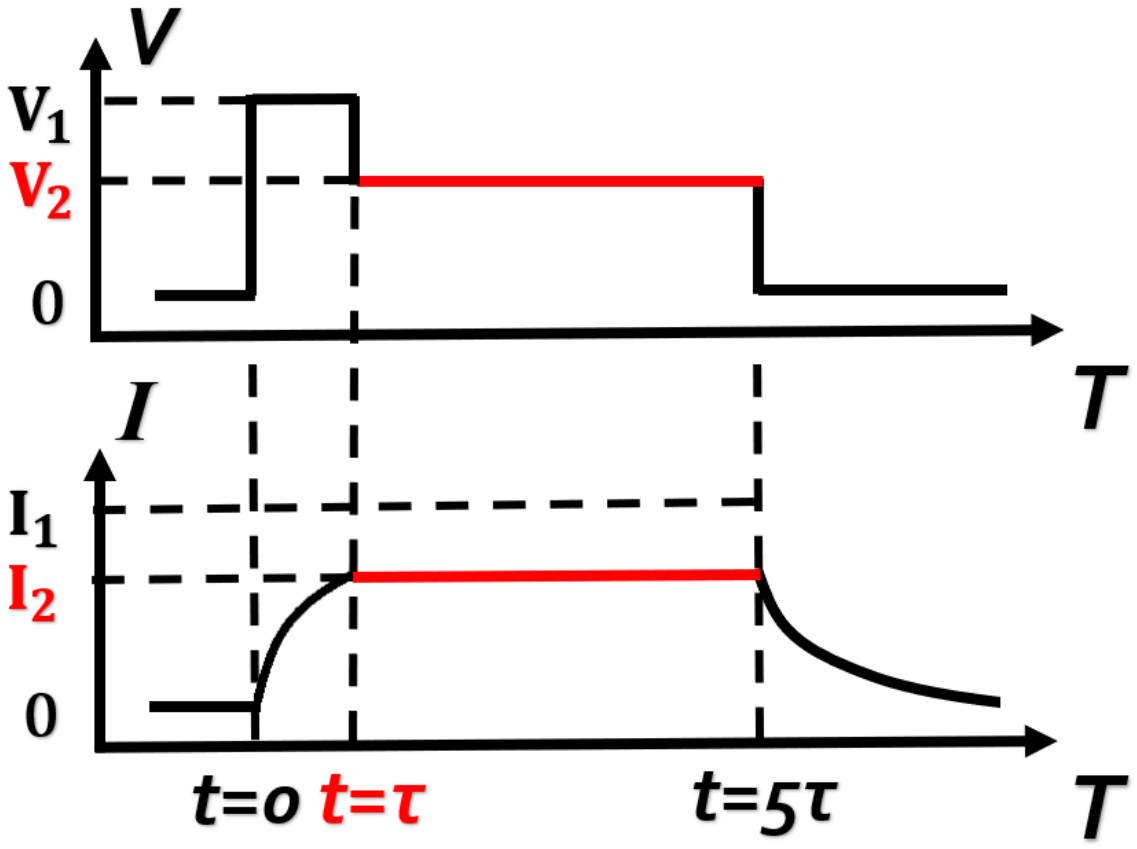
In warm-up phase, we apply V1 = V2/0.632, reach I2 when t= τ

Injection (High-frequency Magnetic Spoofing)

How to speed up current preparing?

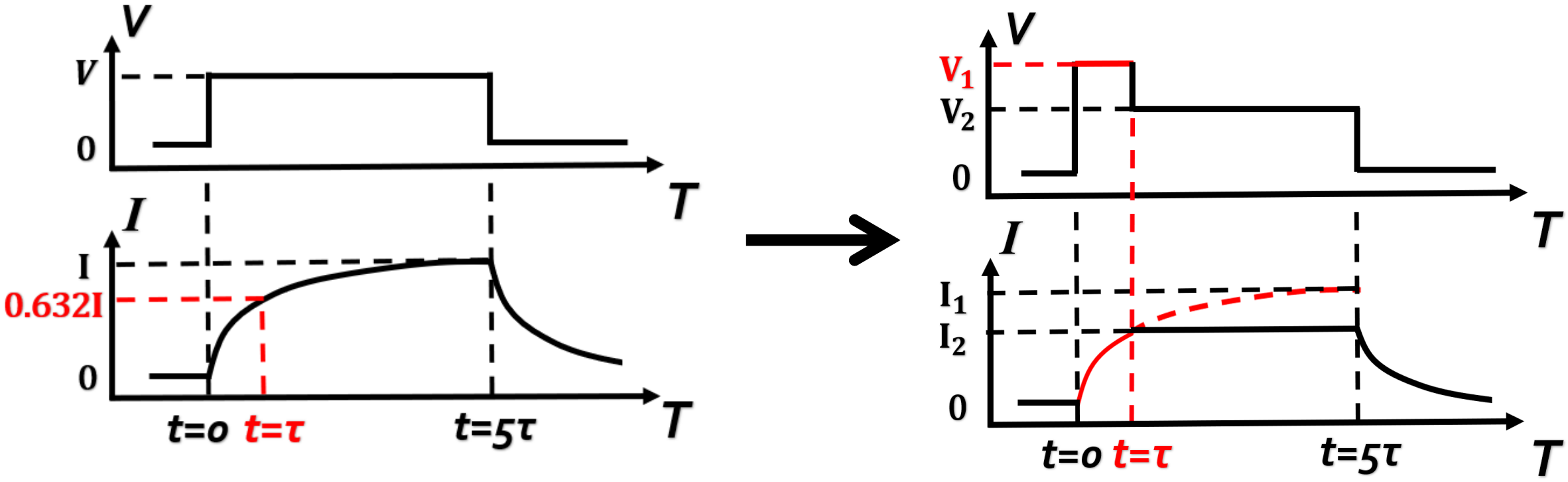
→ after this, maintain this max current





Switch V1 to V2 when t > τ

Injection (High-frequency Magnetic Spoofing)



rise time from 5τ → τ

enabling a 5× switching frequency

Injection (Attack device design)

We now have the eavesdropping magnetometer array, and the injection electromagnet array.

→ **However, Hall-effect keyboards come in different size**

→ **How to assemble a universal attack device**

Injection (Attack device design)

100% Hall effect keyboard

60% Hall effect keyboard

→ The layout of the main typing area is highly consistent

→ We focus on this part

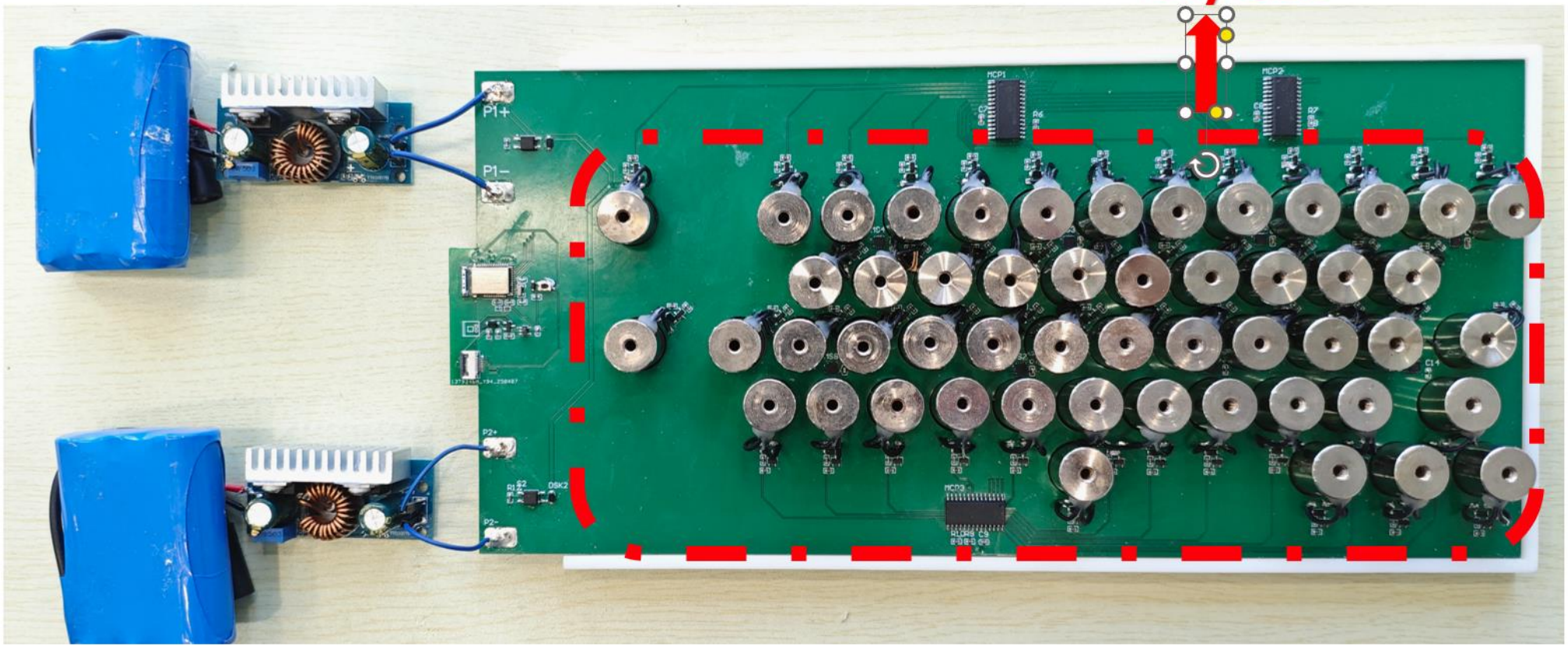
Injection (Attack device design) --Universal electromagnet layout

We target 51 keys, and their spacing/arrangement aligns with the main keyboard area

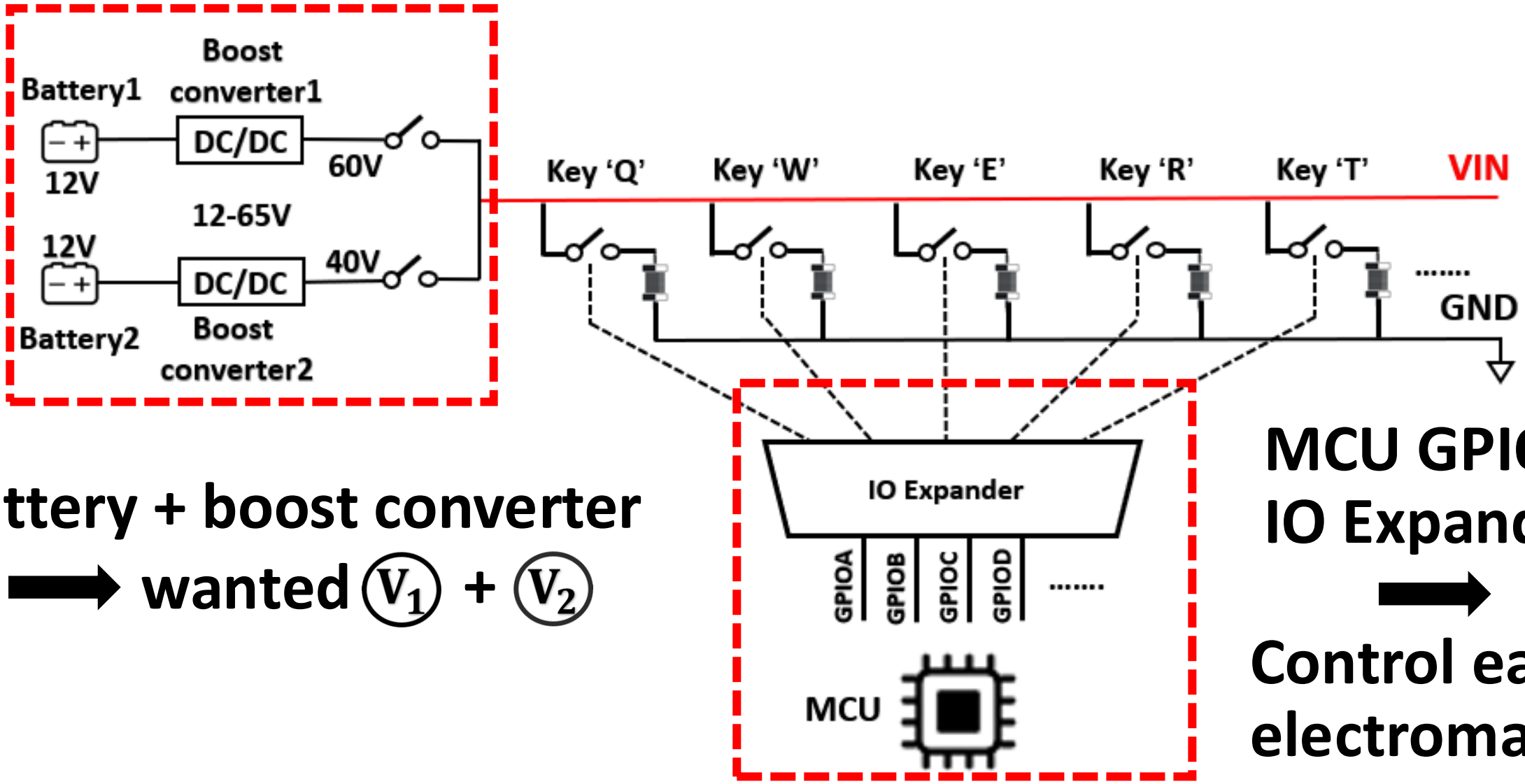
Type	Details
Letters	abcdefghijklmnopqrstuvwxyz
Symbol Keys	,./;’-
Control Keys	Shift,Ctrl,alt,OS,Esc,Backspace,Enter,CapsLk
Numeric Keys	1234567890
Whitespace	’ ’

Injection (Attack device design) --Universal electromagnet layout

We target 51 keys, and their spacing/arrangement aligns with the main keyboard area



Injection (Attack device design)
--Power supply && Switching for electromagnets



Battery + boost converter

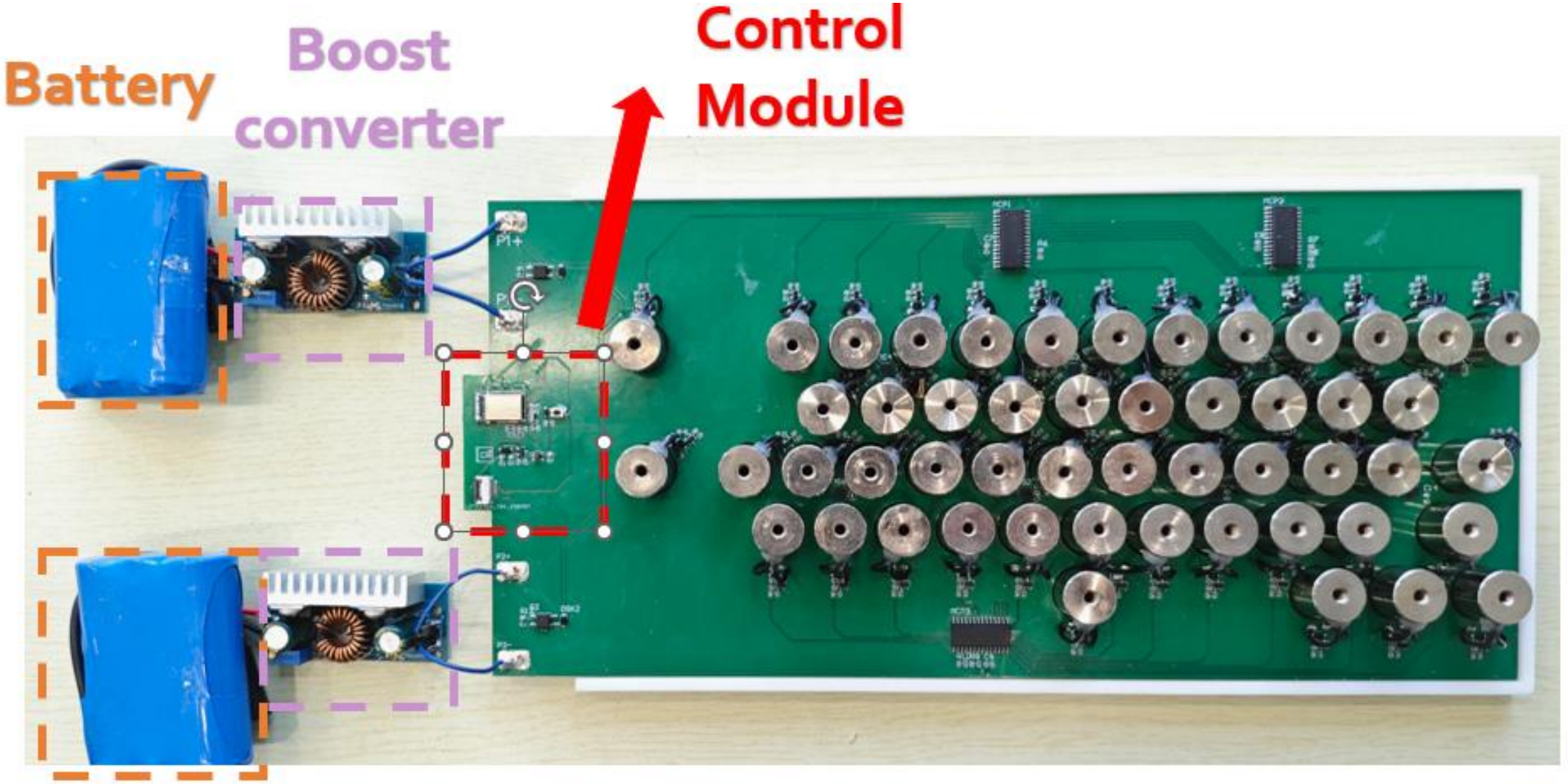
➡ wanted V_1 + V_2

MCU GPIO+
IO Expander

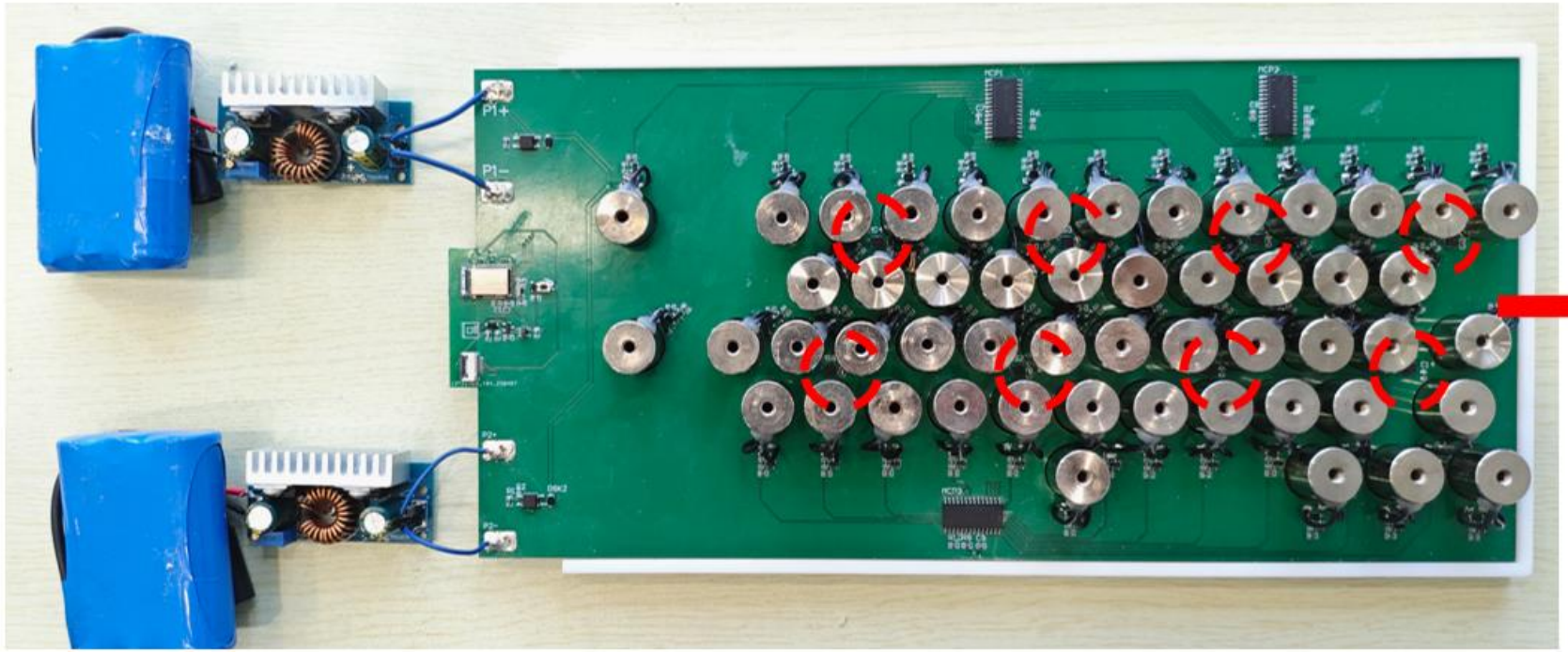
➡

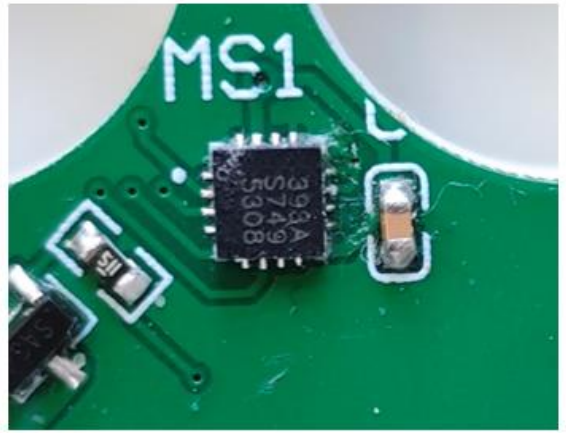
Control each electromagnet

Injection (Attack device design)
--Power supply && Switching for electromagnets



Injection (Attack device design)
--Listening magnetometer array





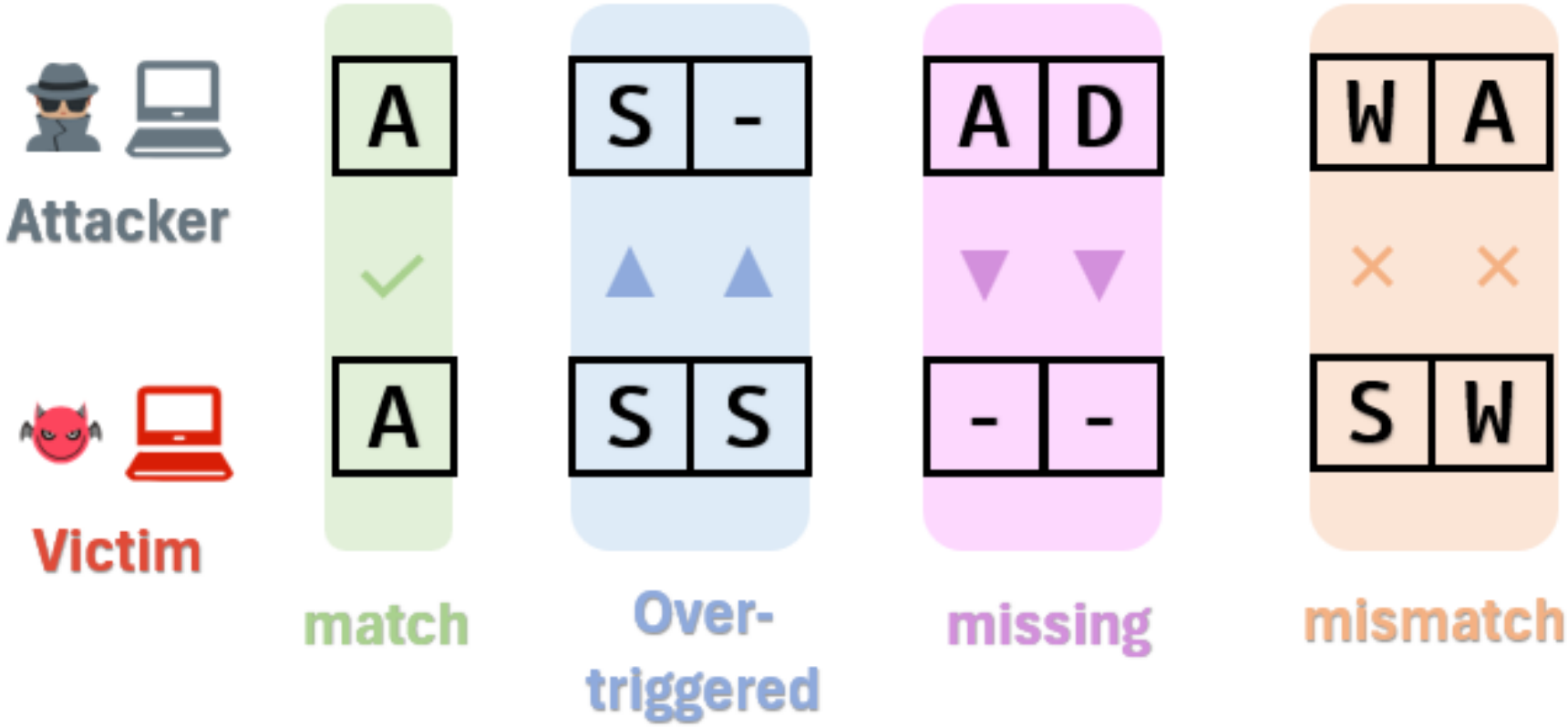
4*2 magnetometer array

Thus, our attack device can simultaneous perform listening + eavesdrop in a universal layout!

Injection (Attack Parameters design)

How to achieve an accurate keystroke injection?

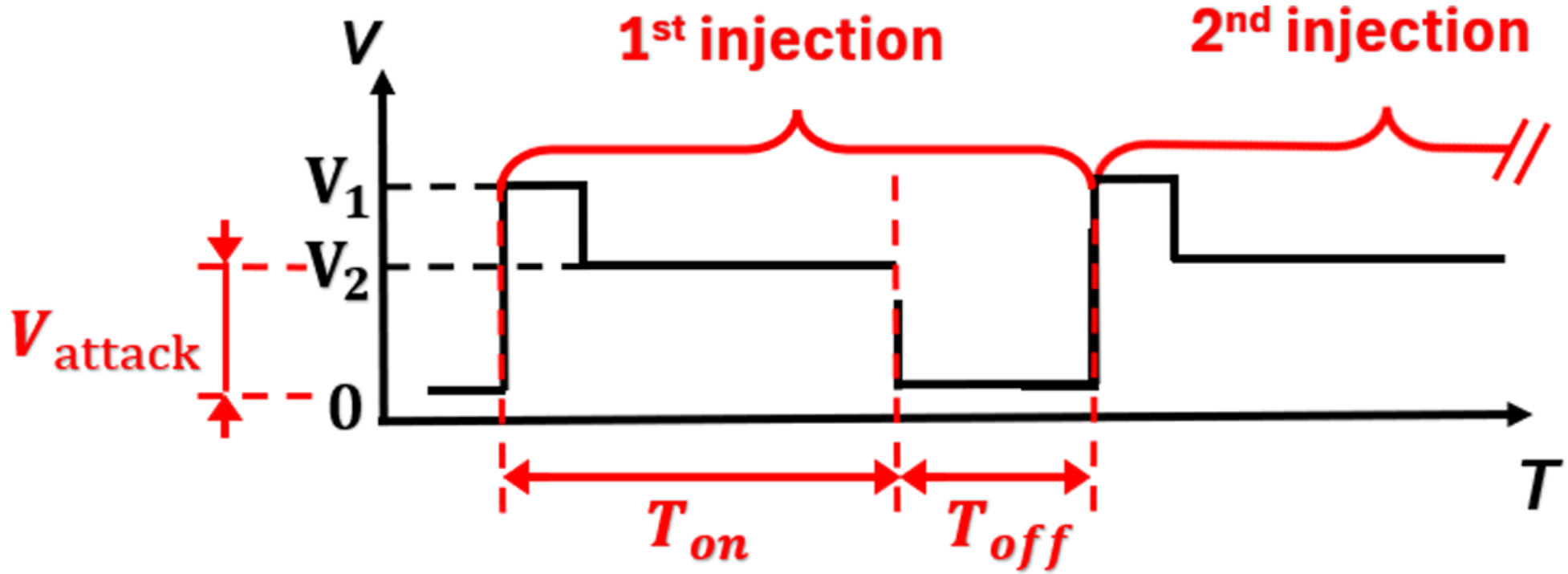
→There could be multiple consequences when injecting a keystroke



Injection (Attack Parameters design)

We define three parameters:

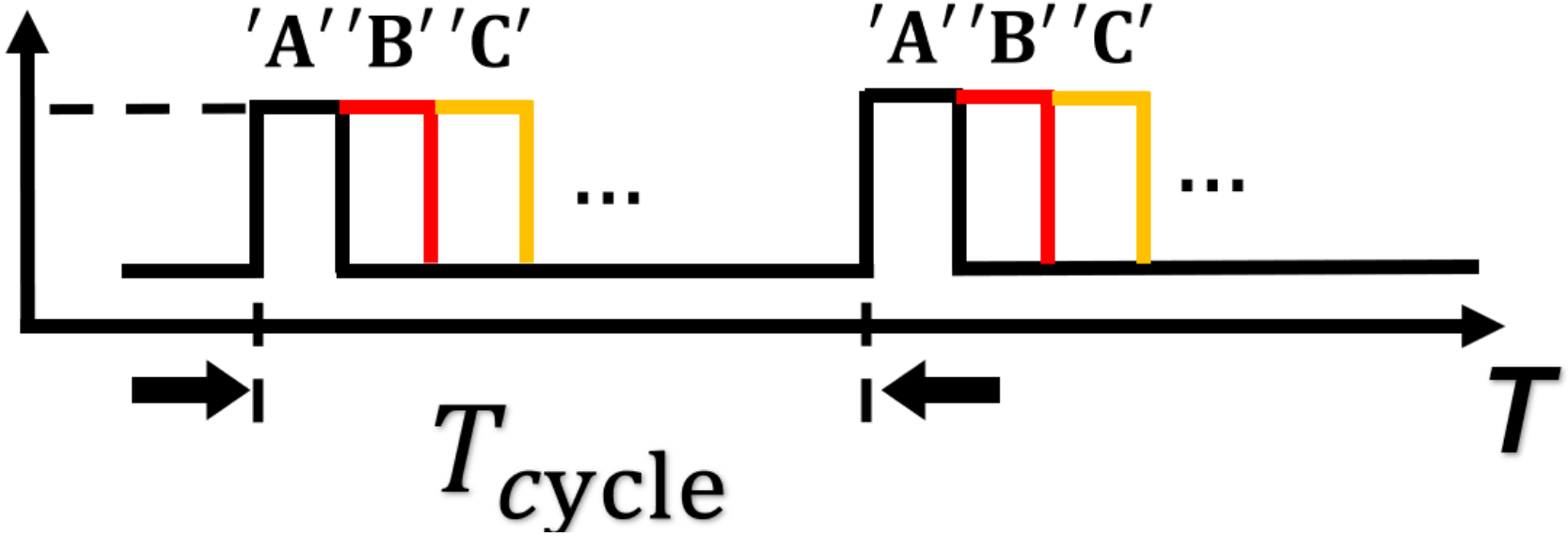
1) voltage activation time T_{on}
2) voltage deactivation time T_{off}
3) Activation voltage V_{attack}



Injection (Attack Parameters design)

scanning mechanism:
In a scan cycle keyboard scans all keys

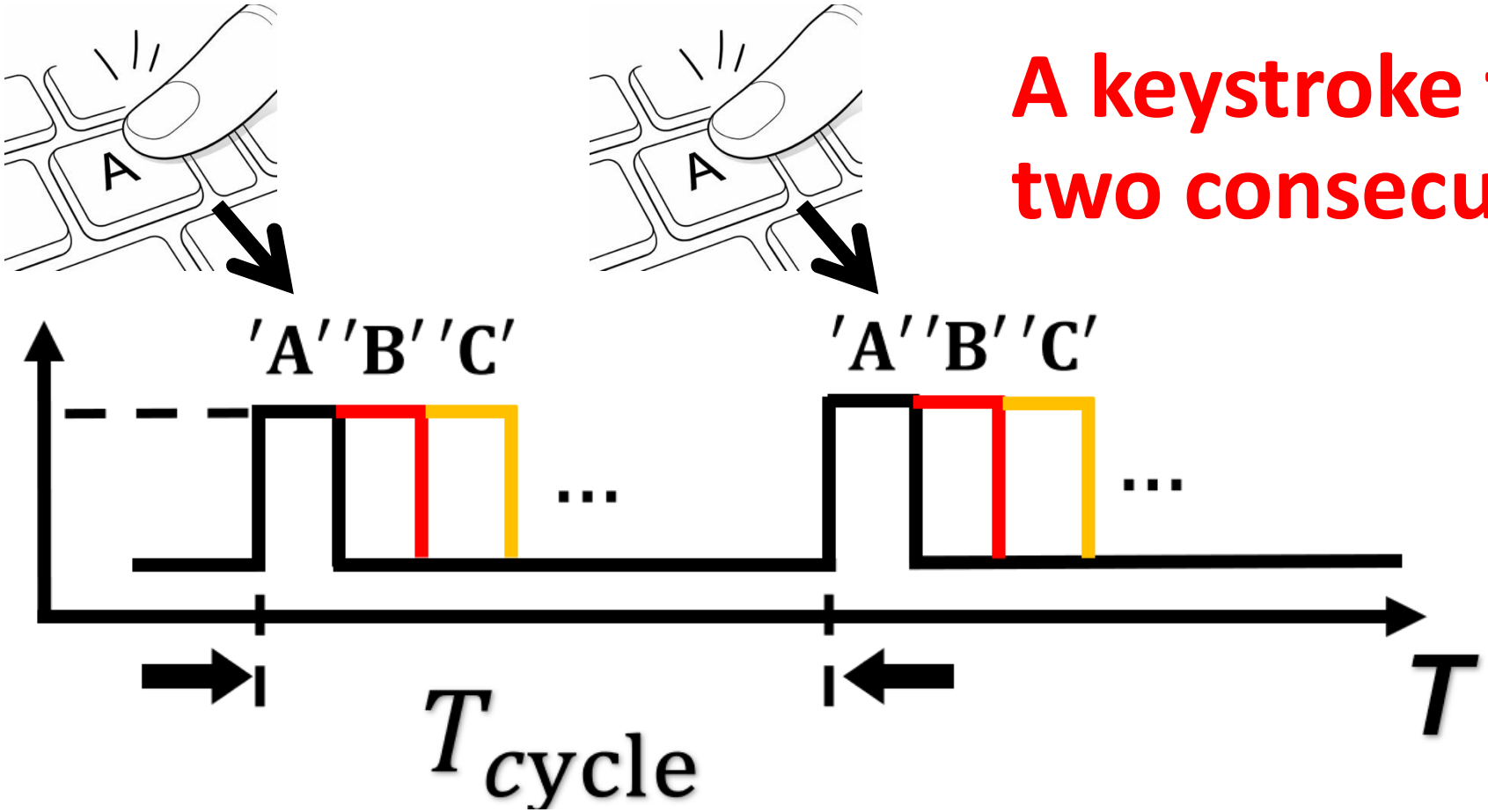
In key ‘A’s scan time, if it detects ‘A’ is tapped, Keystroke ‘A’ is registered!



Injection (Attack Parameters design)

scanning mechanism:

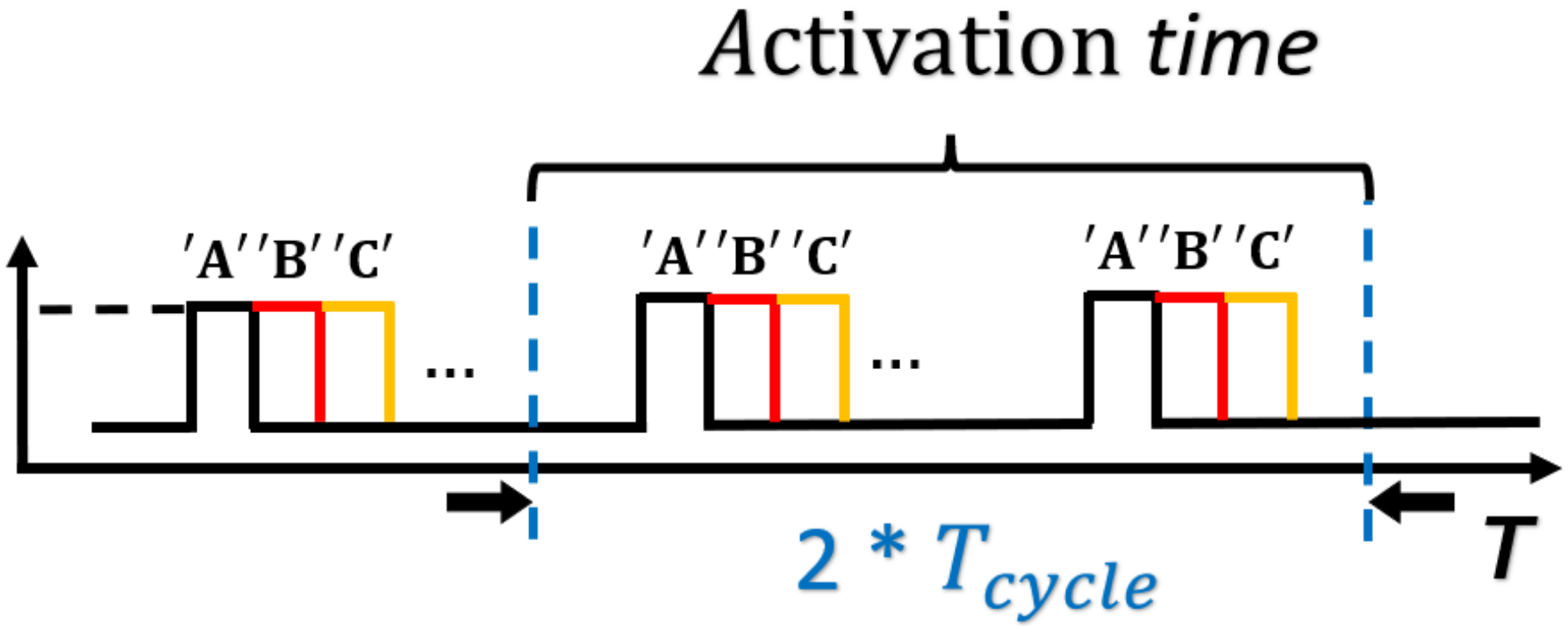
There is a debounce mechanism



A keystroke to be detected in two consecutive scan cycles!

Injection (Attack Parameters design)

1) voltage activation time T_{on}



If activation time ≥ 2* T_{cycle}, debounce is satisfied!
Also synchronization-free.

Injection (Attack Parameters design)

1) voltage activation time T_{on}

Thus $T_{\text{on}} \geq \tau + 2^{*}\, T_{cycle}$

Also if T_{on} is too long, there could be overtrigger.
smallest over-trigger for windows/ubuntu/macos is 300ms

$$300ms \geq T_{\text{on}} \geq \tau + 2^{*}\, T_{cycle}$$

Injection (Attack Parameters design)

2) deactivation time T_{off}

3) Activation voltage V_{attack}

V_{attack}: make sure magnetic field exceed the threshold depend on environment.

T_{off}: For two consecutive keystrokes:

if $T_{off} = 0$ → identify as one key

$$\begin{cases} T_{\min} < T_{\text{on}} < T_{\max},\ V_{\text{attack}} > V_{\min},\ T_{\text{off}} = 0 & \text{Key}_{\text{now}} \neq \text{Key}_{\text{next}} \\ T_{\min} < T_{\text{on}} < T_{\max},\ V_{\text{attack}} > V_{\min},\ T_{\text{off}} = T_{\text{cycle}} & \text{Key}_{\text{now}} = \text{Key}_{\text{next}} \end{cases}$$

Displacement Calibration

Now we can accurately listen and inject when aligned

→what if displaced during usage?

In this case, dx = 6cm, dy = 2cm

Displacement Calibration

→How can we infer this displacement?

Attacker can prompt victim to input specific pre-determined keys

Etc. predetermined Wi-Fi password in library/coffee shop

Displacement Calibration

→Use pre-determined sequence to infer

victim inputs this pre-determined sequence(e.g. wifi password)
In listening, the listened keys changed due to movement
If password is ’26B.’

Key true		Key predicted
2	→	T
6	→	O
B	→	S
.	→	H

Displacement Calibration

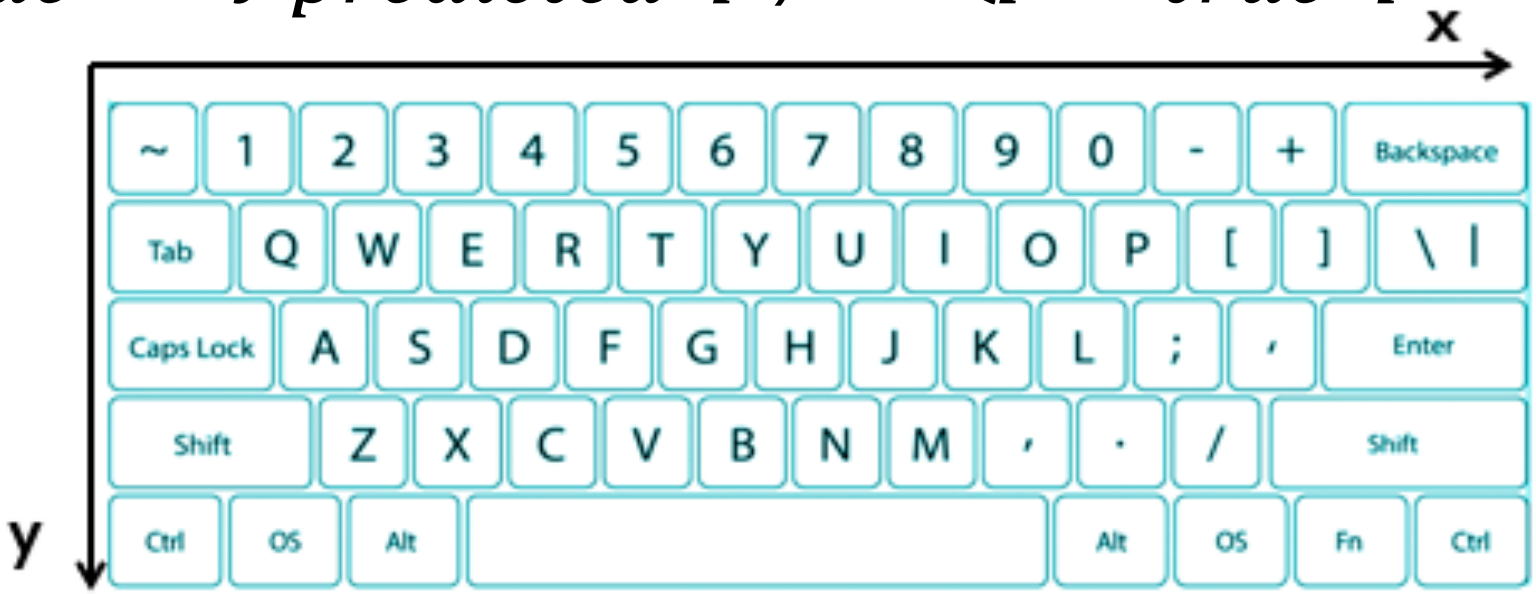
→calculate displacement with this key pairs

Each key has a 2D coordinate:

$$(key_{true}, key_{predicted}) \rightarrow (pos_{true}, pos_{predicted})$$

With inference confidence:

$$(key_{true}, key_{predicted}, p) \rightarrow (pos_{true}, pos_{predicted}, p)$$



Displacement Calibration

→we can apply a weighted least-squares (WLS) algorithm to estimate the displacement (dx,dy,θ)

$$\min_{\mathrm{dx},\mathrm{dy},\theta} \sum_{i=1}^{n} \|\mathbf{pos}_{\mathrm{predicted},i} - (\mathbf{R}(\theta) \cdot \mathbf{pos}_{\mathrm{true},i} + [\mathrm{dx}, \mathrm{dy}]^\top)\|^2 \cdot \mathrm{p}_i$$

$(\mathrm{key}_{\mathrm{true}}, \mathrm{key}_{\mathrm{predicted}}, p)$

(2,T,0.98)

(6,O,0.97)

(B,S,0.99)

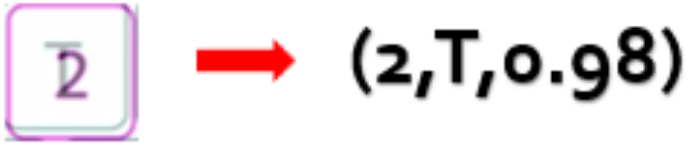
(.,H,0.99)

dx = 6.50cm
dy = 2.00cm
theta = 0.0rad

Displacement Calibration

→after obtain displacement, we can apply remapping to inferred keys and injected keys

→infer and inject the right keys!



Infer: a press intended for "2" may be sniffed as "T"

$$\mathbf{pos}^{cali}_{\text{eavesdrop}} = \mathbf{R}^{-1}(\theta) \cdot (\mathbf{pos}_{\text{eavesdrop}} - [\text{dx}, \text{dy}]^\top)$$

Injection: if the attacker intends to press key "2", remap, and find the nearest key to new position

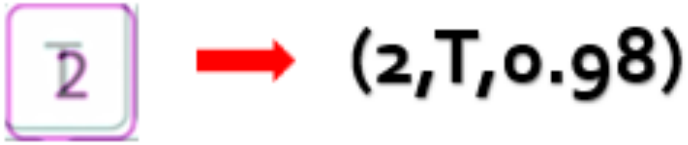
→ attack key 'T' now

$$\mathbf{pos}^{cali}_{\text{inject}} = \mathbf{R}(\theta) \cdot \mathbf{pos}_{\text{inject}} + [dx,\ dy]^\top.$$

Displacement Calibration

→after obtain displacement, we can apply remapping to inferred keys and injected keys

→infer and inject the right keys!



Infer: a press intended for "2" may be sniffed as "T"

$$\mathbf{pos}^{cali}_{\text{eavesdrop}} = \mathbf{R}^{-1}(\theta) \cdot (\mathbf{pos}_{\text{eavesdrop}} - [\text{dx}, \text{dy}]^\top)$$

Injection: if the attacker intends to press key "2", remap, and find the nearest key to new position

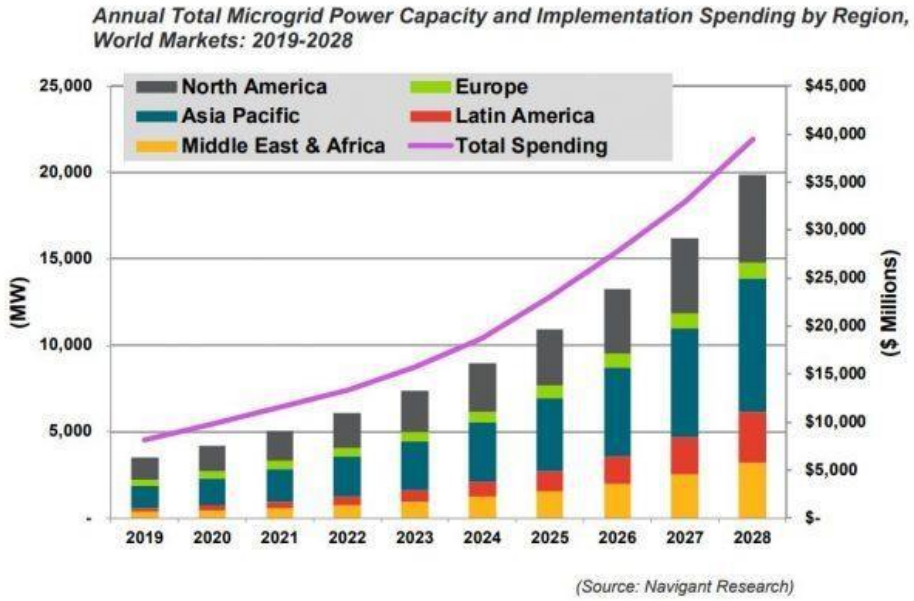
→ attack key 'T' now

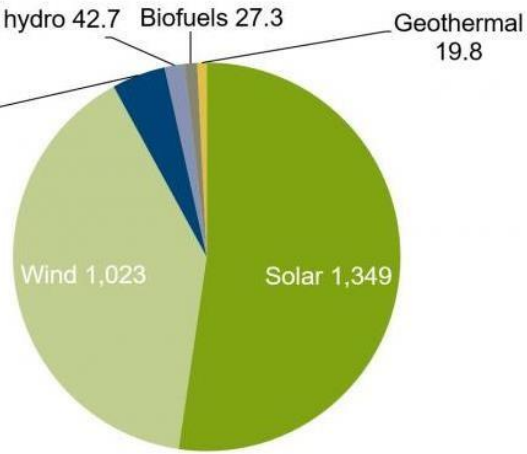
$$\mathbf{pos}^{cali}_{\text{inject}} = \mathbf{R}(\theta) \cdot \mathbf{pos}_{\text{inject}} + [dx,\ dy]^\top.$$

Hall Spoofing: A Noninvasive DoS Attack on Grid-Tied Solar Inverter

Credit: Anomadarshi Barua, Mohammad Abdullah Al Faruque
Department of Electrical Engineering and Computer Science, University of California, Irvine (UCI)

Solar Inverter Market Growth

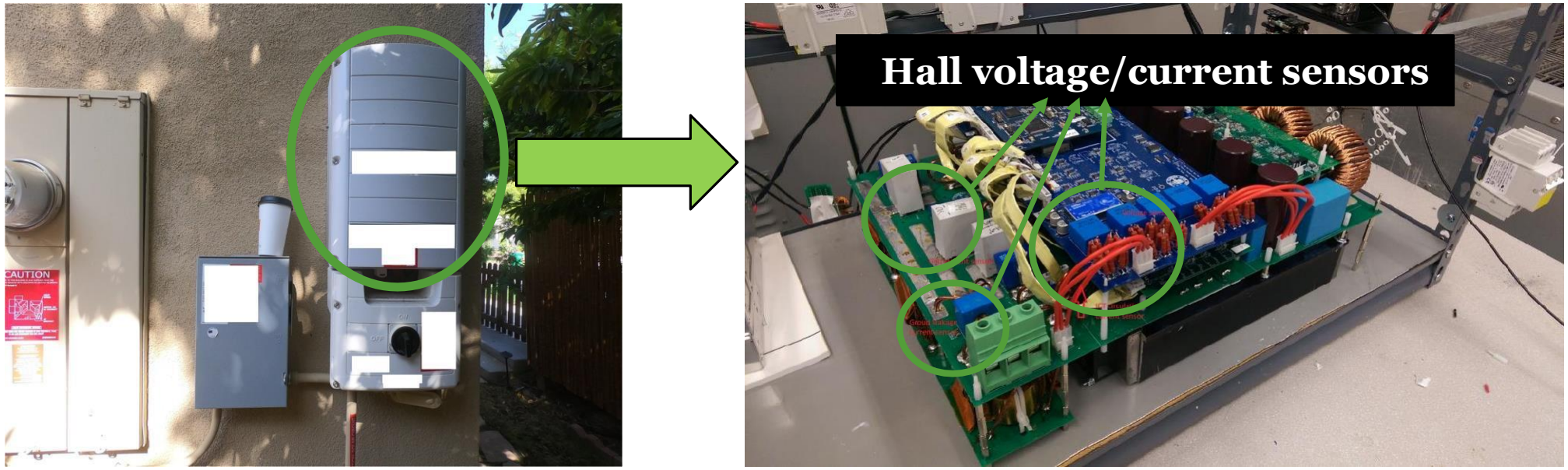




Solar Inverter（光伏逆变器）

- 光伏逆变器（PV inverter或solar inverter）可以将光伏（PV）太阳能板产生的可变直流电压转换为市电频率交流电（AC）的逆变器，可以反馈回商用输电系统，或是供离网的电网使用。

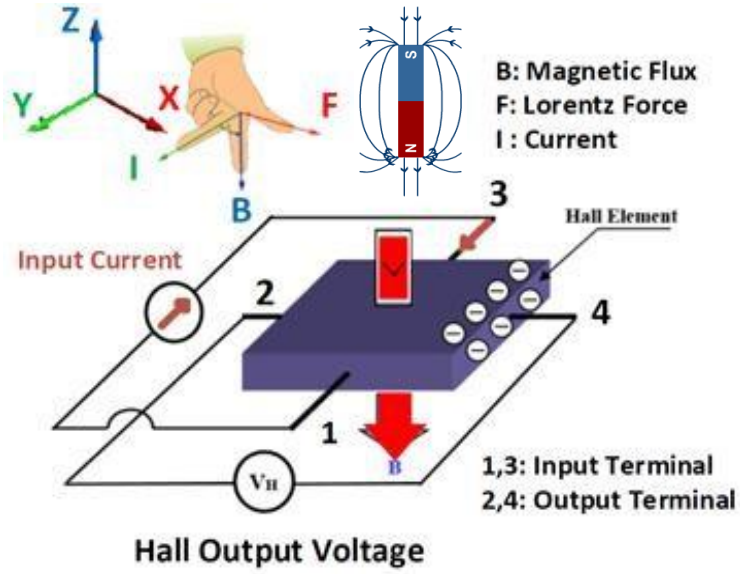
Hall Sensors Inside of Grid-Tied Inverters



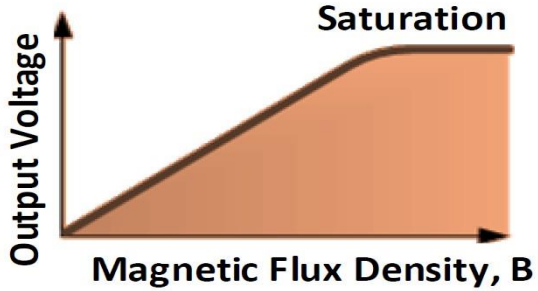
Contributions

- A new attack on the Hall sensor
- Algorithms and attack tool (i.e., Embedded Hall Spoofing Controller)
- Validation in a testbed with a scaled-down model of a power grid
- Evaluation in a medium-sized 2.3 MW grid
- Countermeasures

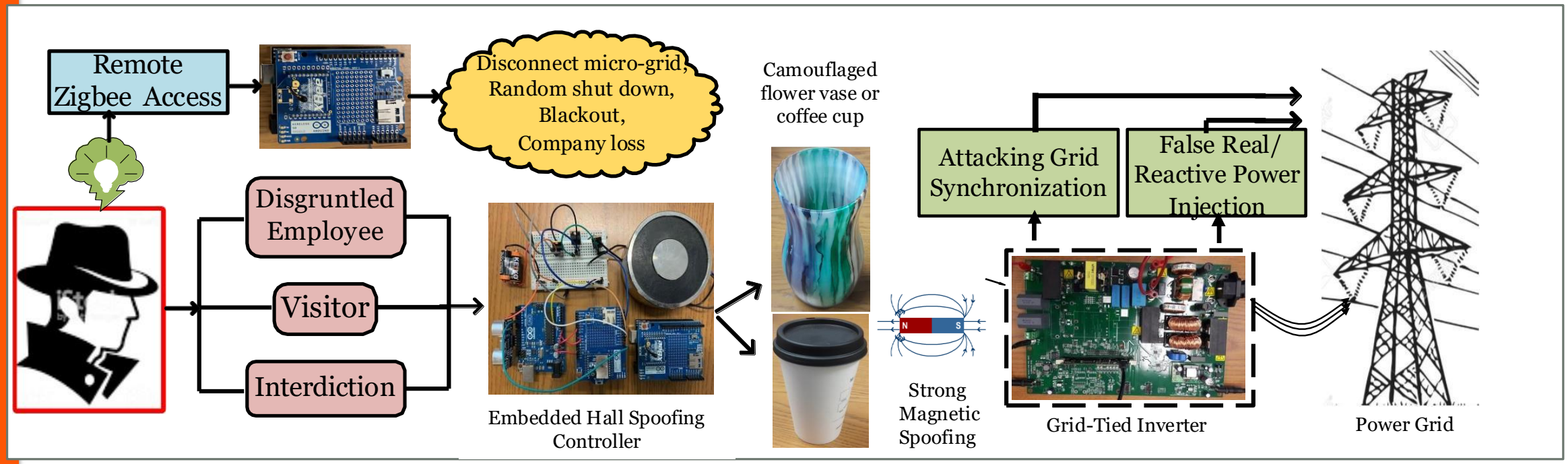
Hall Sensor Basics



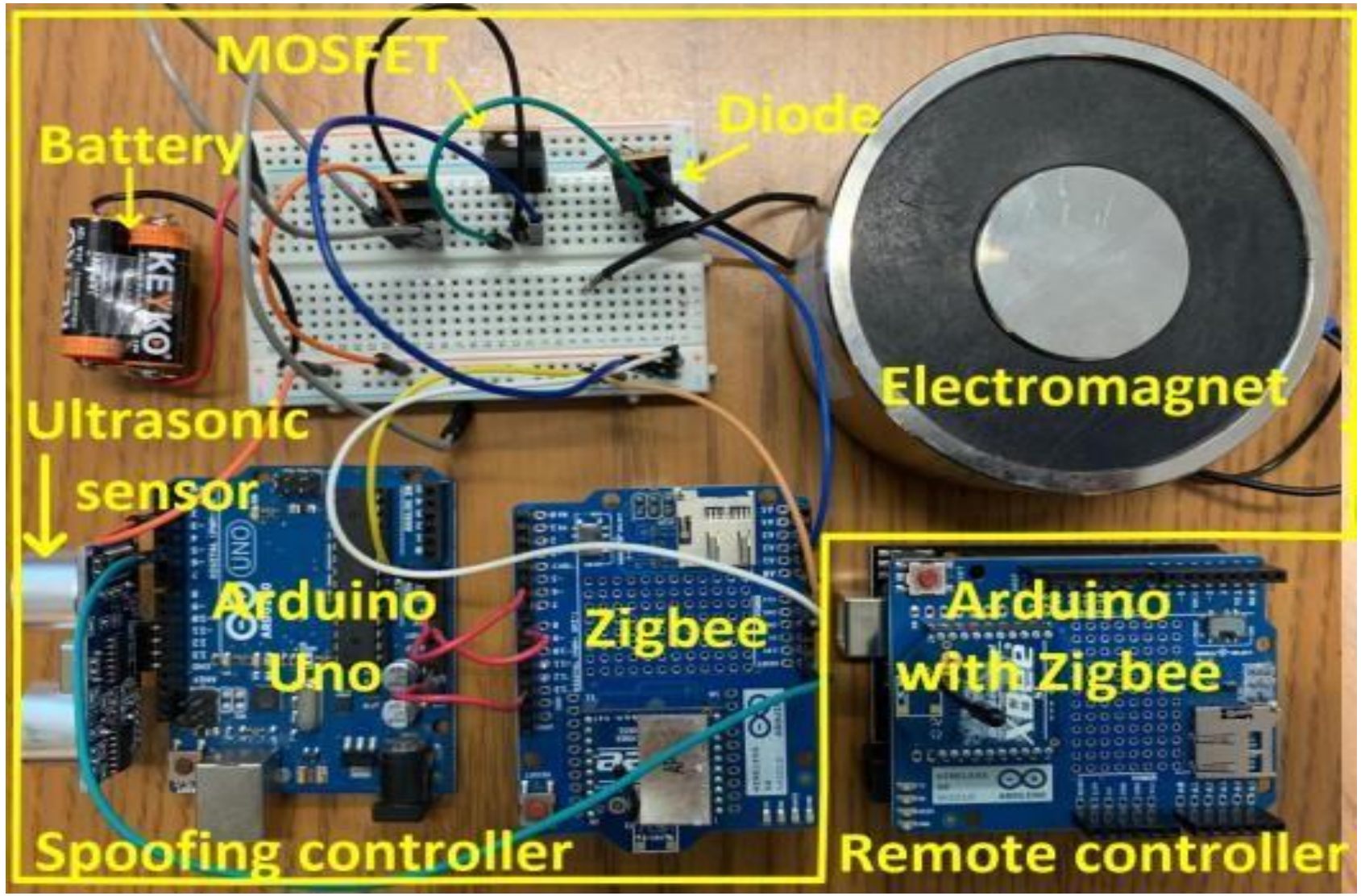
$$V_{hall} = k(\frac{I_{bias}}{d} \times B)$$



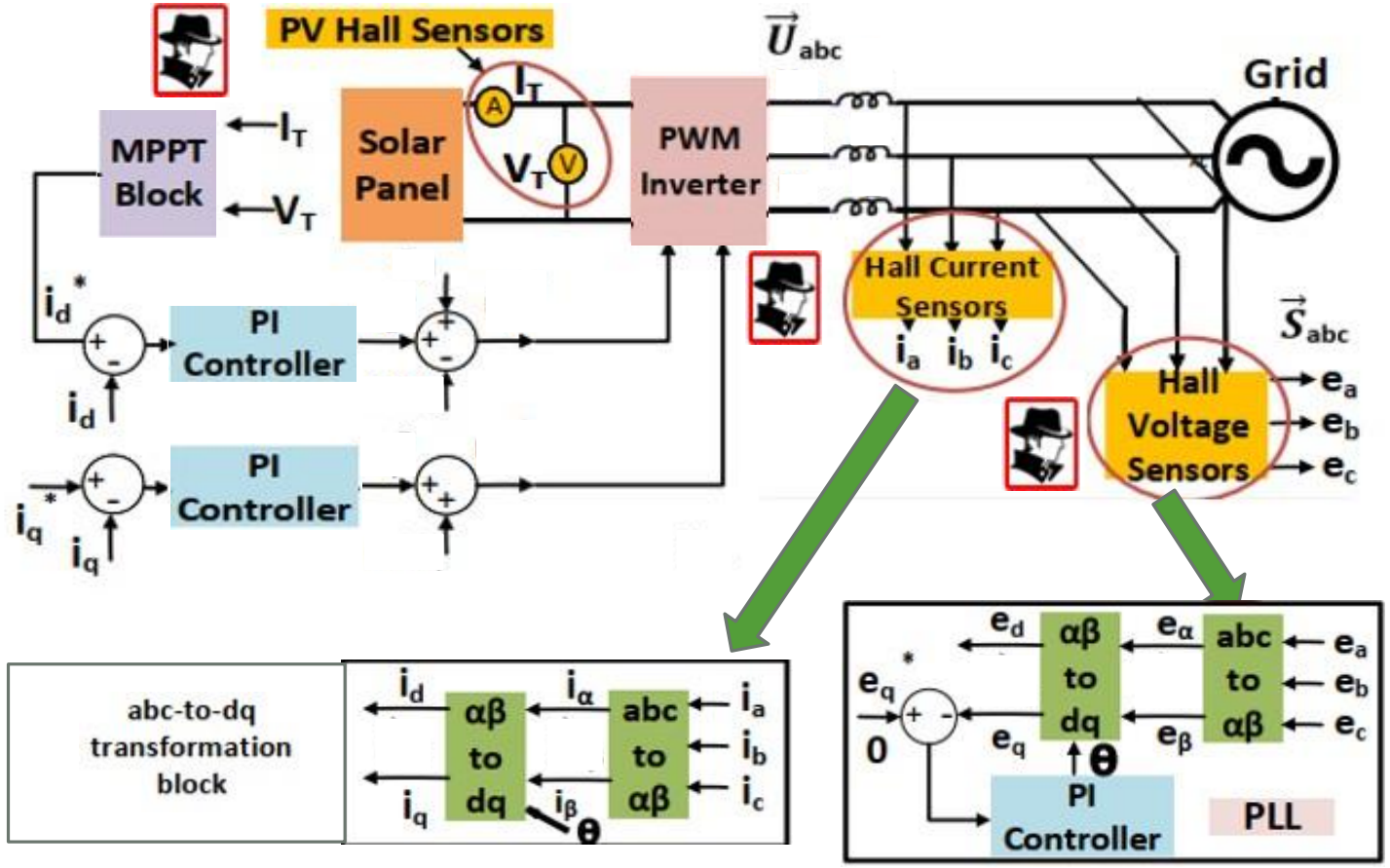
Attack Model



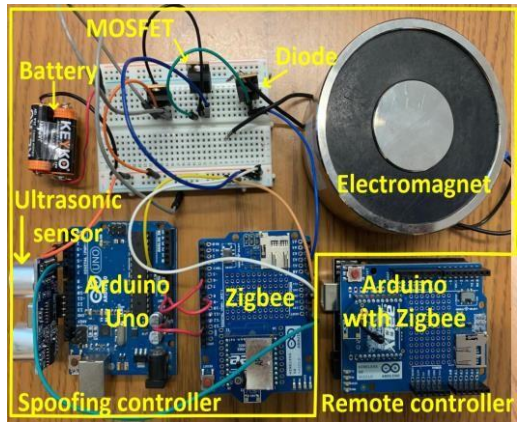
The Embedded Hall Spoofing Controller

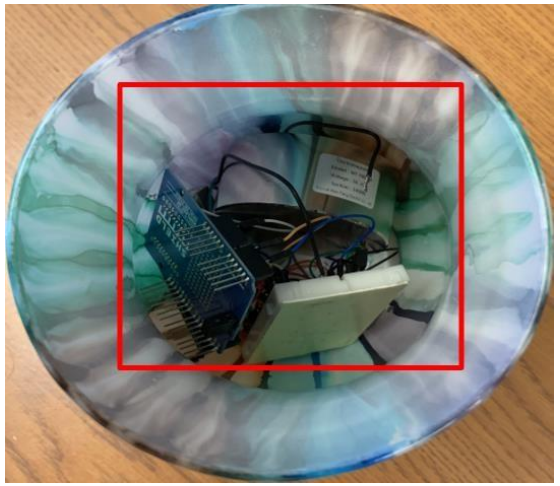


The Embedded Hall Spoofing Controller



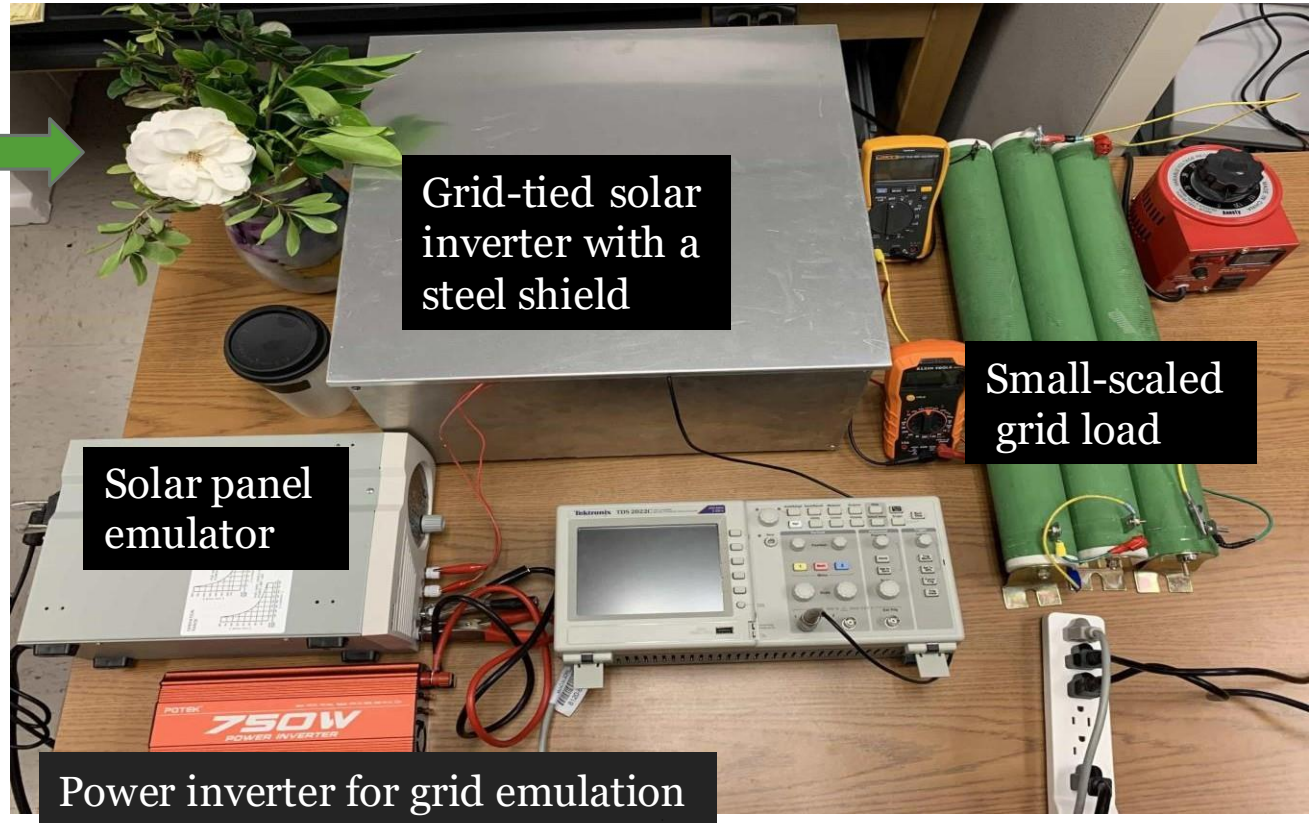
The Embedded Hall Spoofing Controller



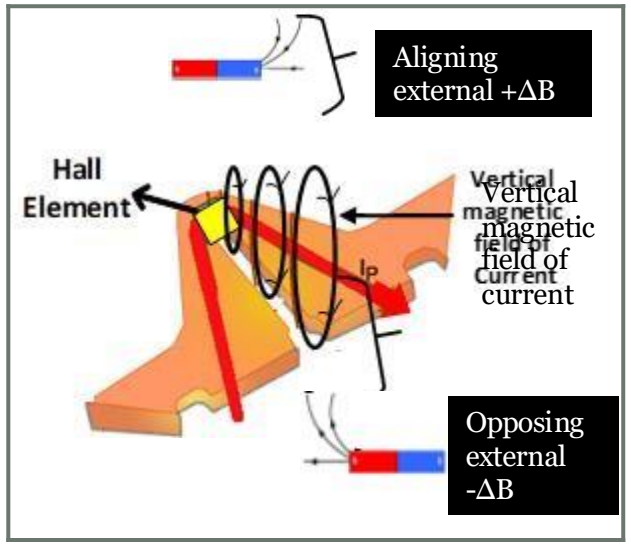


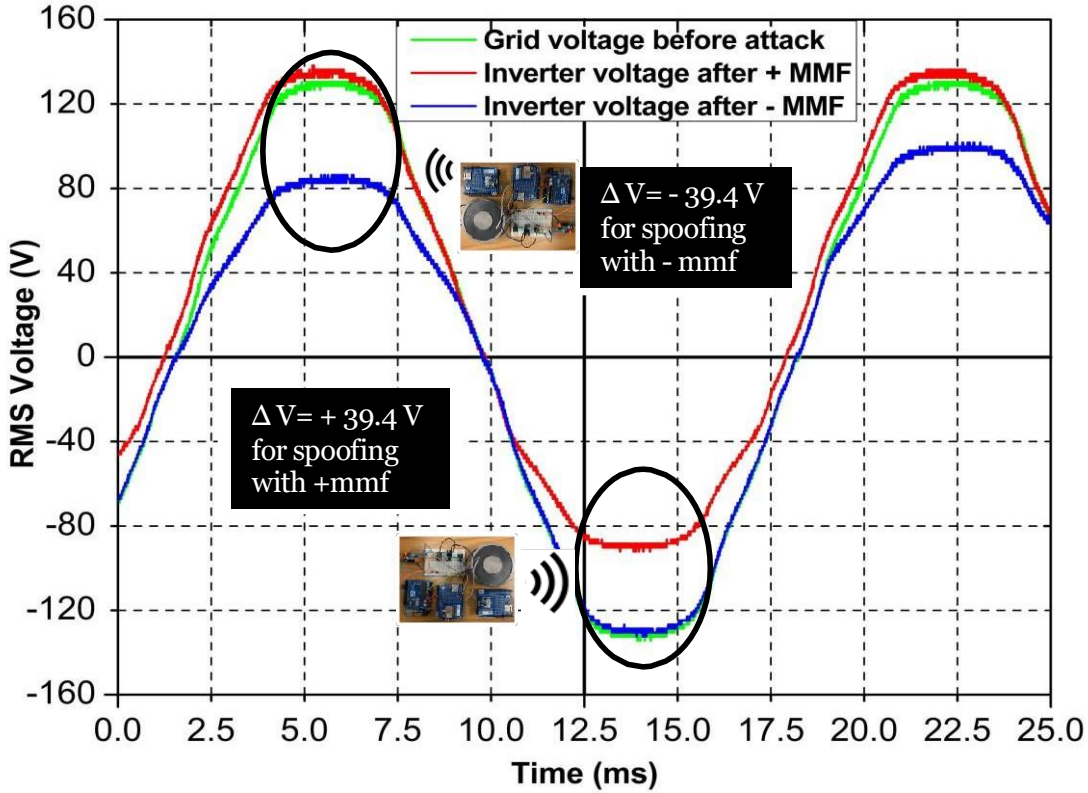
Experimental Setup

Camouflaged attack tool placed 8cm away from the inverter

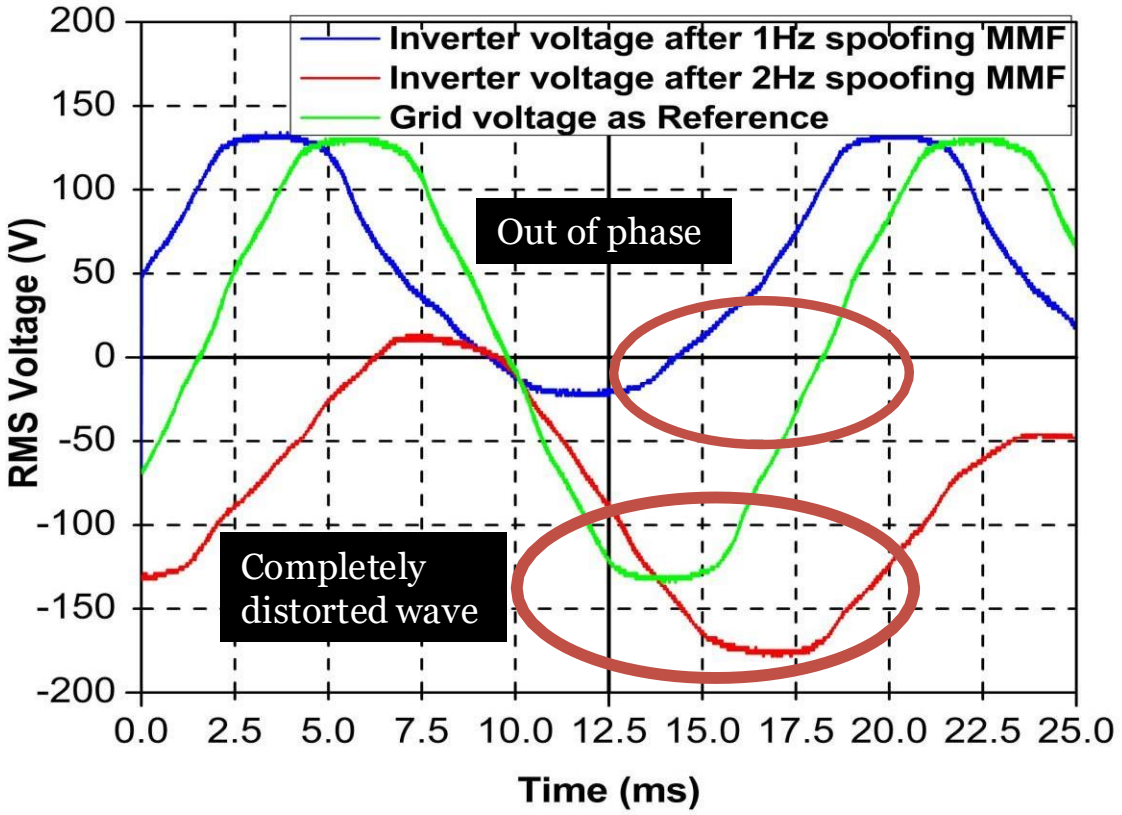


Spoofing the Grid-tied Inverter Voltage

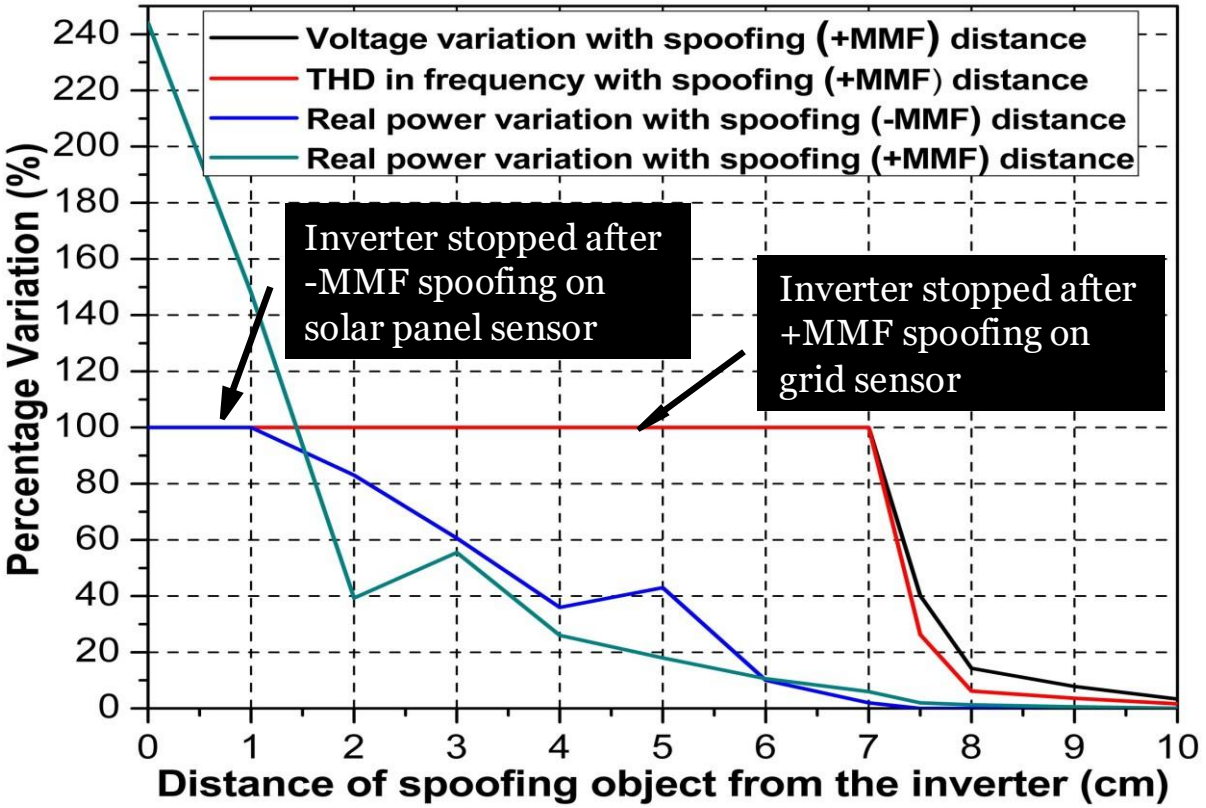




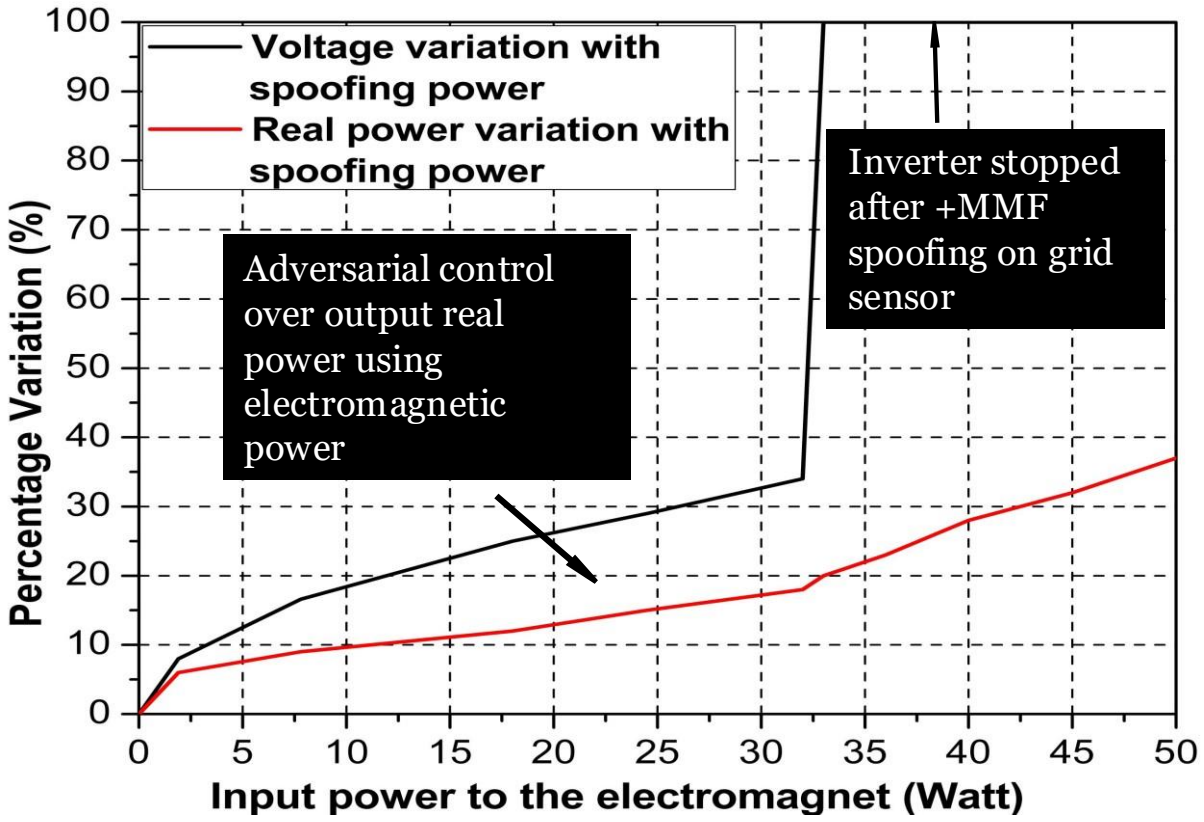
Spoofing the Grid-Tied Inverter Frequency



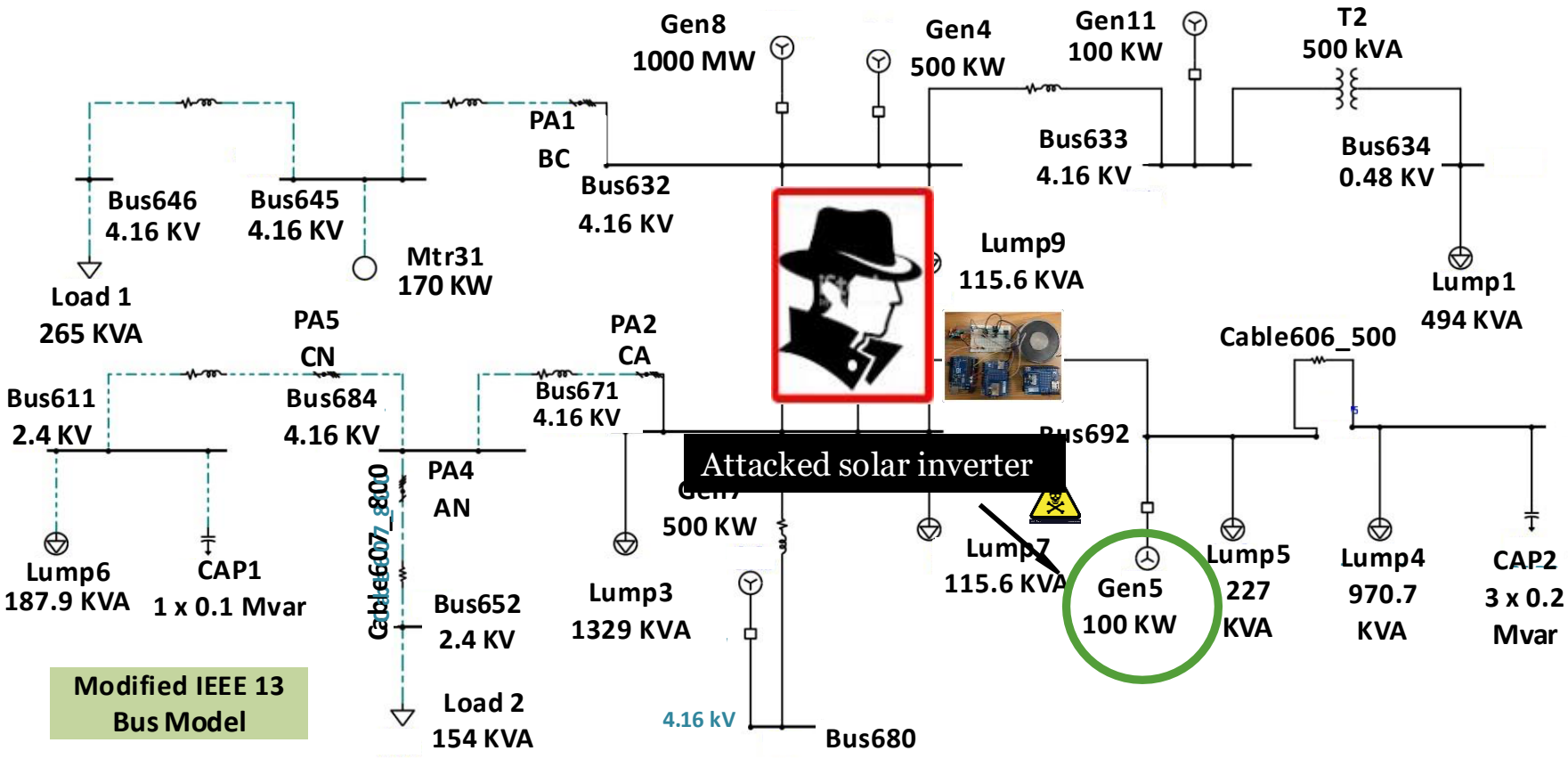
Attack-Impact with Spoofing-Distance



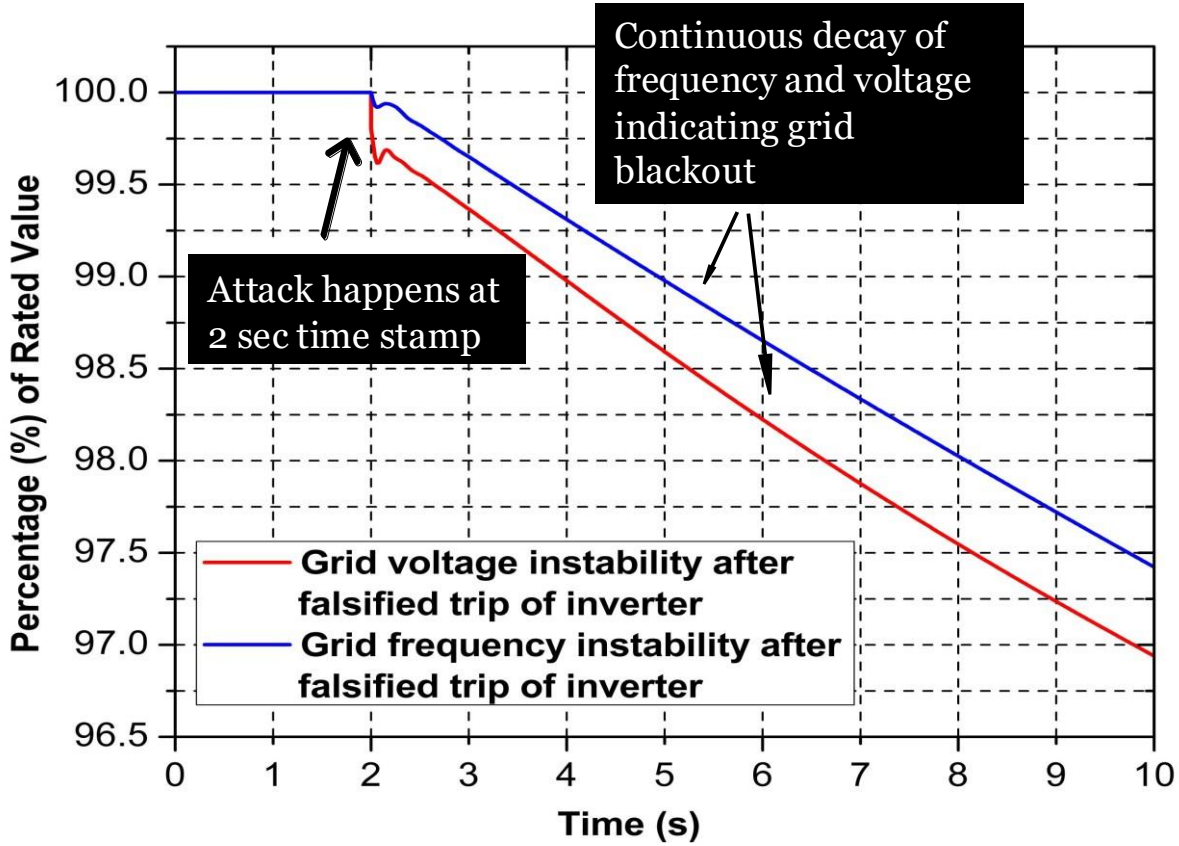
Attack-Impact with Spoofing-Power



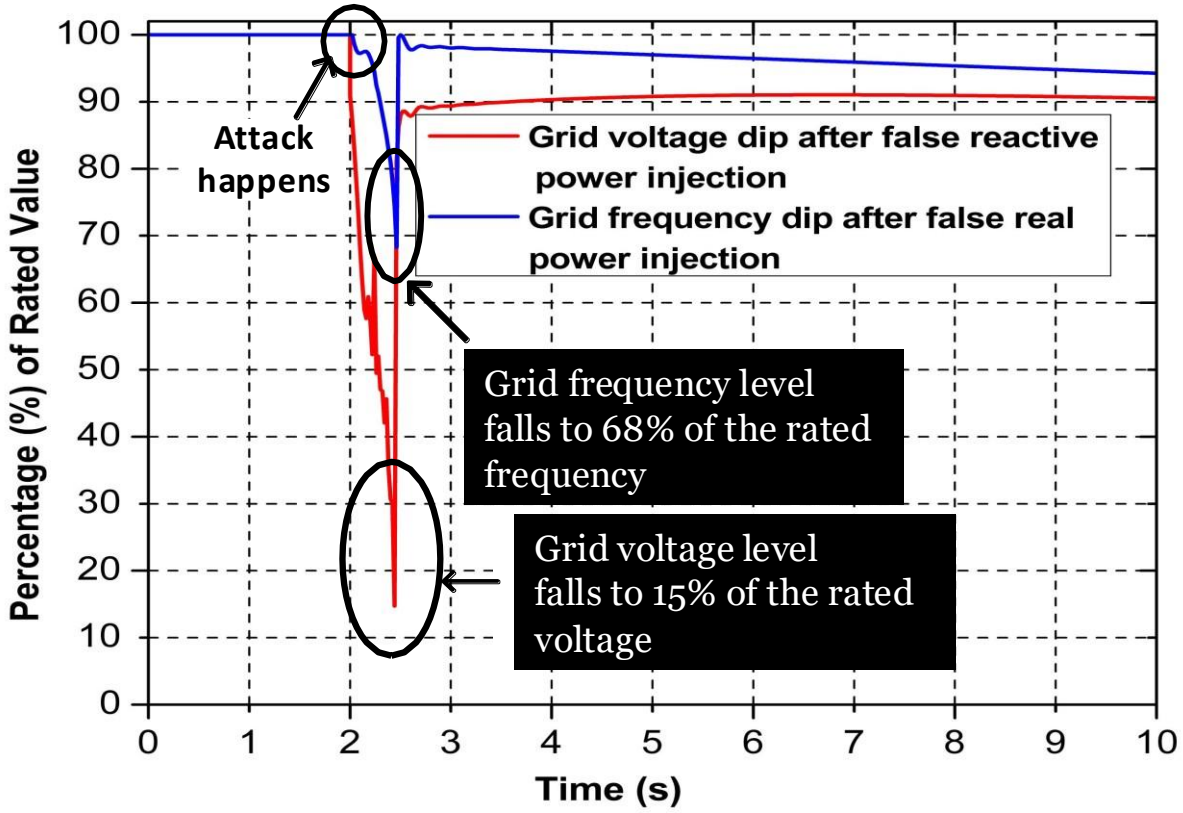
Attack Evaluation in a Practical Grid



Grid Synchronization Attack



False Real & Reactive Power Injection Attack



Countermeasures

- Sensing presence of external magnetic field
- Secured surrounding environment
- Shielding: CO-NETICAA, NETIC S3-6, and MuMETAL
- Robust sensors: differential Hall effect sensors

Summary

- A new attack on the Hall sensor
- Algorithms and attack tool (i.e., Embedded Hall Spoofing Controller)
- Validation and evaluation of the attack model

LOTS of Connected Devices

User-Device Interactions

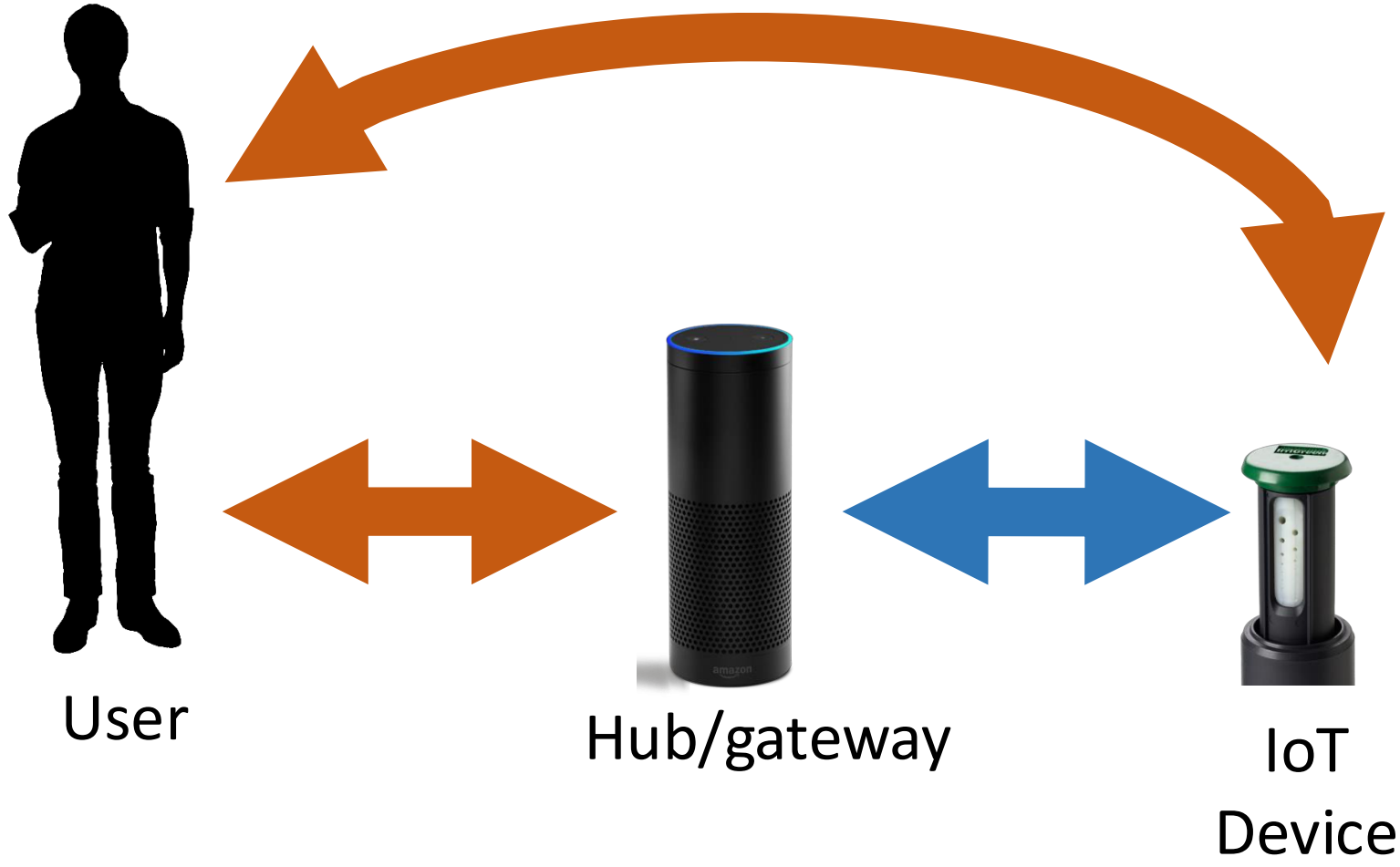
Hands-Free User-Device Interactions

Direct

- User → device
- Voice-based Interaction
- 30% of interactions through **"conversations"** with smart machines

Indirect

- User → hub → device
- Bluetooth Low Energy (BLE)
- 75K unique products with BLE support



With great power comes great responsibility

(or more security and privacy issues)

Security and Privacy of User-Device Interactions

Bluetooth Low Energy

Voice interactions

Hands-free interactions

BLE Security

- Black Hat 2016 and DEF CON 2016
  - “80 % of those BLE smart devices are vulnerable to MitM attacks.”



- Reverse Engineering of BLE communications


...

Voice-enabled Devices Listen to Everything

INTERNET OF THINGS

Listening To NPR Drives Th
Echo Insane

Google Home ad sets off devices during

TV anchor says live on-air 'Alexa, order me a
ulhouse' – guess what happens next

order begets story on accidental order begets

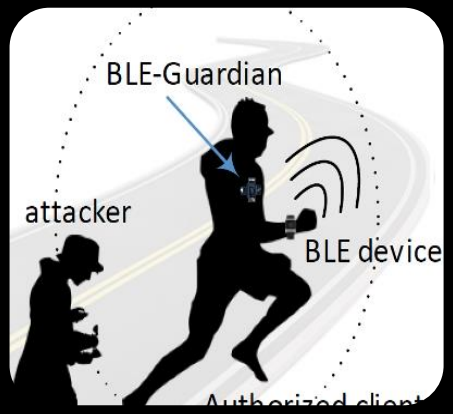
Technology

Amazon Echos activated by TV comment

9 January 2017 | Technology

Share

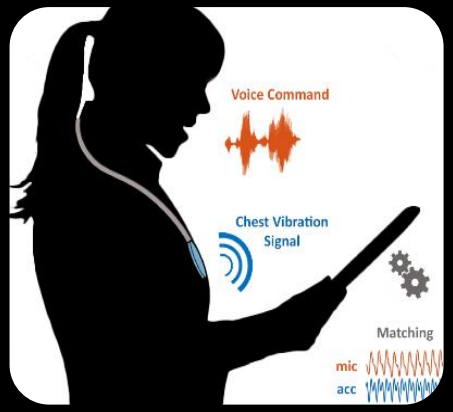
Security and Privacy of User-Device Interactions



BLE-Guardian

- Access control layer to BLE-equipped devices

[USENIX Sec '16]



VAuth

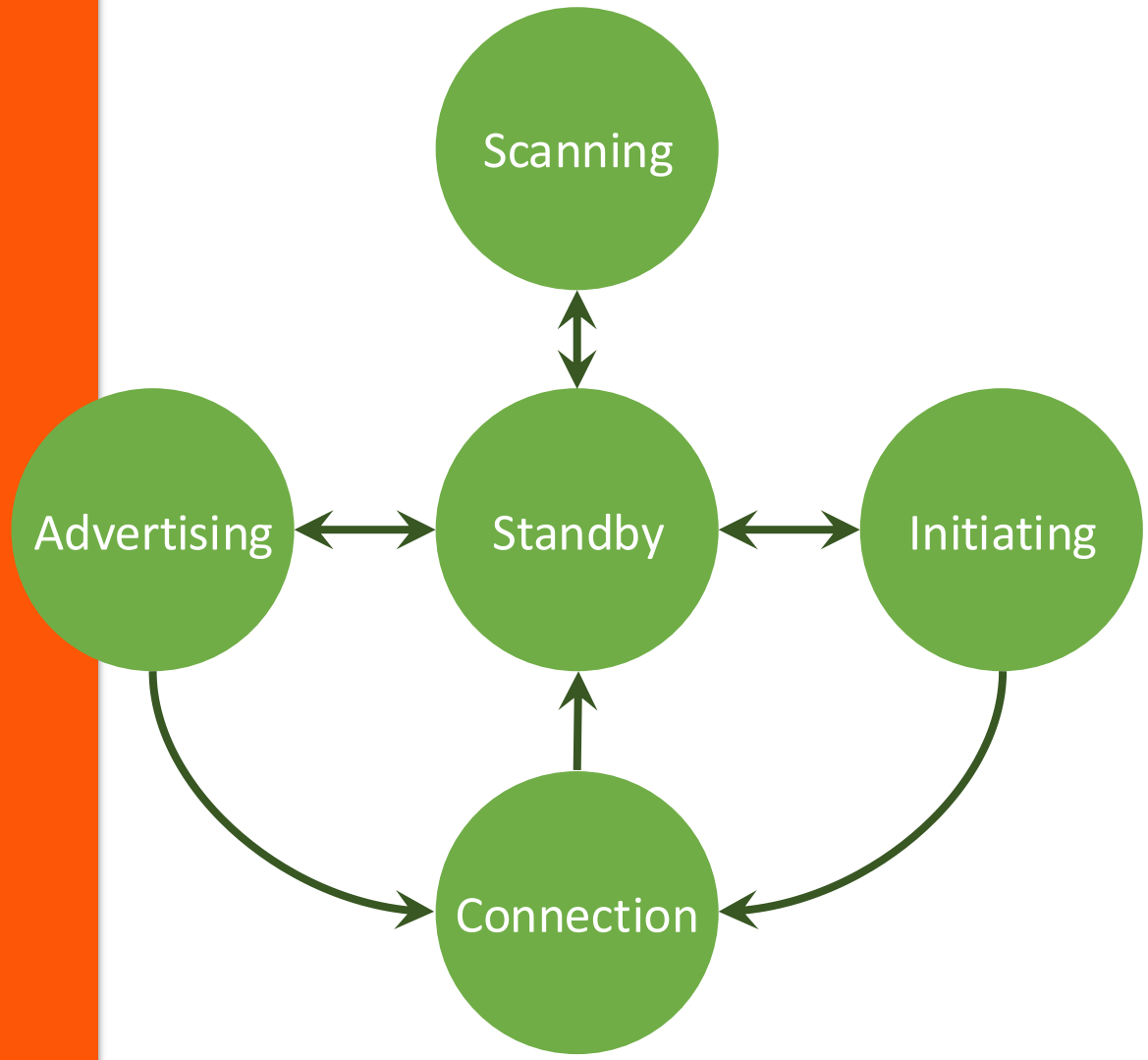
- Continuous authentication interface to voice-activated devices

[MobiCom 2017]

BLE-Guardian

[USENIX Sec ’16]

BLE Primer



- **Standby:** Low Power Mode. Receiver and transmitter switched ‘off’
- **Advertising:** Used by low power ‘IoT Device’. Only transmitter required.
- **Scanning:** Used by ‘gateway’. Receiver listens to advertising channels.
- **Initiating:** ‘Gateway’ sends connection request
- **Connection:** Communication over data channels.

BLE Privacy & Security Effectiveness

- Indirect Advertisements
  - Detected 214 different unique **types of** devices
- Address Randomization

Name	Description
ihere	key finder
DEXCOMRX	Glucose monitor
Frances's Band ea:9d	smartband
Otbeat	heart rate monitor
JS00002074	digital pen

Revealing Names

Device	Days observed
One	37
Flex	37
Zip	37
Forerunner 920	36
Basis Peak	25

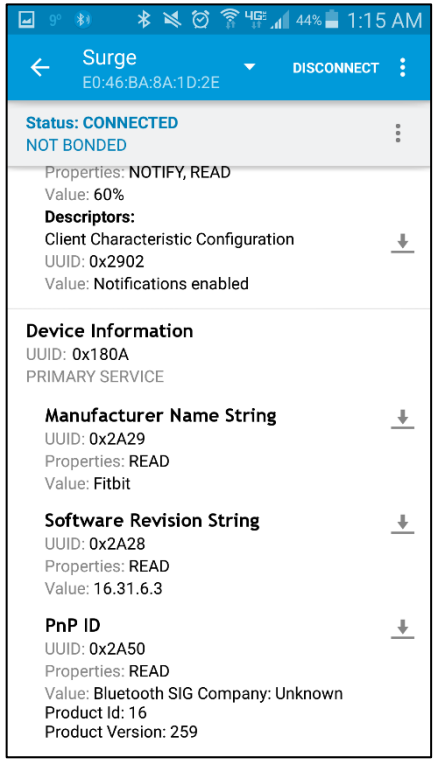
Consistent Addresses

Address
00:17:E9:CB:F3:61
00:17:E9:CB:F5:01

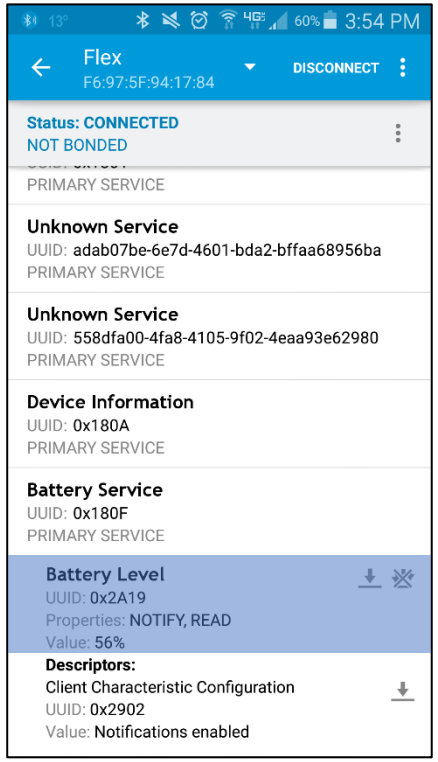
Poor Randomization

BLE Privacy & Security Effectiveness

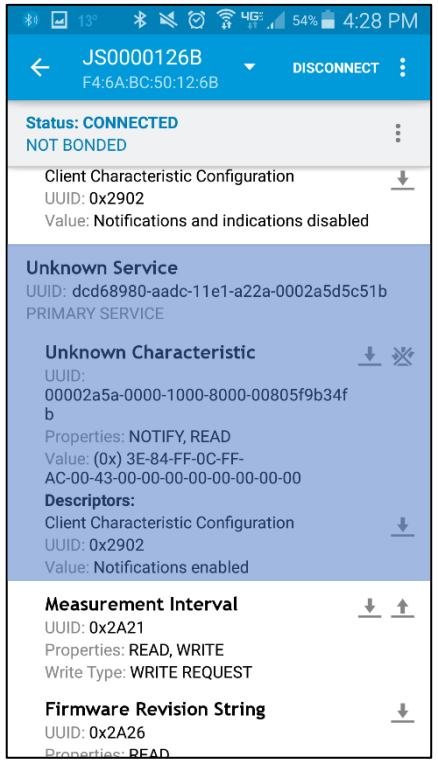
- Device Pairing



Advertise and accept connections

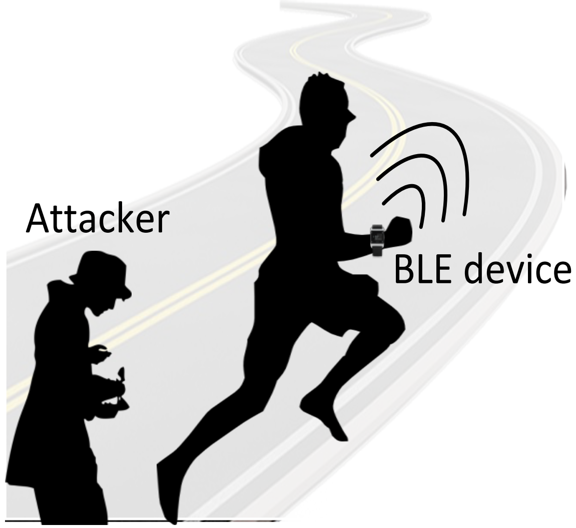


Battery level

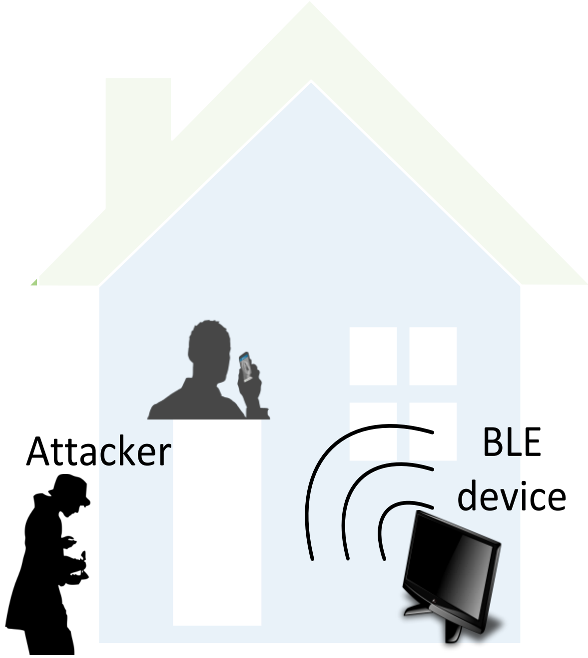


Unique identifiers

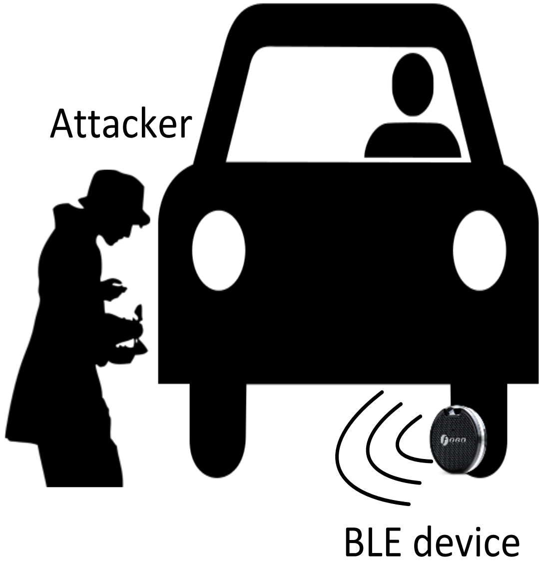
It All Starts with the Advertisements…



Tracking User



Profiling User



Harming User

[illegible]

Can we effectively fend off the threats to BLE-equipped devices

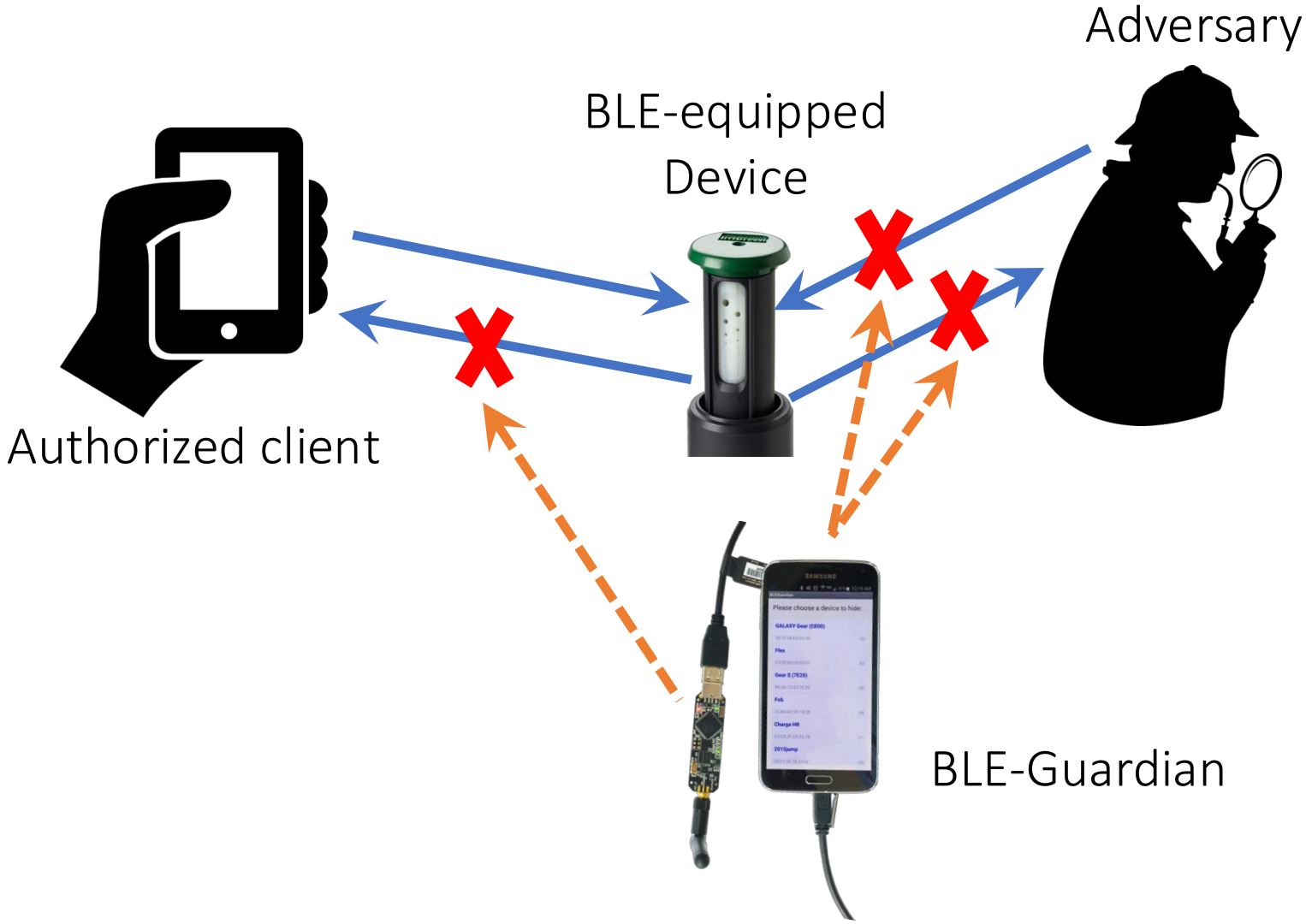
(1) in a **device-agnostic** manner, and

(2) using **COTS** (Commercial-Off-The-Shelf) hardware only?

BLE-Guardian

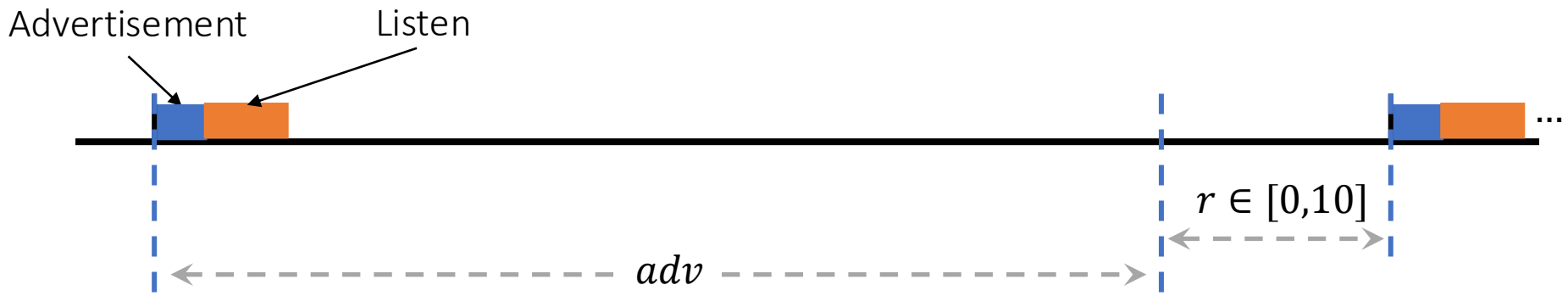
Device Hiding

Access Control

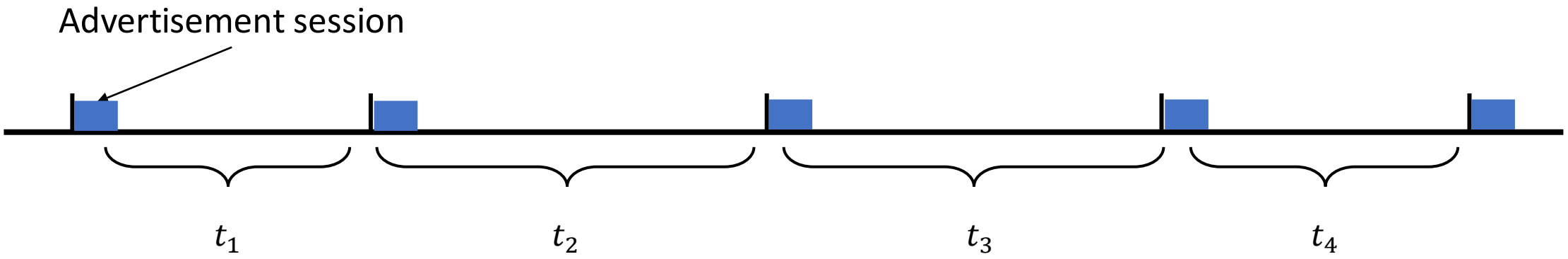


Device Hiding

- Jam BLE device advertisements to hide its existence
- Need to learn device advertising Interval
  - Otherwise jamming will be ineffective or inefficient



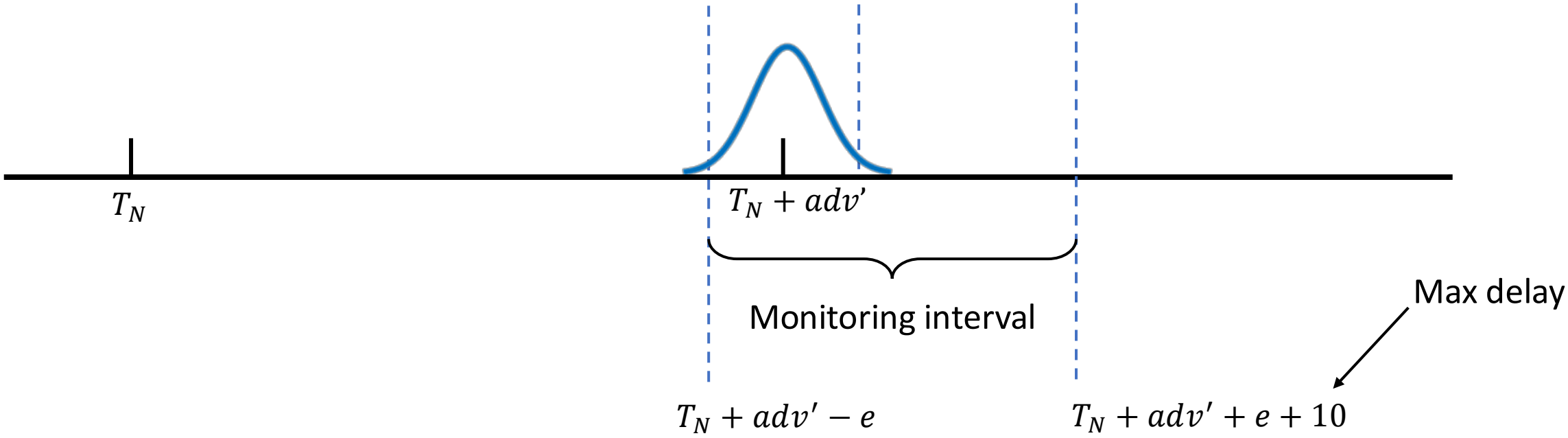
Device Hiding



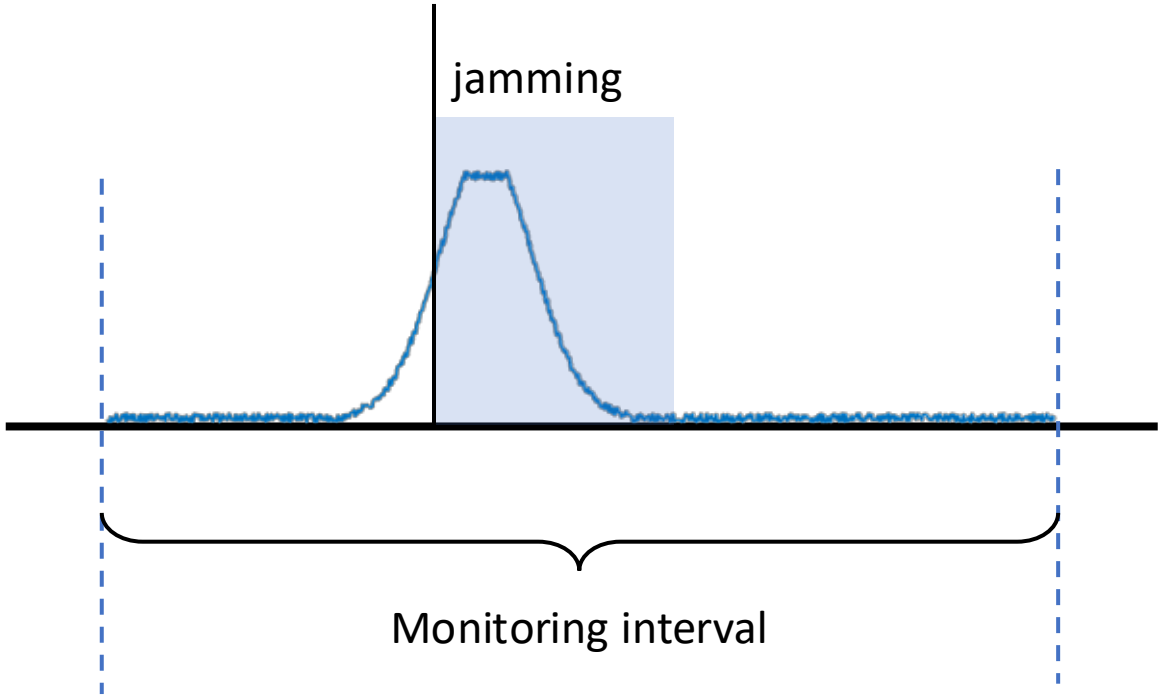
Estimate advertising interval:

$$adv' = E(t_i) - 5$$

Device Hiding



Device Hiding



- Detect RSSI (received signal strength indication) increase
- Apply jamming

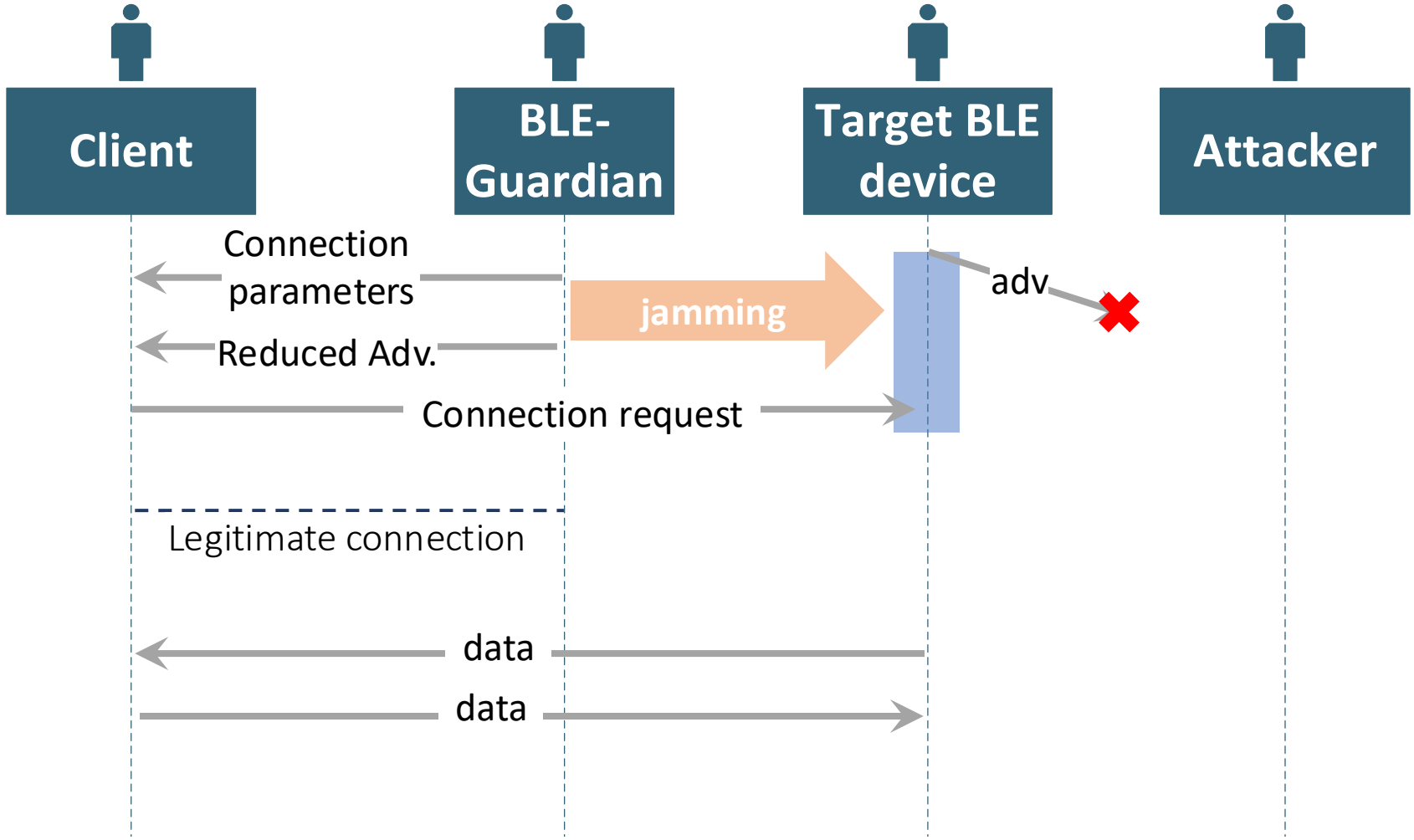
At this point, the target BLE device is **hidden**.

How to enable **access** to it?

Access Control

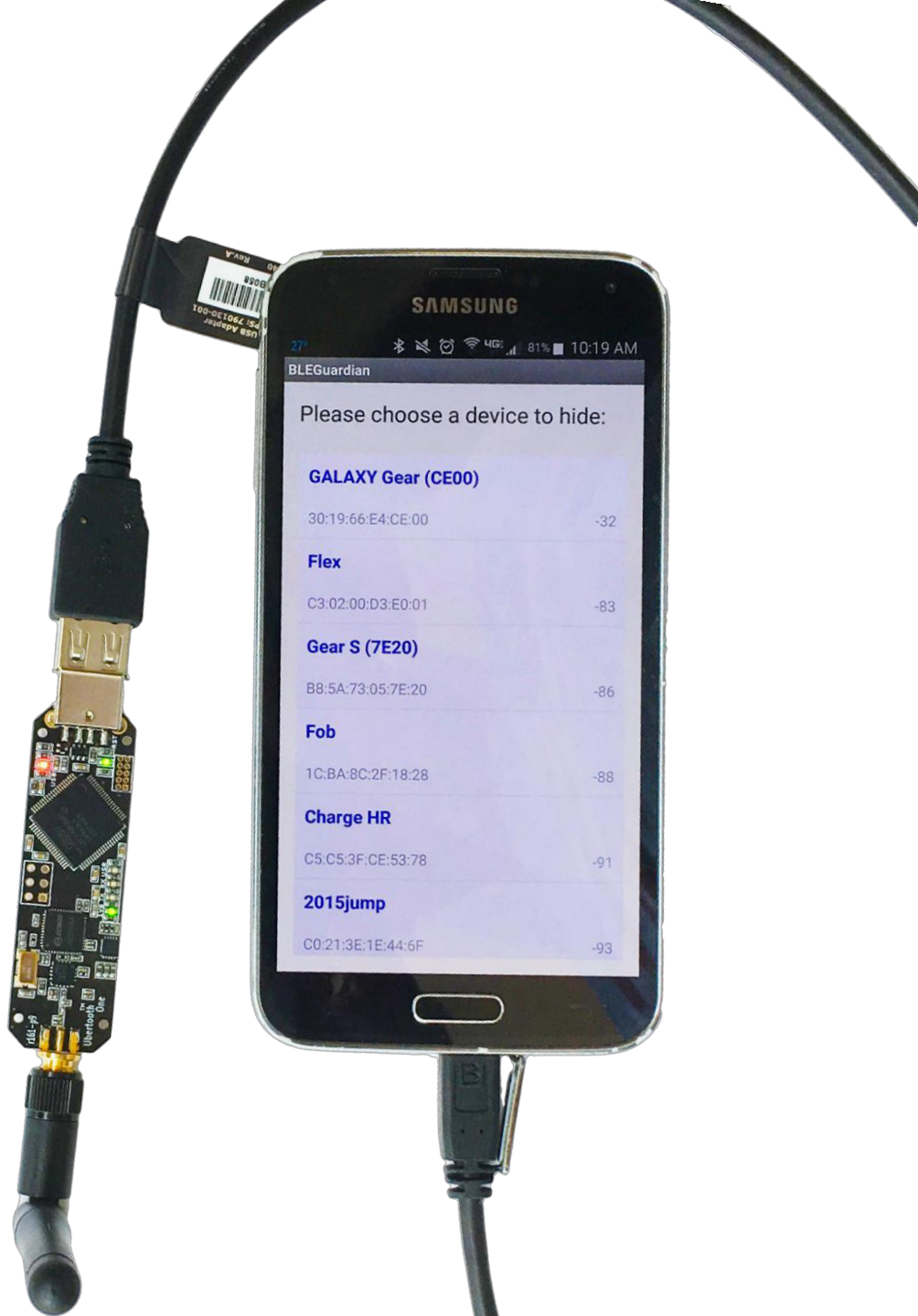
Bluetooth classic as an OOB channel（带外信道：是指在主信道外发生信息传递的单独通信信道）

Connection parameters to distinguish legitimate connection request.



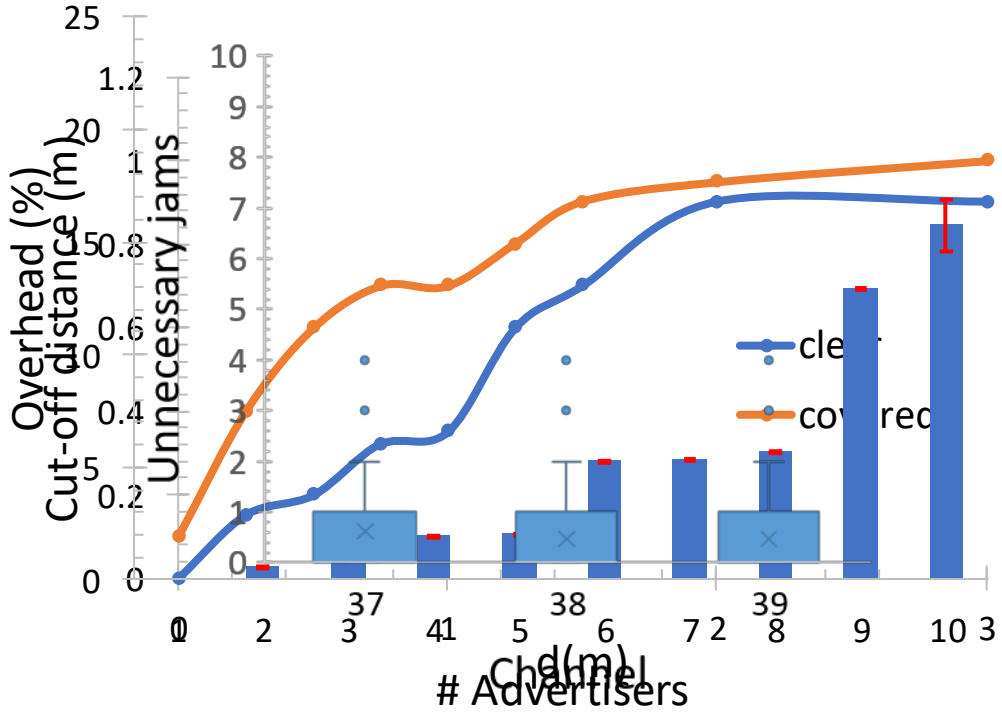
BLE-Guardian Prototype

- External hardware
  - Programmable BT radio
  - Open source firmware
  - Rx/Tx on each BT channel
- User-level app
  - Control BLE-Guardian
  - Update firmware seamlessly



Evaluation

- Cut-off distance
  - Less than 1m
- Impact on advertising channels
  - Less than 1 unnecessary jam in 20 *ms* in worst-case scenario
- Energy overhead
  - Less than 16%



Summary

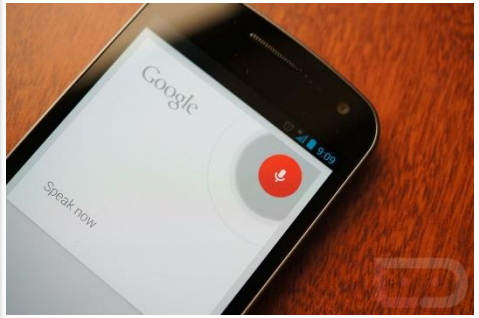
- BLE-equipped devices enable:
  - tracking, profiling and potential physical harm
- Challenge: Cannot modify BLE devices post-production
- Solution: BLE-Guardian
  - Privacy protection for BLE device users
  - Device agnostic and relies on COTS hardware
  - Low overhead on advertisement channels

VAuth

[MobiCom 2017]

Voice – An Emerging Interaction

- While driving, cooking, exercising …
- Voice assistants and voice-activated devices



Voice Is an Open Channel

with repercussions …

Malicious apps issuing voice commands

[Ben Itzhak '14]

Command injection through wireless signals

[Kasmi *et al.* ’15]

Mangled voice attack

[Vaidya *et al.* ‘15, Carlini *et al.* ’16]

Why **Not** Voice Biometrics?

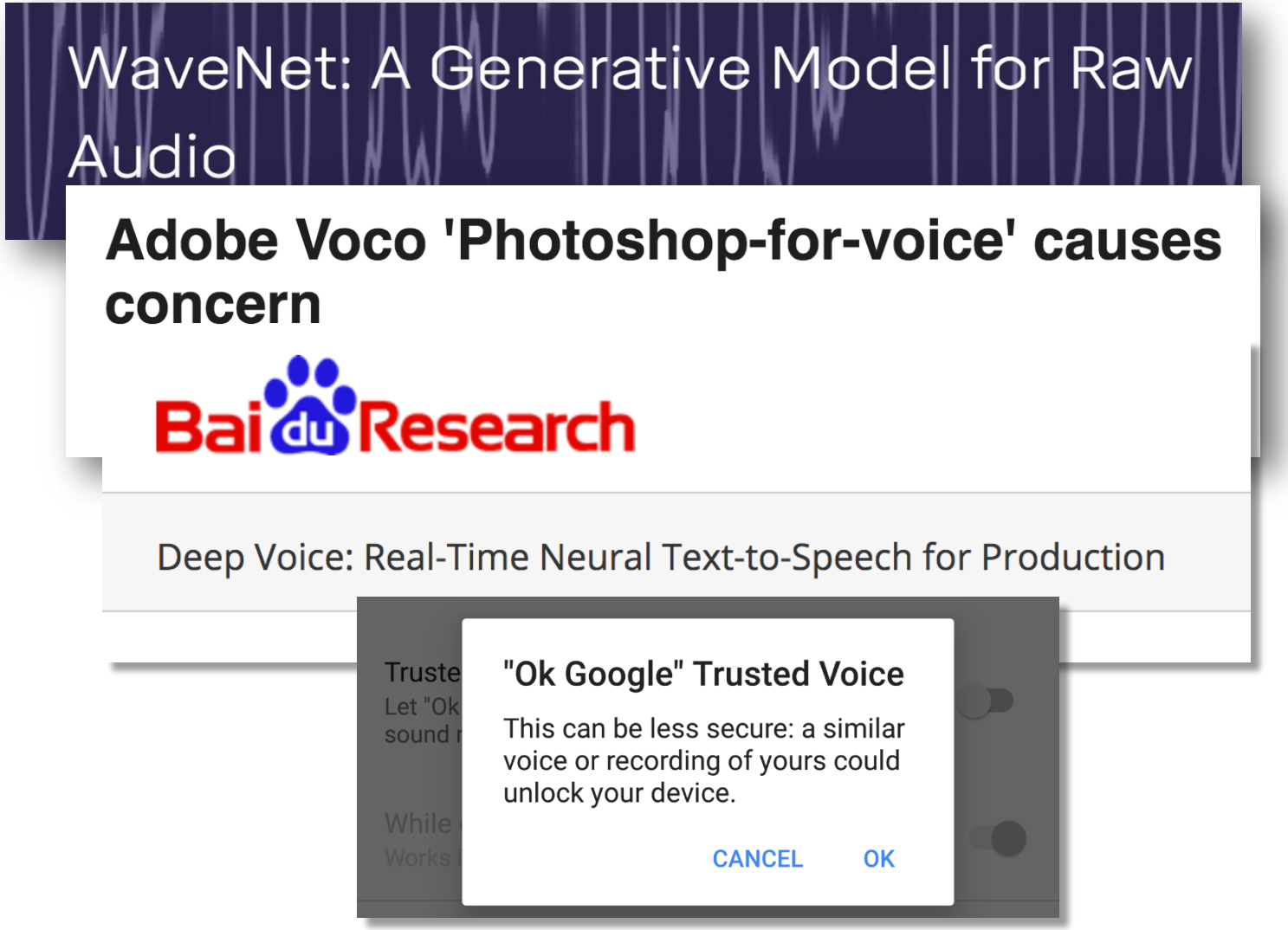
citibank

BARCLAYS

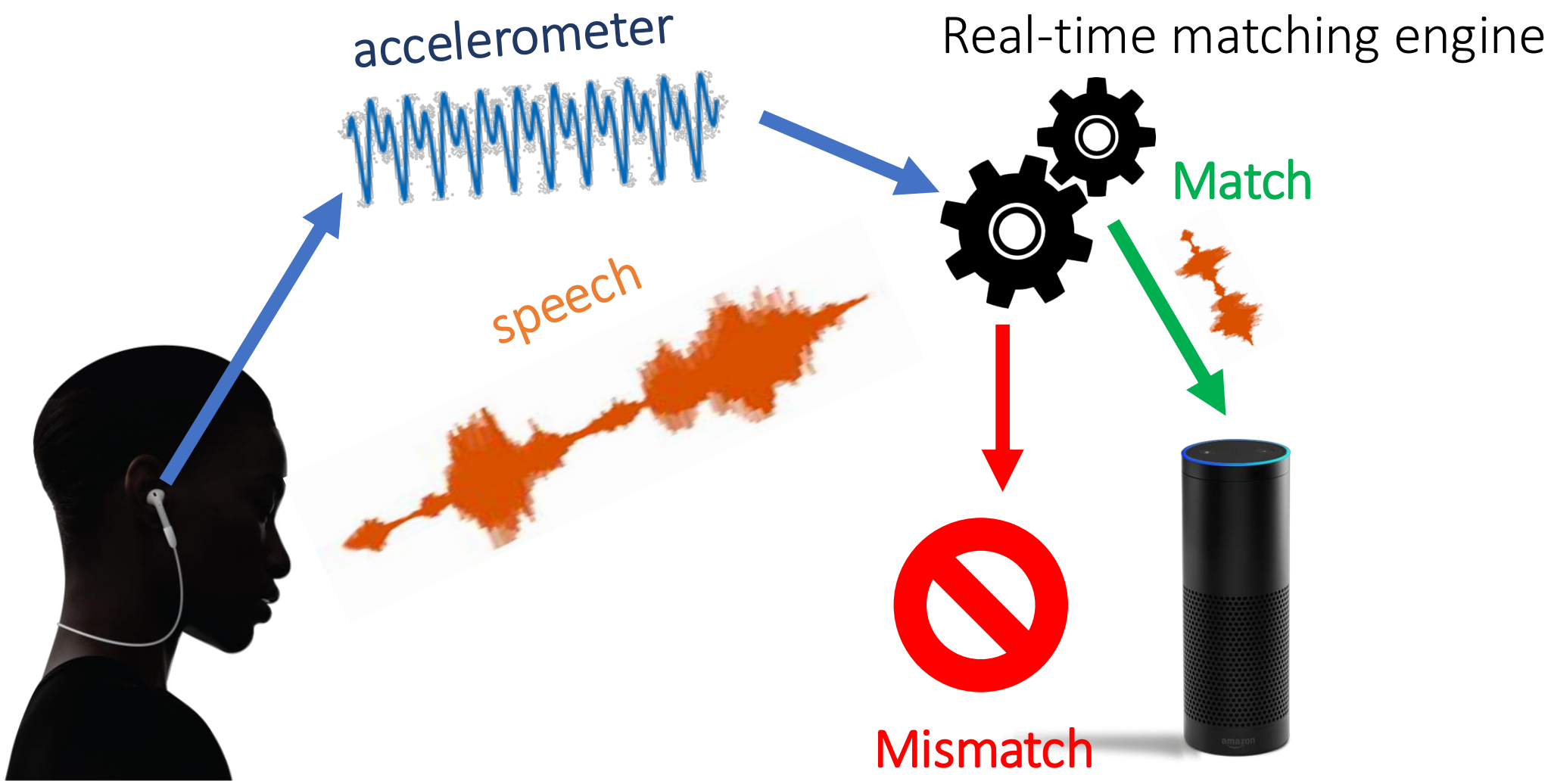
招商銀行
CHINA MERCHANTS BANK

HSBC

NUANCE

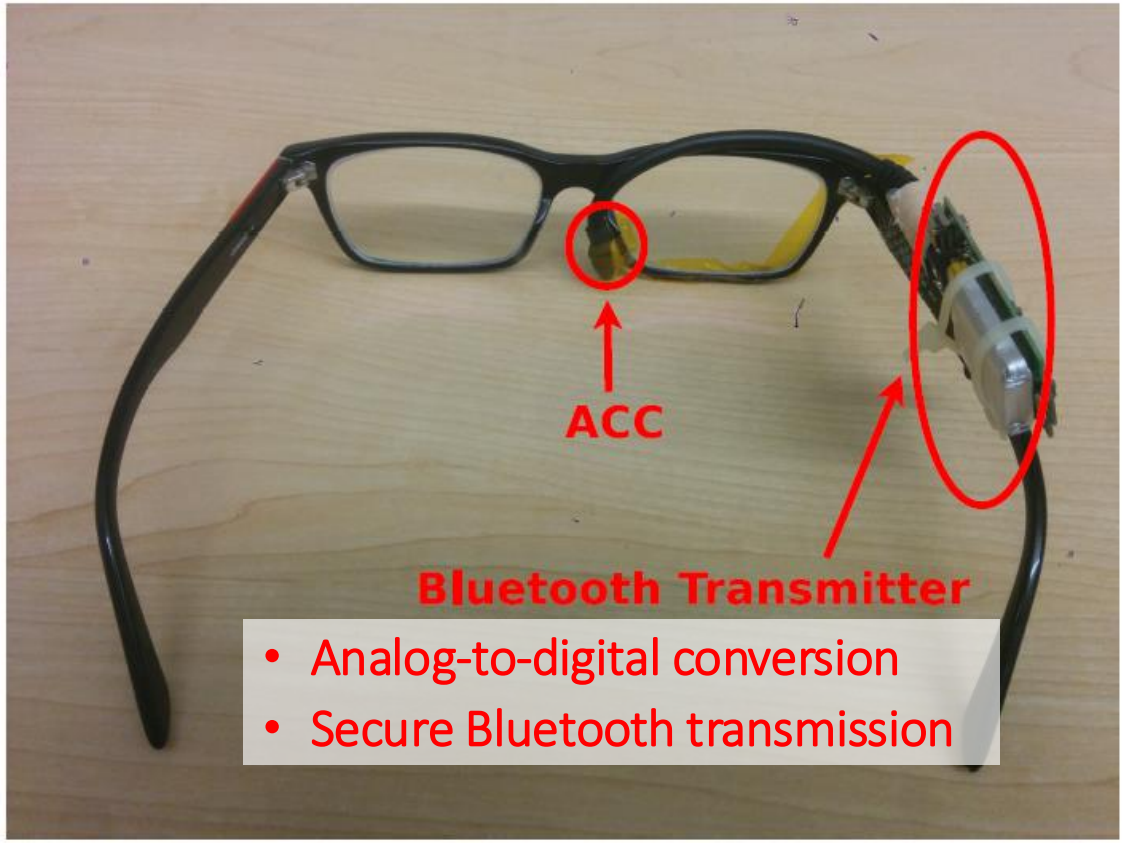


VAuth – **Continuous** Voice Authentication



VAuth Prototype

(a) Wireless



(b) Eyeglasses

Evaluation Results

- Recruited 18 users issuing 30 commands
  - Three positions: (eyeglasses, earbuds, necklace)
  - Two mobility scenarios: (still and jogging)
  - Five languages: (English, Korean, Arabic, Persian, Chinese)

- Takeaways:
  - Security: almost 0% false positive rate
  - Accuracy: 97% matching rate
  - Overhead: 0.35*s* matching delay, 1 week on 500 mAh battery

Summary

- Voice is an open channel
  - Unauthorized access to voice-activated devices
- Challenge: Need continuous authentication mechanism for voice that does not rely on signature
- Solution: VAuth
  - Couple the voice channel with physical assurances from on-body vibrations
  - Secure, real-time and continuous voice authentication

Conclusion of this Lecture

- Security for different sensing modalities
  - Attack on microphone (LightCommand)
  - Attack on IMU (Wallnut)
  - Eavesdropping on IMU (VeFi)
  - Attack on Hall-effect Sensors (Hall spoofing)
- For IoT Systems
  - Secure Connections between IoT devices (BLE Guardian and VAuth)
  - Secure I/O devices (GhostType)
- **Impact: Attack model/targeted scenario**
- **Novelty: technical elements**
- **Thoughtfulness: Evaluation**