GhostType: The Limits of Using Contactless Electromagnetic Interference to Inject Phantom Keys into Analog Circuits of Keyboards

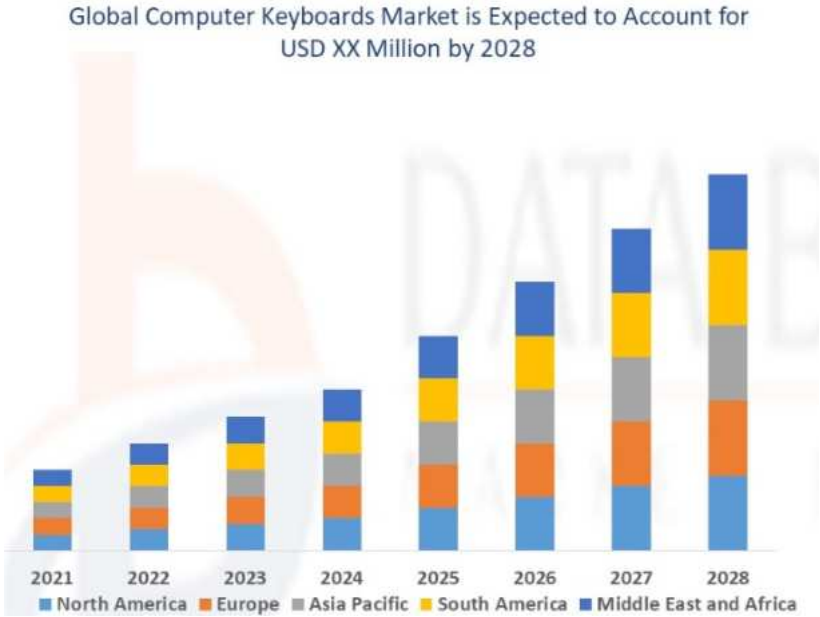
Qinhong Jiang[1], Yanze Ren[1], Yan Long[2], Chen Yan[1], Yumai Sun[2], Xiaoyu Ji[1], Kevin Fu[3], Wenyuan Xu[1]

[1]Ubiquitous System Security Lab (USSLAB), Zhejiang University
[2]Security And Privacy Research Group (SPQR), University of Michigan
[3]Northeastern University

NDSS SYMPOSIUM/2024

Keyboards Are Ubiquitous

Keyboard brand



The growth of keyboard market[1]

Keyboards: Indispensable Input Component

Keyboards: Indispensable Input Component

Keyboards: Indispensable Input Component

Keyboards: Indispensable Input Component

Trustworthy keystroke sensing lays the foundation to secure computer operations

Keyboards Workflow

User

- ✓ **Hand motion**
- ✓ **Key travel**

Keyboards Workflow

User

Typing

Keyboard

- ✓ **Hand motion**
- ✓ **Key travel**

- ✓ **Matrix scanning**
- ✓ **Firmware**

Keyboards Workflow

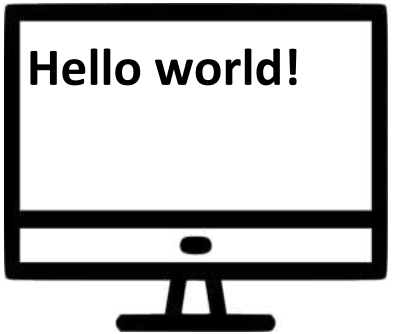
User

Typing

Keyboard

USB
Bluetooth

Computer



- ✓ **Hand motion**
- ✓ **Key travel**

- ✓ **Matrix scanning**
- ✓ **Firmware**

- ✓ **Polling**
- ✓ **Command executing**

Existing Work: Bad USB Attacks

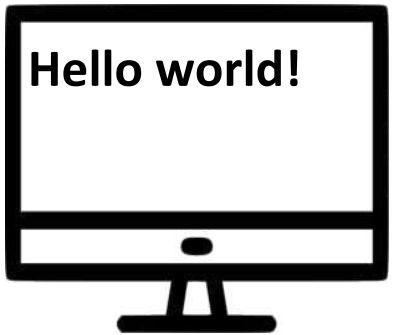
User

Keyboard

Computer

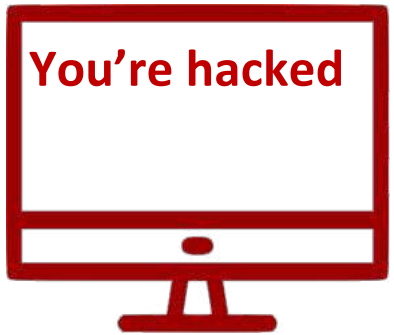
Typing

USB
Bluetooth



Adversary

USB
Bluetooth



Existing Work: Bad USB Attacks

User

Typing

Keyboard

Authentication

USB
Bluetooth

Hello world!

Adversary

USB
Bluetooth

You're hacked

Is the keyboard trustworthy even with authentication?

Our Goals

- *To uncover and understand the new threat vector against keyboard analog security with EMI.*

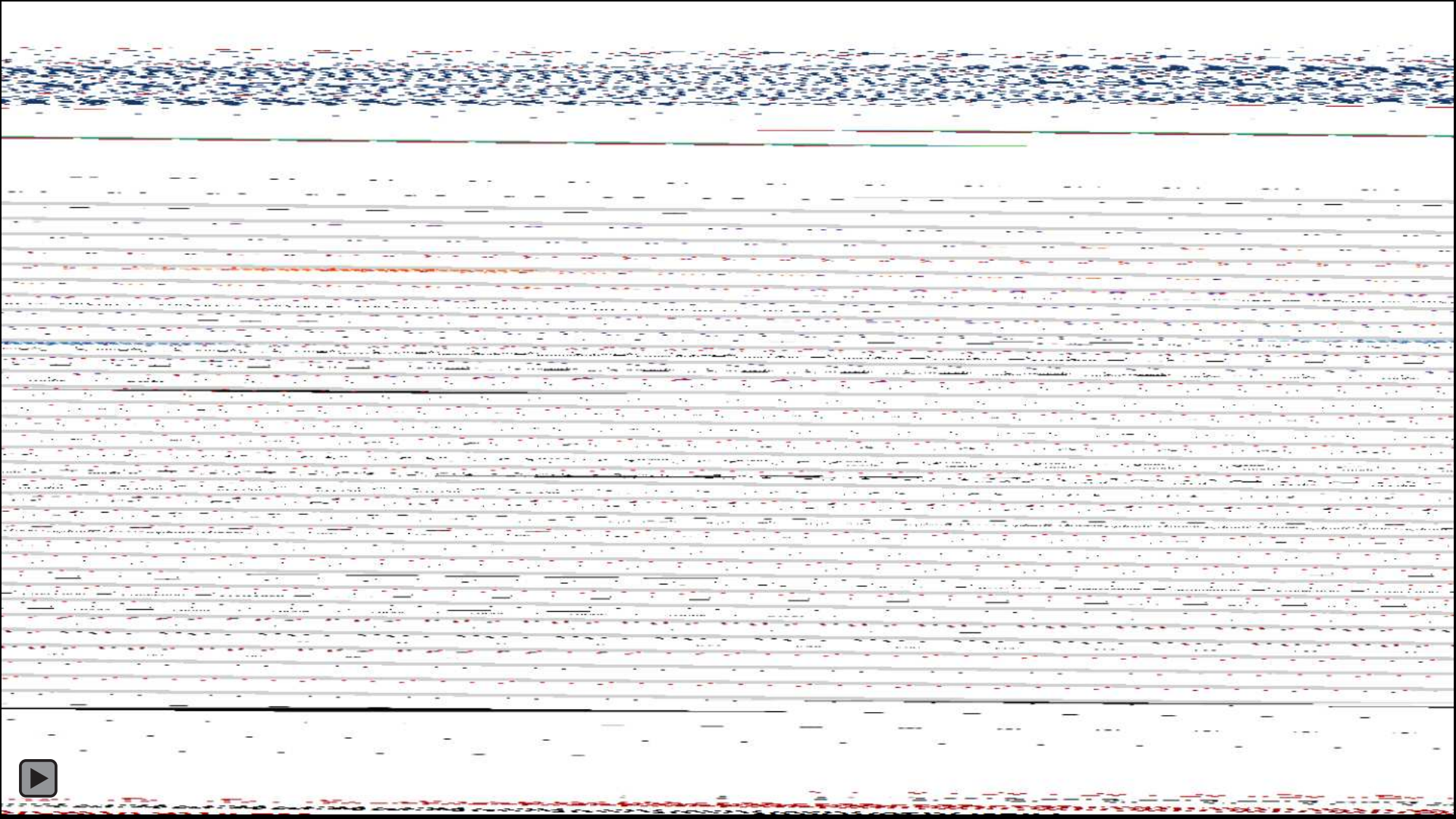
- *To mitigate the new threat and improve the security of keyboard sensing.*

Manipulate Keyboard Operation with EMI

Manipulate Keyboard Operation with EMI

Outcomes

DoS Attack

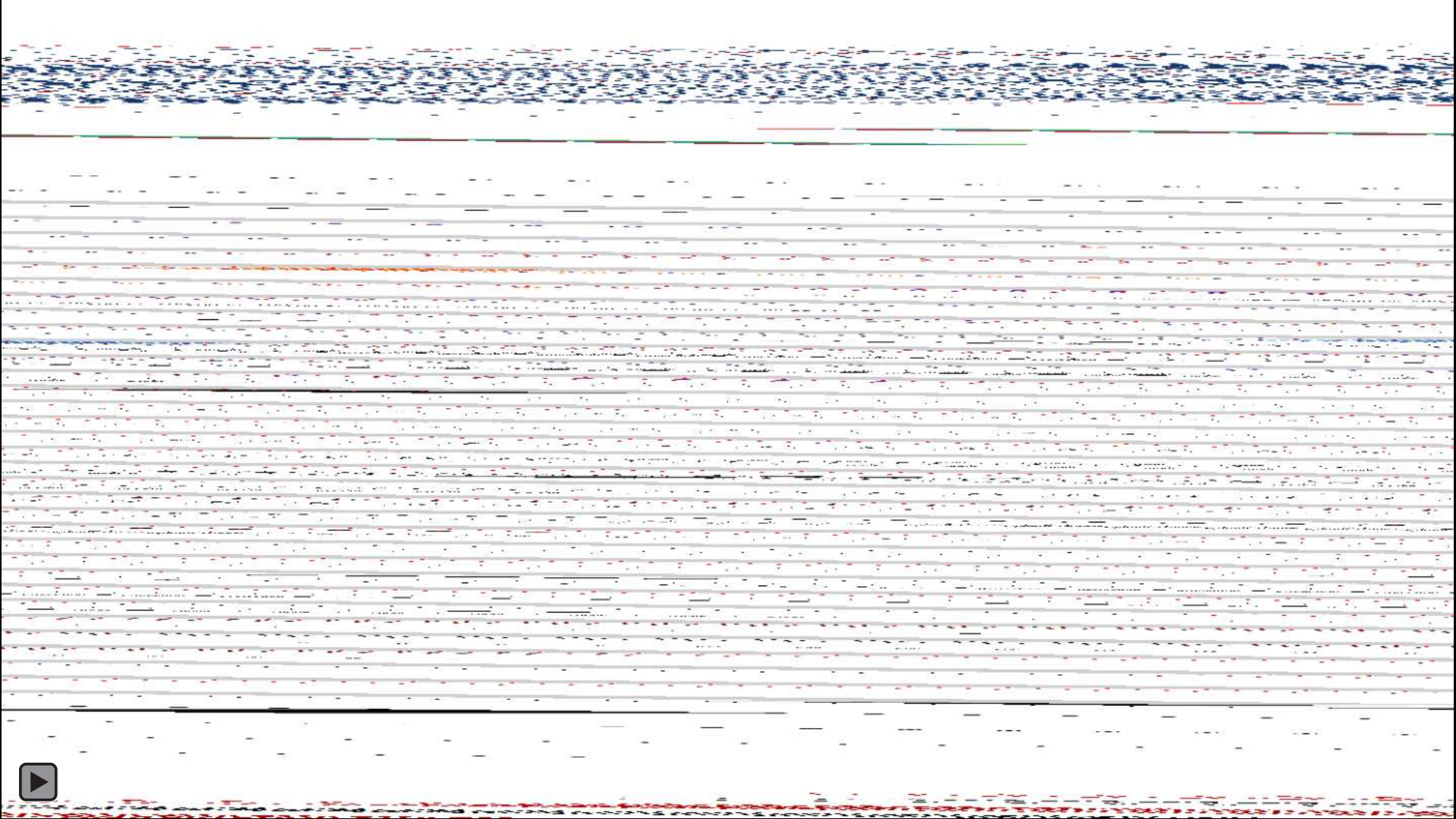


Manipulate Keyboard Operation with EMI

Outcomes

DoS Attack

Random Keystroke



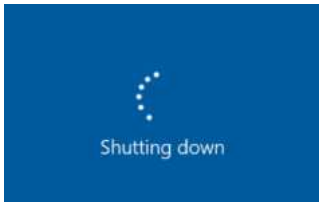
Manipulate Keyboard Operation with EMI

Outcomes

DoS Attack

Random Keystroke

Targeted Keystroke



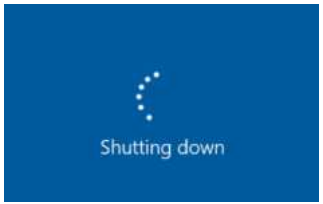
Manipulate Keyboard Operation with EMI

Outcomes

DoS Attack

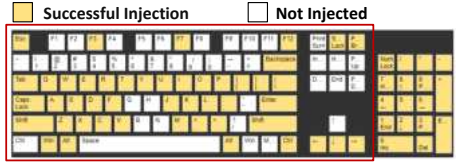
Random Keystroke

Targeted Keystroke



Hidden Keys

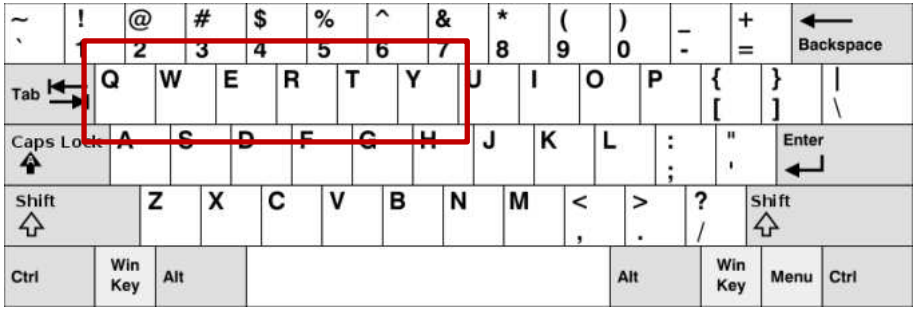
Physical Layout



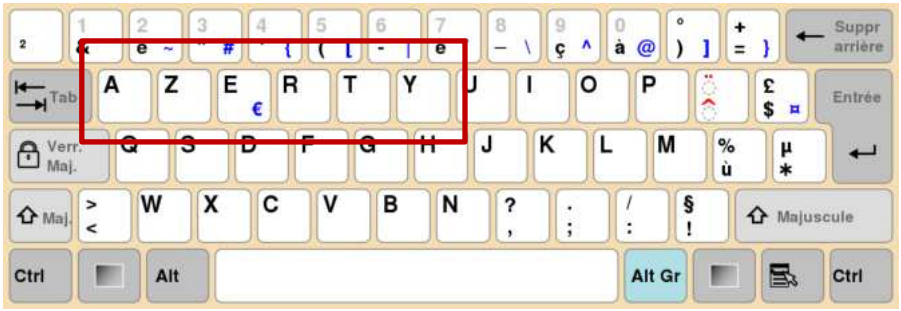
44 hidden keys

Why keyboards can accept EMI?

Keyboard Physical Layout



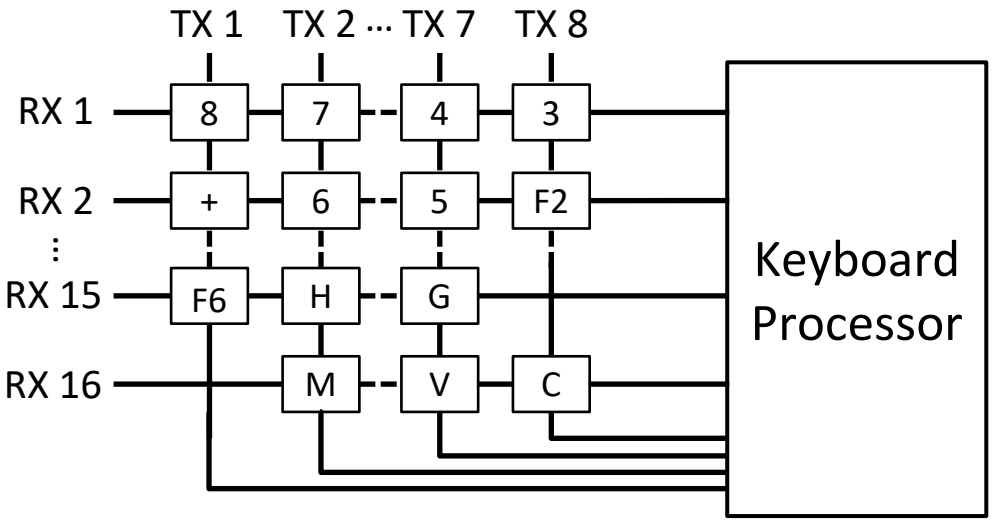
QWERTY Keyboard



AZERTY Keyboard

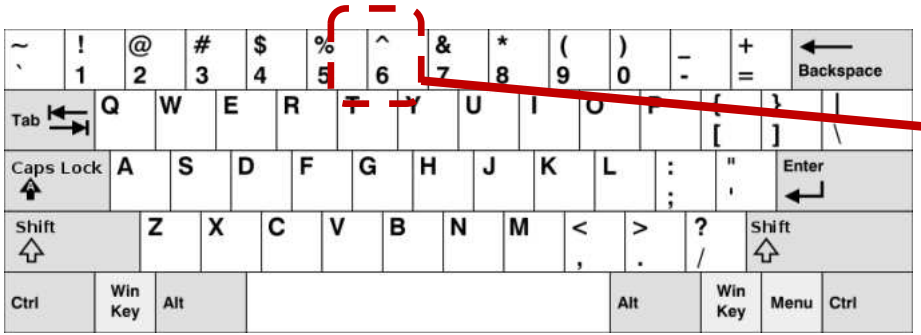
Most keyboards have 80 to 110 keys

Keyboard Logical Layout

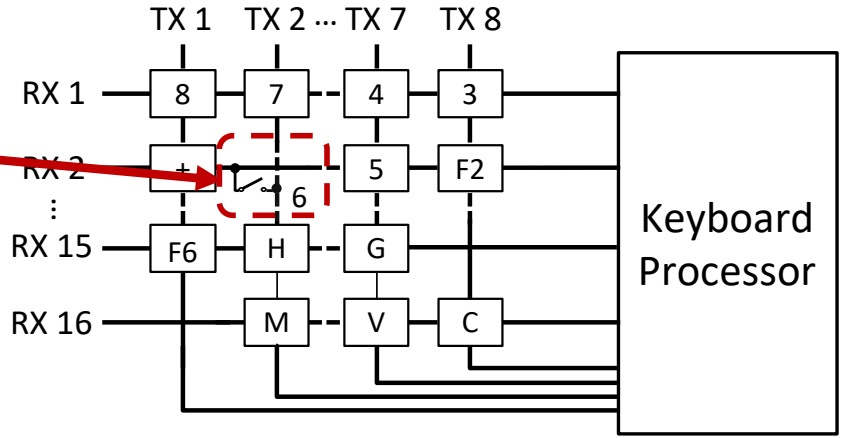


Keys are arranged in a grid-like array logically

Physical Layout vs. Logical Layout

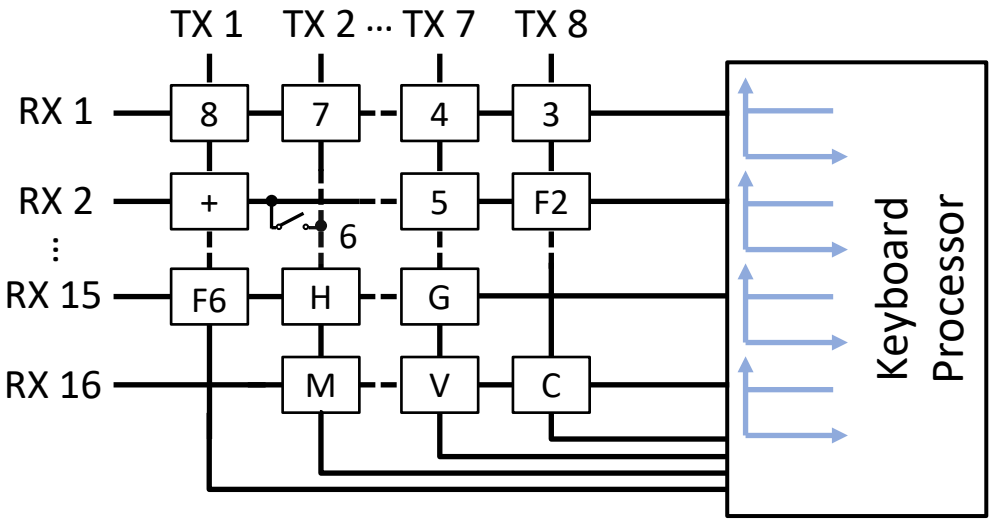


Physical layout

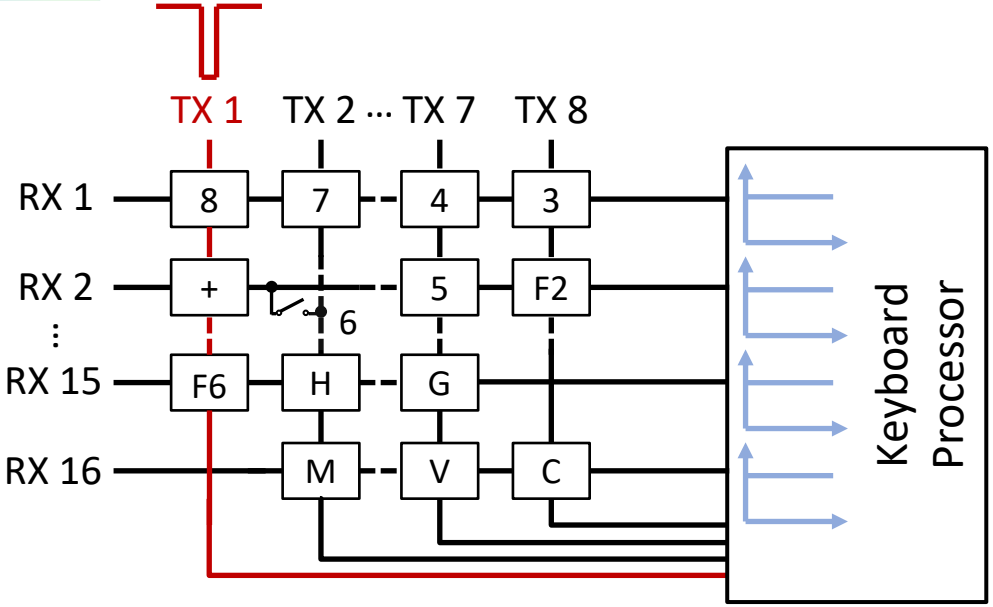


Logical layout

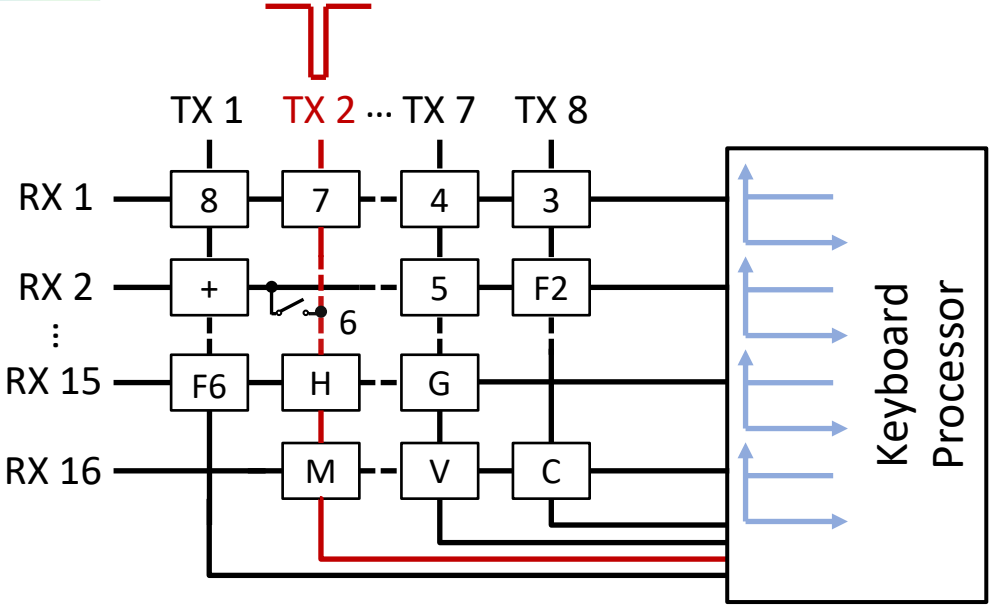
Matrix Scanning Mechanism



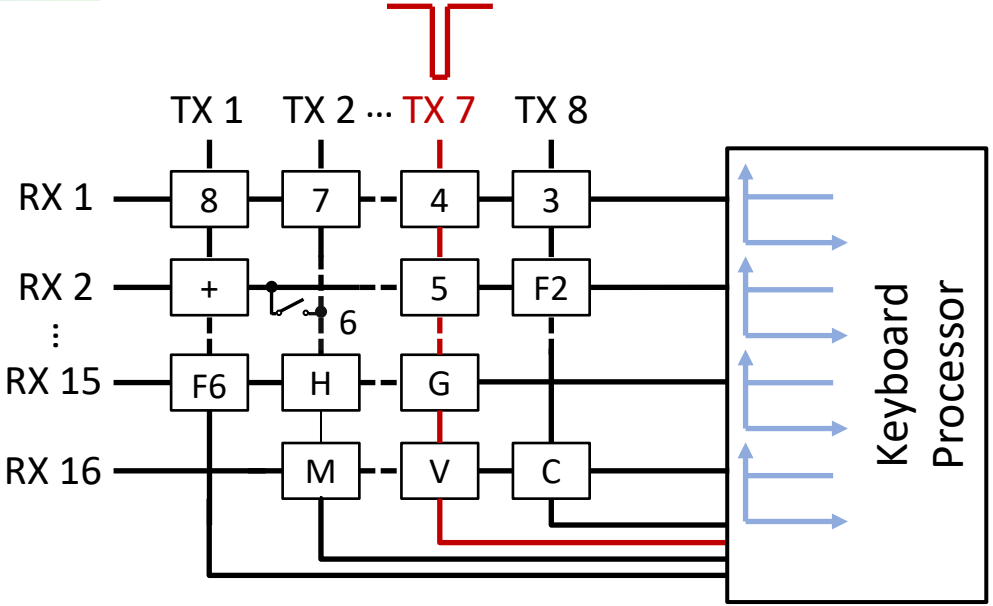
Matrix Scanning Mechanism



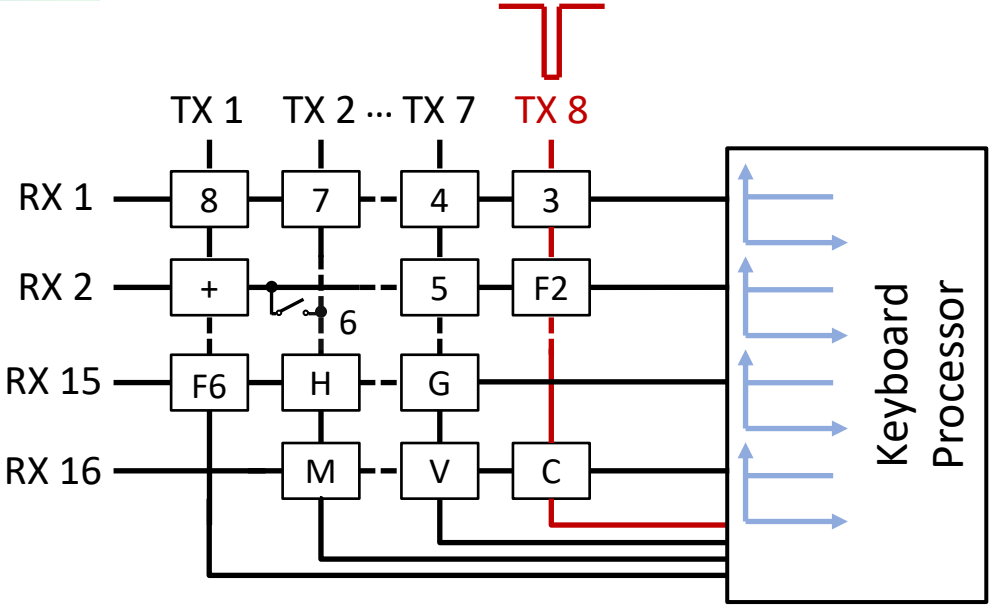
Matrix Scanning Mechanism



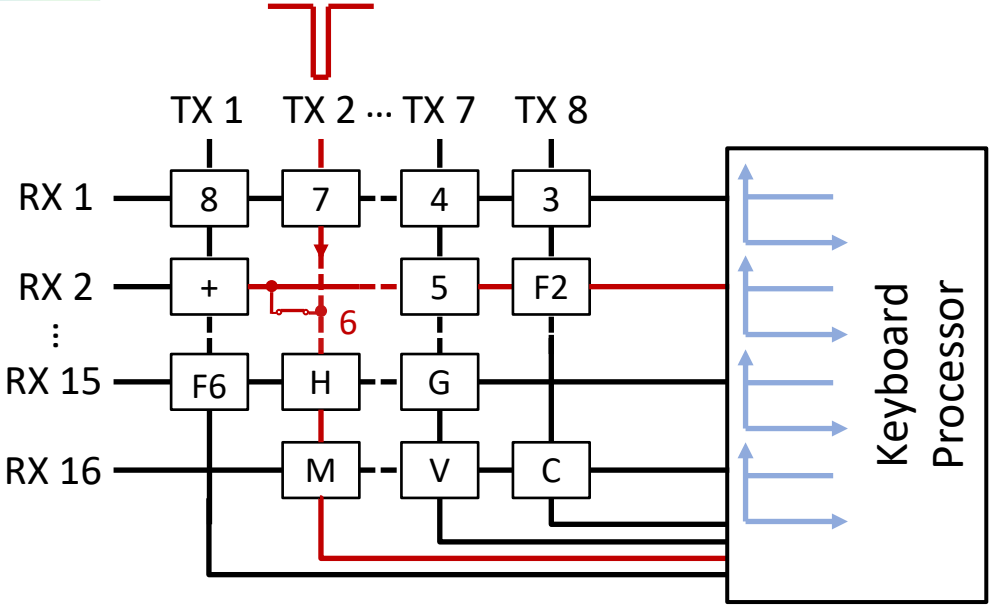
Matrix Scanning Mechanism



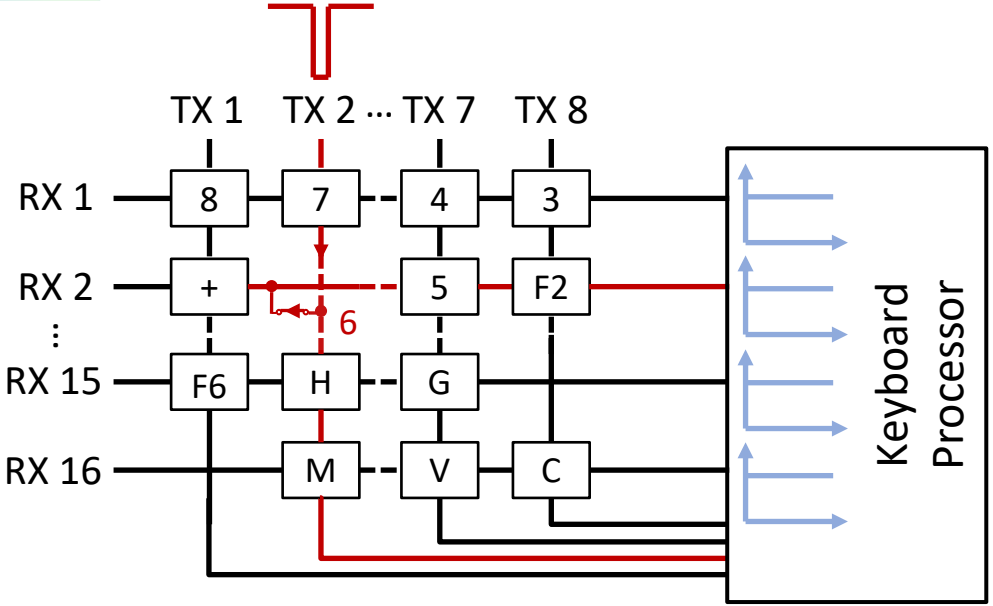
Matrix Scanning Mechanism



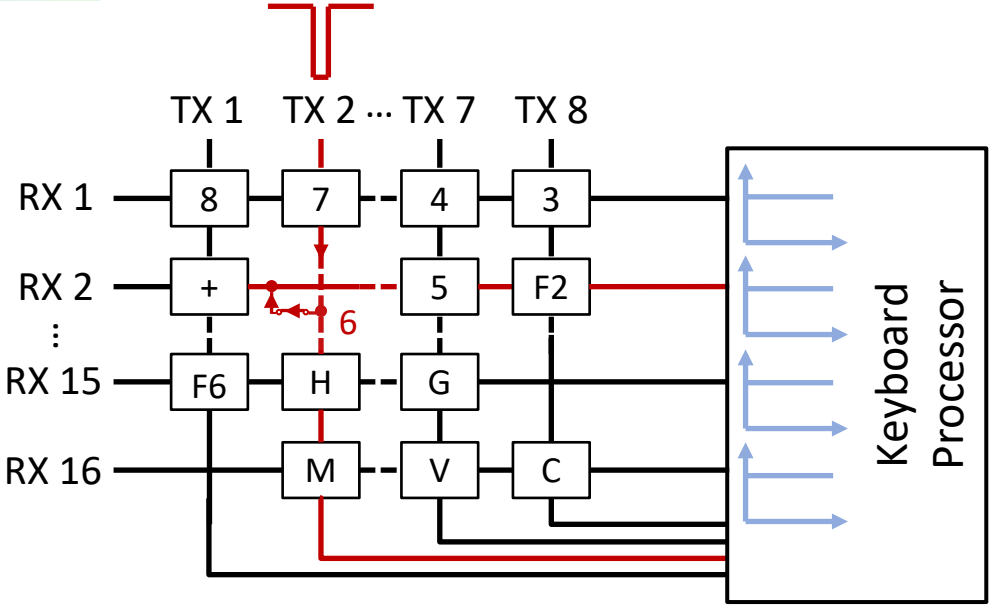
How a keypress is detected?



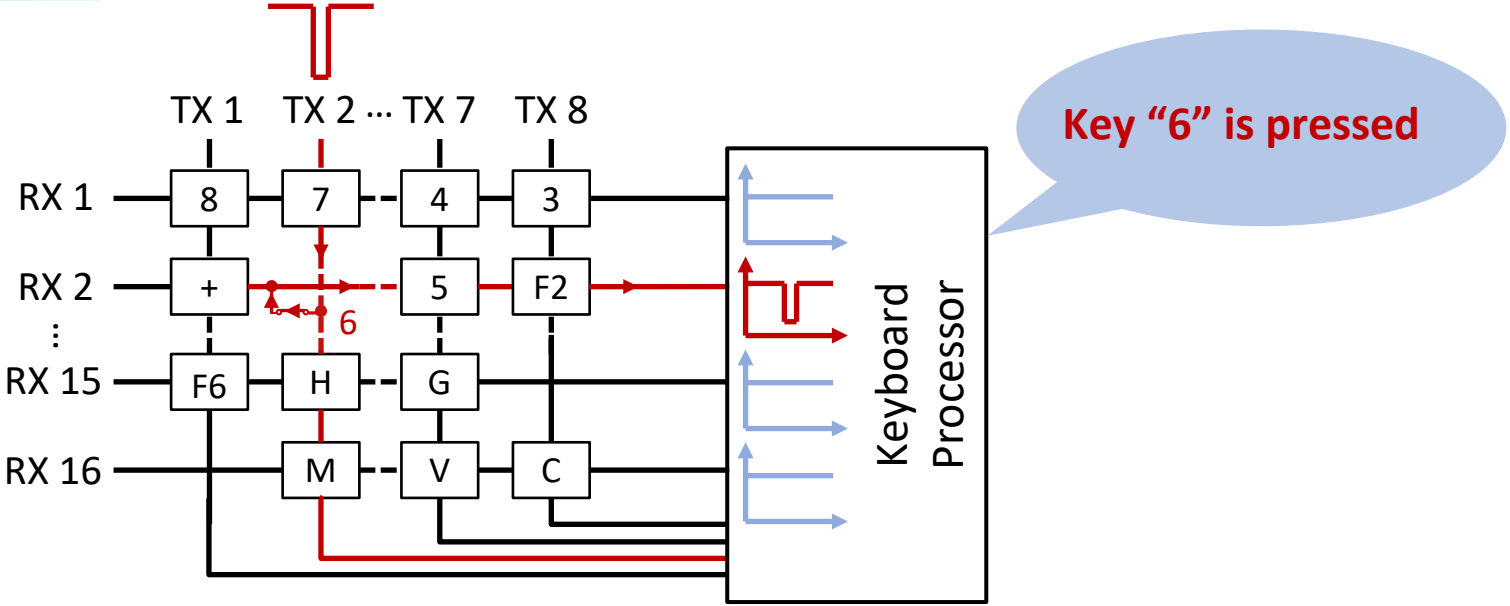
How a keypress is detected?



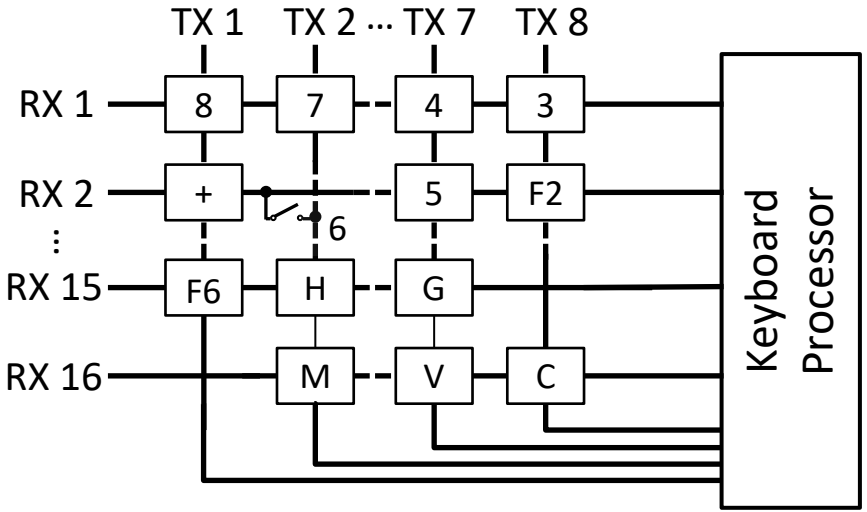
How a keypress is detected?



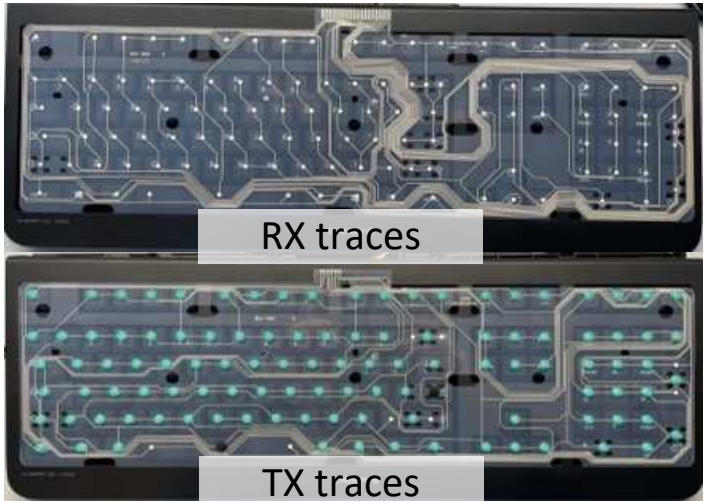
How a keypress is detected?



EMI Coupling Path



Logic traces

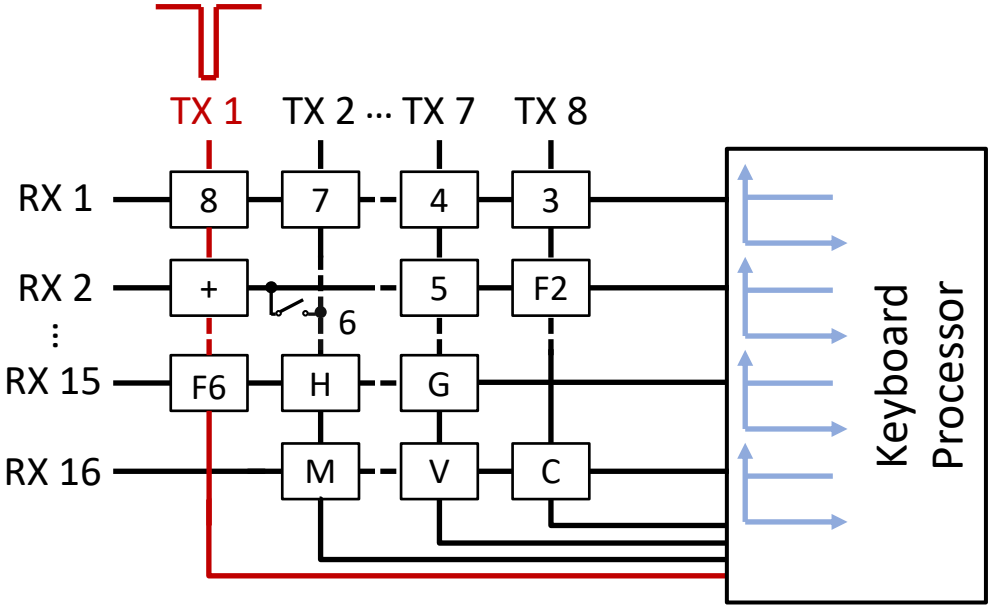


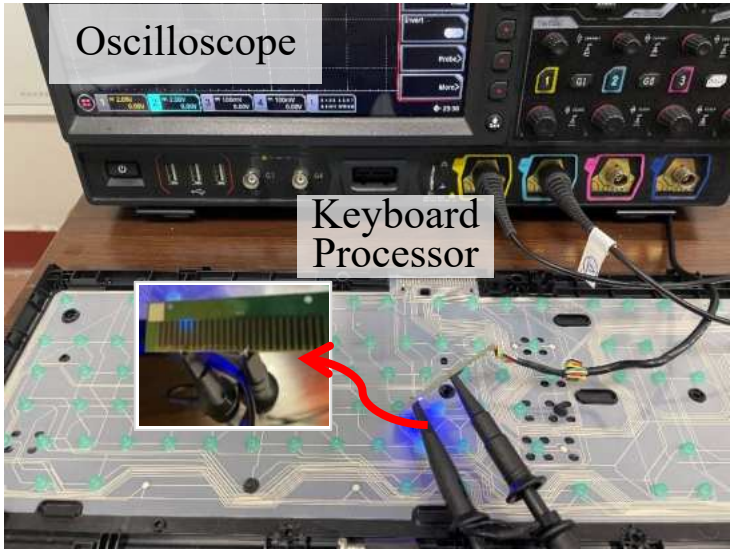
Physical traces

The long and dense physical traces are coupling paths for EMI injections.

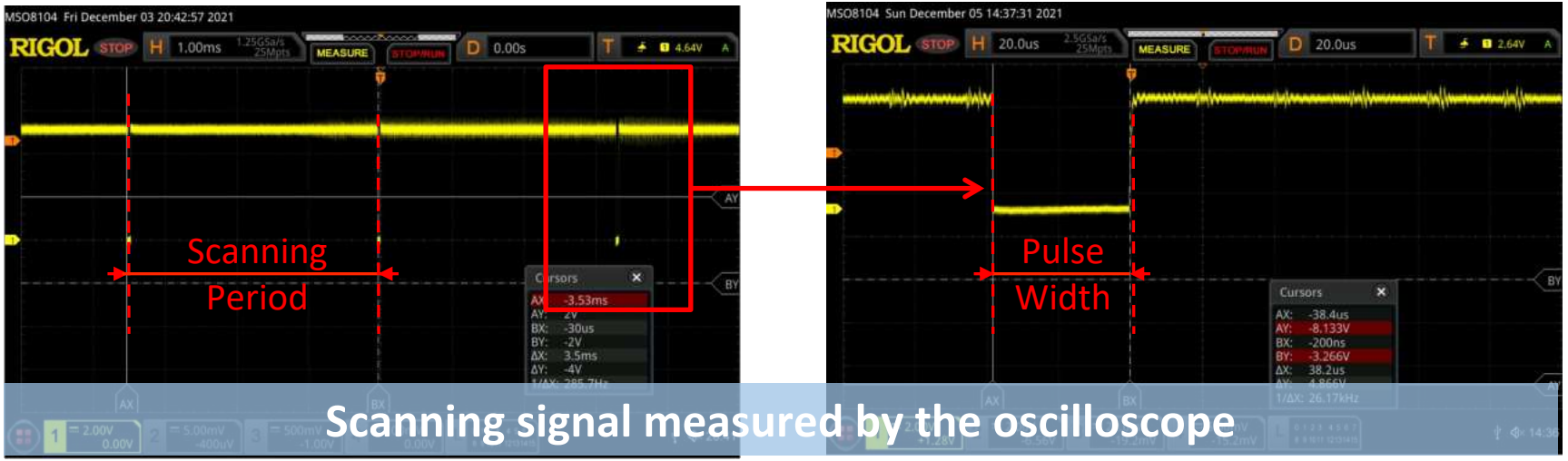
Why EMI can be detected as a keystroke?

Why EMI can be detected as a keystroke?



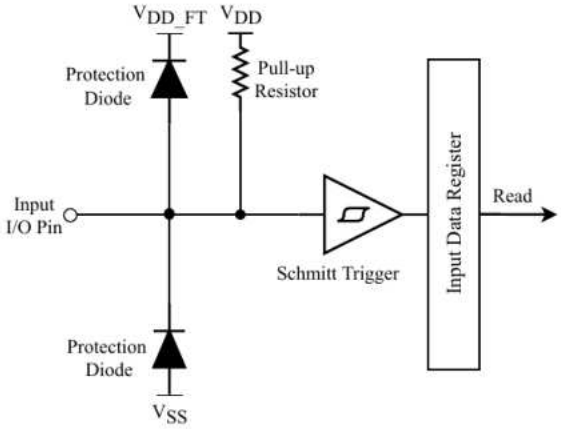


Why EMI can be detected as a keystroke?

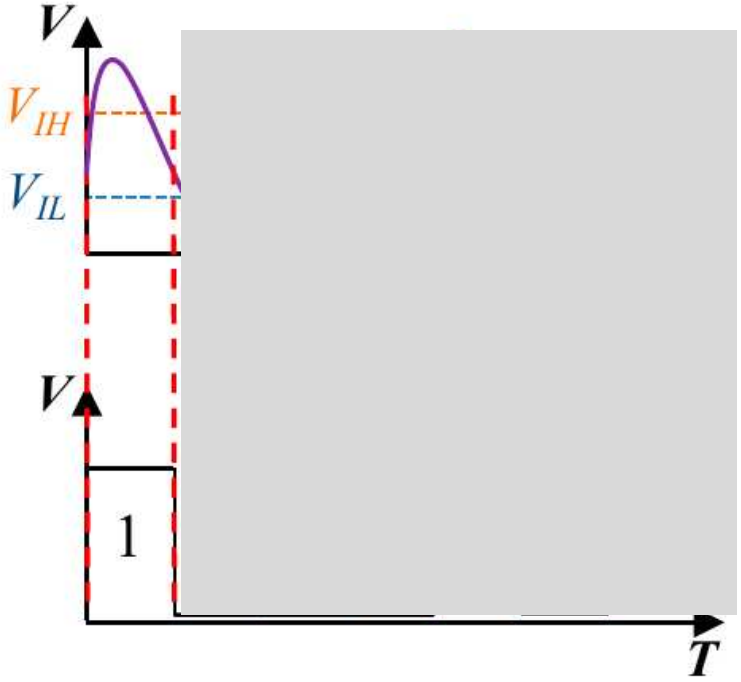


The scanning signals are simple and keystroke sensing can be spoofed

Why EMI can be detected as a keystroke?

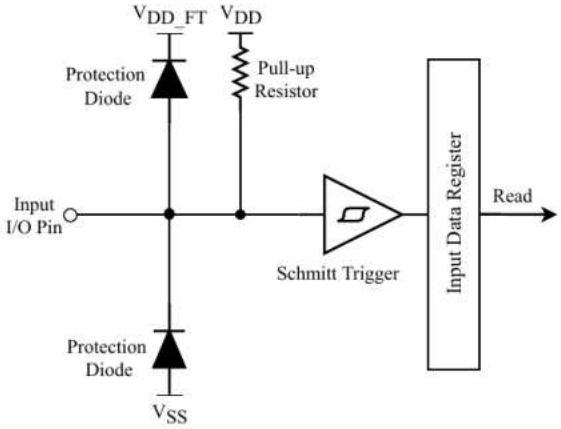


Structure of GPIO

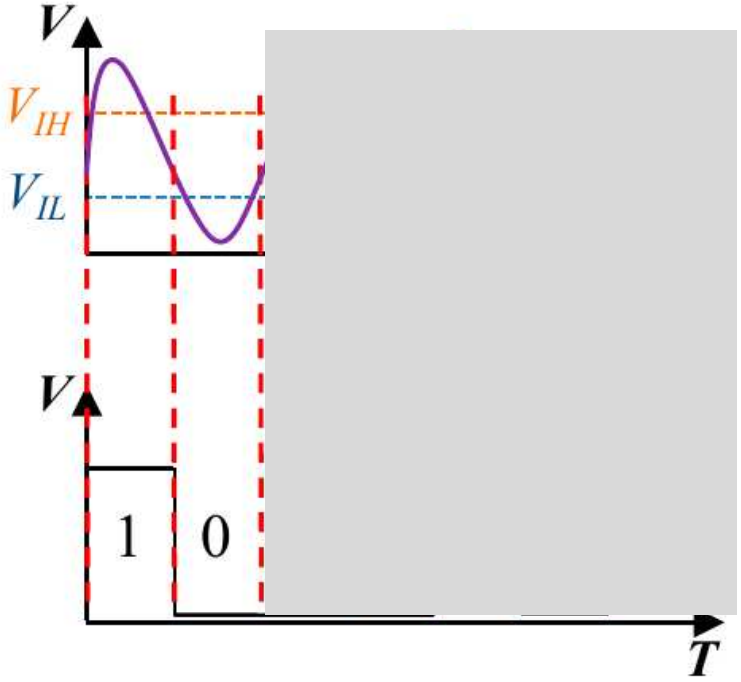


Digitalization Process

Why EMI can be detected as a keystroke?

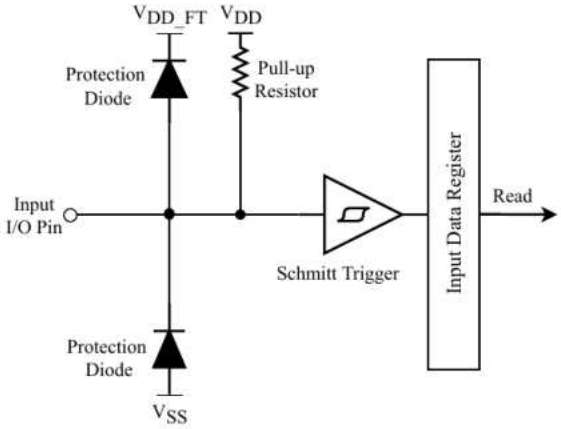


Structure of GPIO

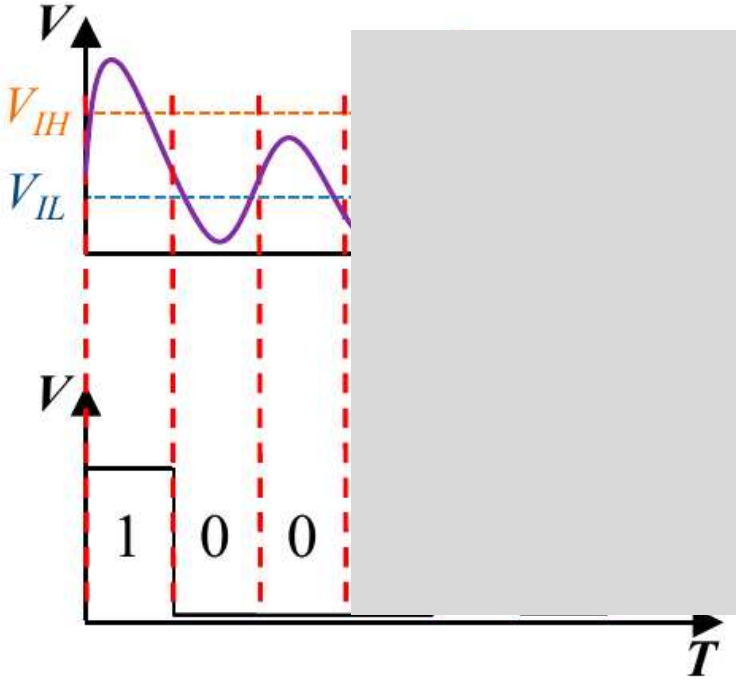


Digitalization Process

Why EMI can be detected as a keystroke?

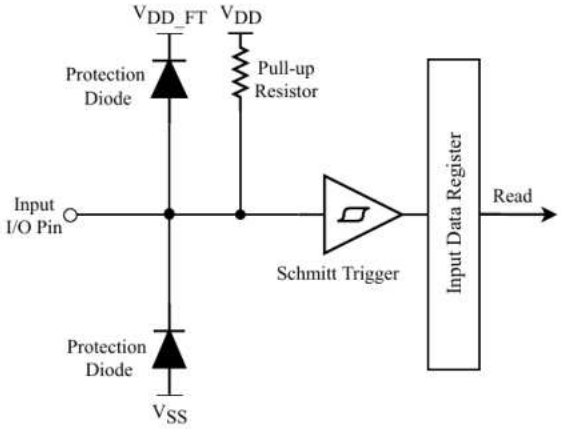


Structure of GPIO

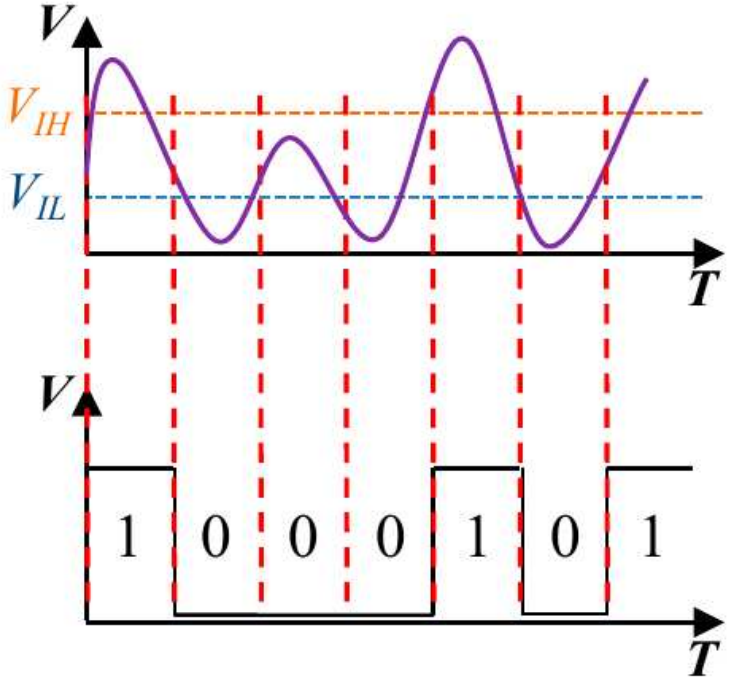


Digitalization Process

Why EMI can be detected as a keystroke?

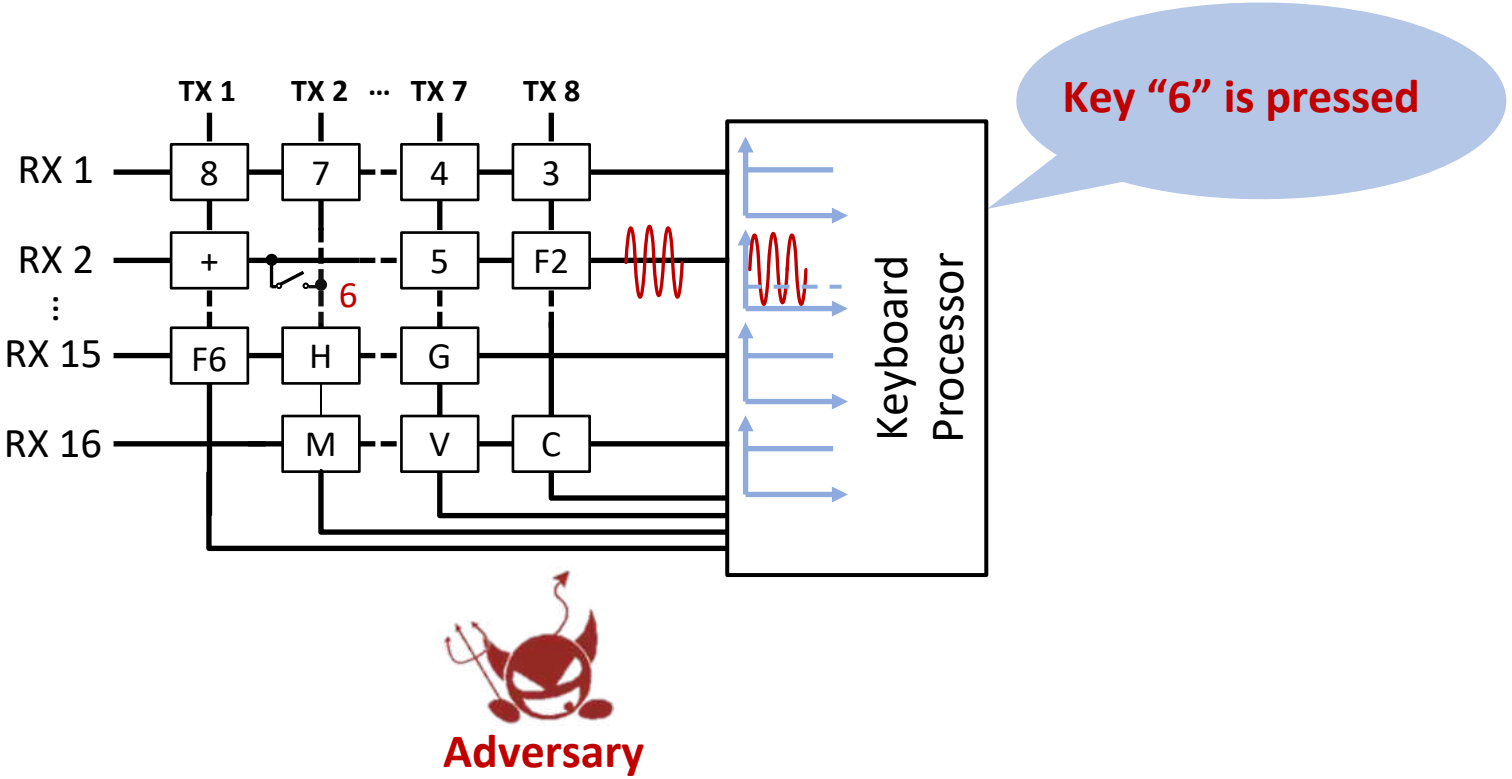


Structure of GPIO



Digitalization Process

Why EMI can be detected as a keystroke?

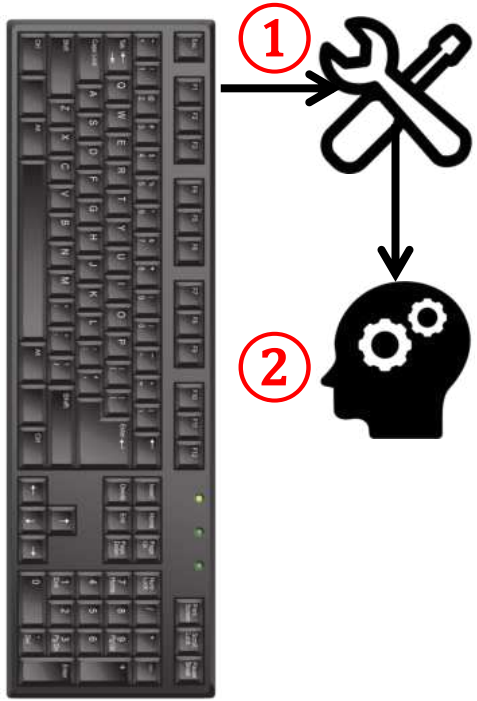


How to inject a targeted keystroke?

Steps for Targeted Keystroke Injection

Identify TX and RX traces

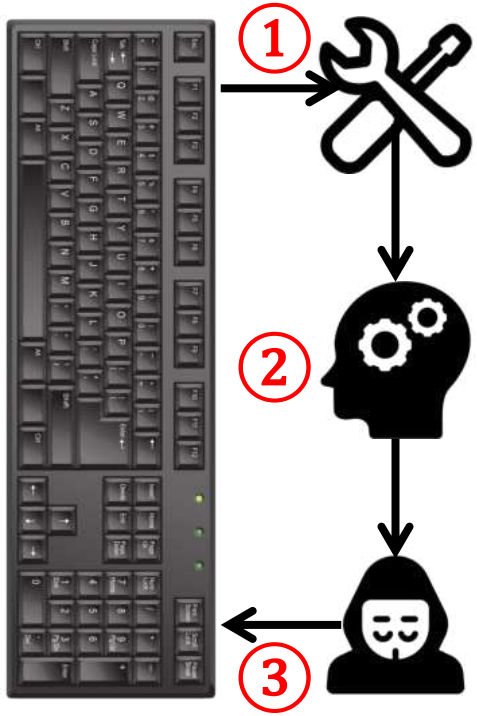
Steps for Targeted Keystroke Injection



Identify TX and RX traces

Inject EMI into the targeted RX

Steps for Targeted Keystroke Injection

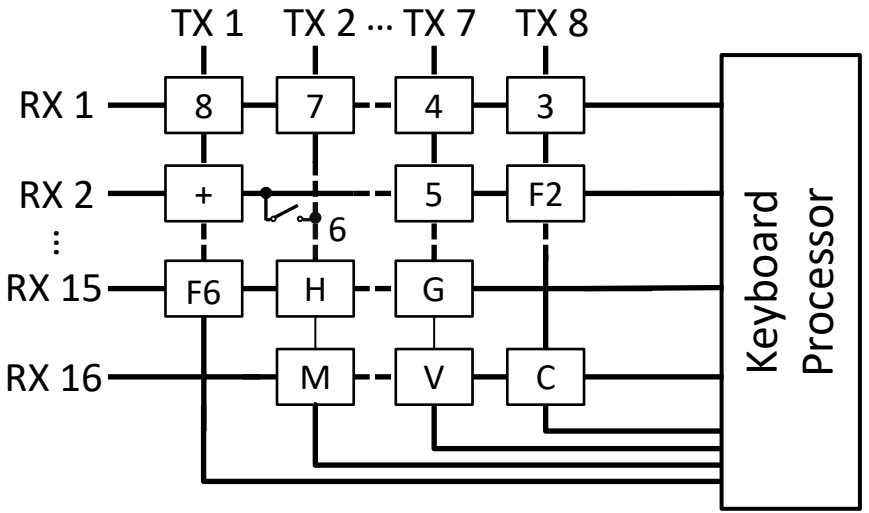


Identify TX and RX traces

Inject EMI into the targeted RX

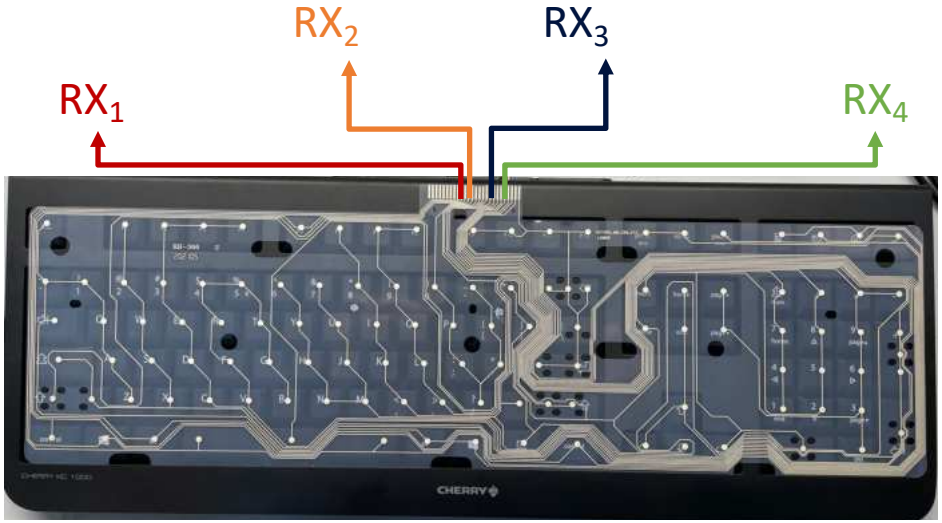
Synchronize with the targeted TX

Step 1: *Reverse Engineer* the Keyboard



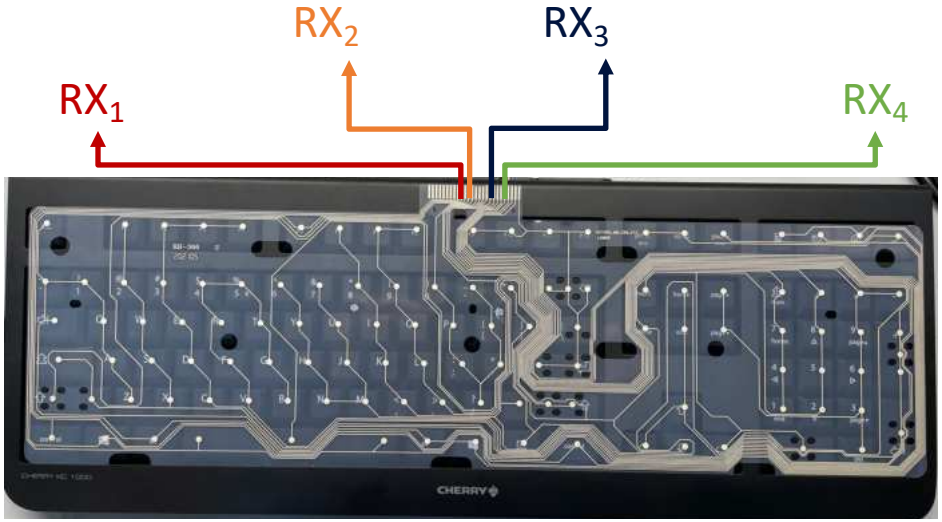
- TX/RX numbers
- Logical layout
- Matrix scanning sequence
- Matrix scanning timing

Step 2: Find *the Best Spot* to Interfere RX_1

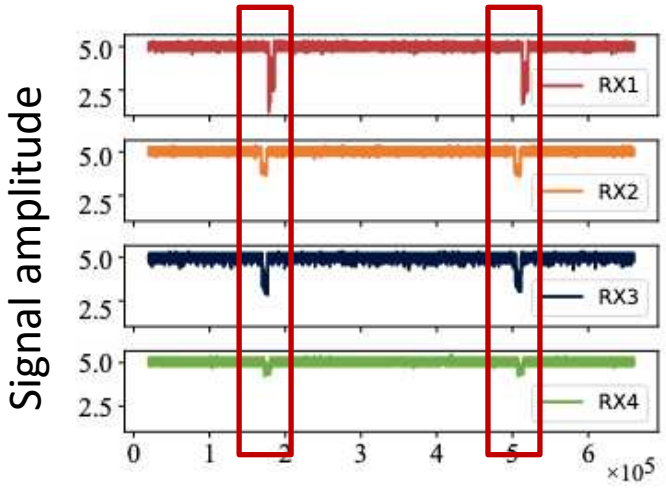


Measurement ports

Step 2: Find *the Best Spot* to Interfere RX_1



Measurement ports



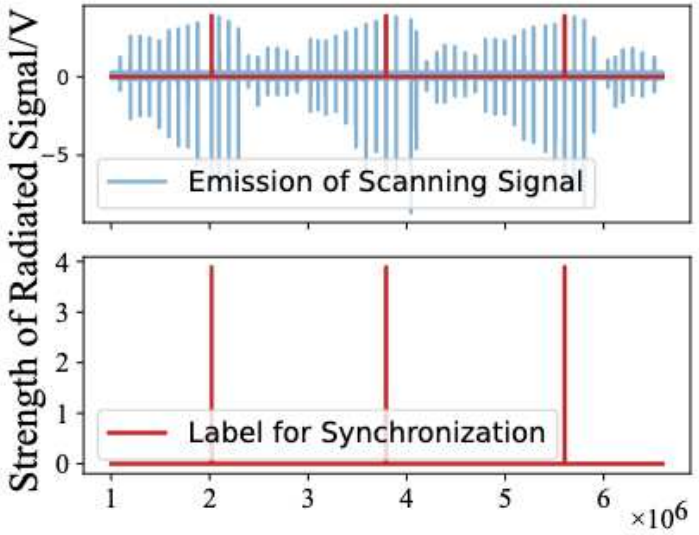
RX measurement at location 1

Inject into the different RXs with different positions

Step 3: *Synchronize* Injection with Targeted TX

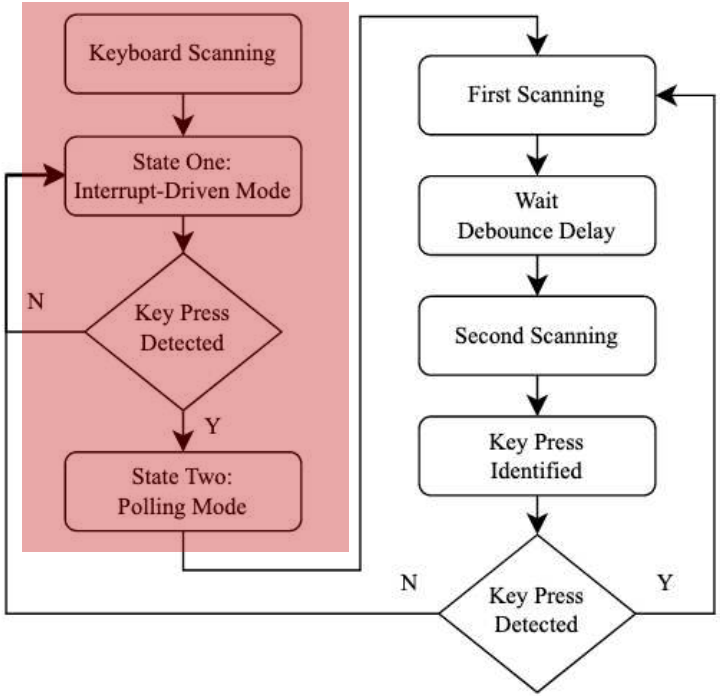
- Strategy 1: synchronize with the scanning EM radiations (EMR)

EMR



Step 3: *Synchronize* Injection with Targeted TX

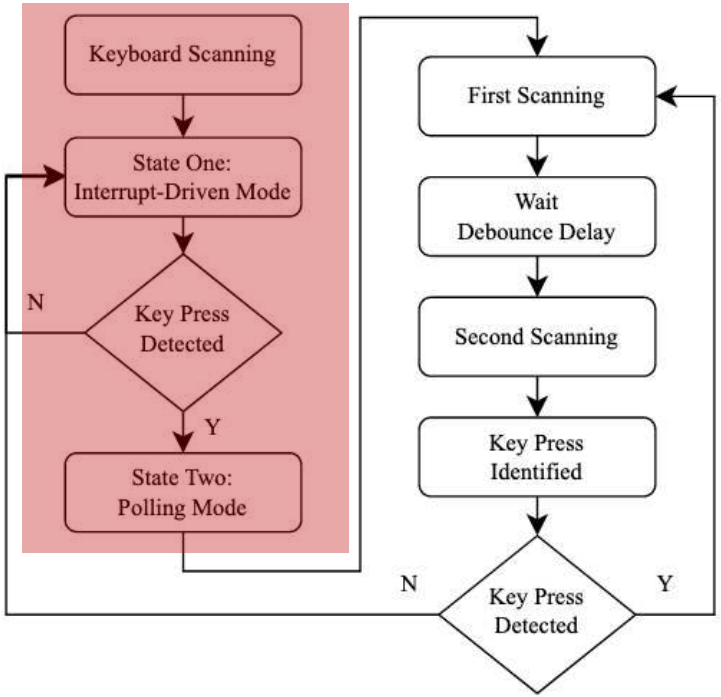
- Strategy 2: synchronization-free strategy



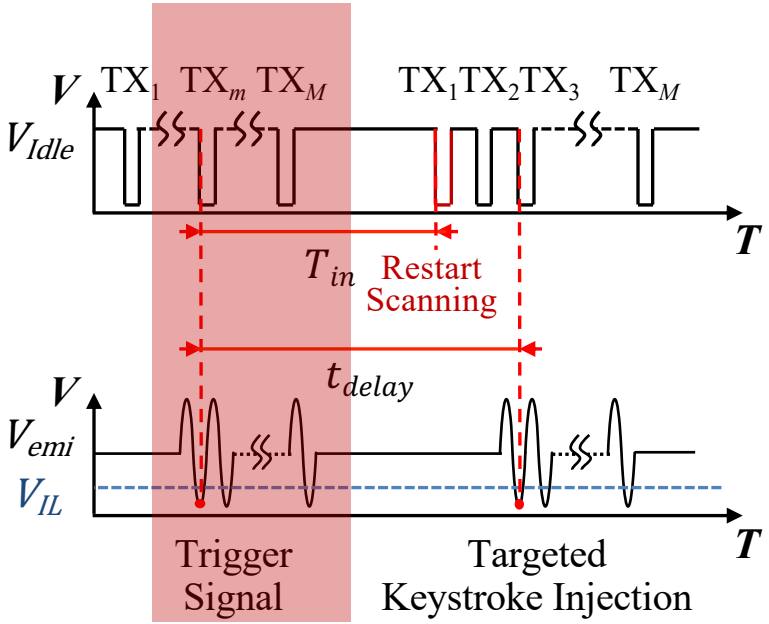
Interrupt-driven method

Step 3: *Synchronize* Injection with Targeted TX

- Strategy 2: synchronization-free strategy



Interrupt-driven method



Synchronization-free strategy

Evaluation Overview

- Compromised Devices
- Impact Factors
  - Impact of attack distance
  - Impact of table material
  - Impact of table thickness

Experiment Setup

Antenna

Compromised Devices

- 50 keyboards from 20 brands
  - Logitech, Dell, Microsoft, etc.
- 35 USB and 15 Bluetooth
- 40 Membrane and 10 Mechanical
- 44 Keyboards and 6 Keypads

Overall Performance

- Frequency sweeping experiment
  - 10 MHz – 100 MHz, 0.1MHz
  - 1 Vpp
- 48/50 keyboards are vulnerable
  - DoS: 36 keyboards
  - Keystroke injection: 39 keyboards

#	Specificaiton			DoS		Keystroke Injection		
	Vendor and Model	Structure	Protocol	Fre.	Succ.	Fre.	Succ.	Targeted Keys
1	A4TECH MK100	Mem.	USB	76-78	30/30	33-37.7	30/30	14
2	A4TECH KBN-8510	Mem.	USB	68.2-80.1	30/30	42-48	30/30	3
3	A4TECH FG1010	Mem.	BLE	88.3-100	30/30	17.3-88.2	28/30	8
4	A4TECH KB-N9100	Mem.	USB	75.2-86.3	30/30	23.5-58.7	30/30	2
5	ACER YKB913	Mem.	USB	100	30/30	44.8, 82.5 93.3	30/30	5
6	ACER KM41-2K	Mem.	BLE	17.8-19.5 31.5-33.7	30/30	15.1-17.7 27.5-31.4	30/30	5
7	BOW MK610	Mem.	BLE	80-90	30/30	10-80 90-100	30/30	6
8	BOW HW098A	Mem.	USB	10-100	30/30	✗	-	-
9	Cherry KC1000	Mem.	USB	17.8-23.1 83.3-100	30/30	23.2-31.3 42.1-83.2	30/30	10
10	Cherry Stream	Mem.	USB	✗	-	✗	-	-
11	Dell KB216-t	Mem.	USB	23.9-27.7 37.7-44.2 73.3-100	30/30	✗	-	-
12	Dell KM17	Mem.	BLE	15-96	30/30	96.1	30/30	1
13	Dell KM2123D	Mem.	BLE	10-26.5 27-74.8	30/30	26.6 75-100	30/30	2
14	Dell KB3022D	Mech.	USB	✗	-	93.3-100	29/30	1
15	Dell KB522P	Mem.	USB	24.0-24.5 92.7-97.6	30/30	✗	-	-
16	HP GK400F	Mech.	USB	✗	-	43.6-100	30/30	5
17	HP KM10	Mem.	USB	10-27.6	28/30	27.7-85.9	30/30	3
18	HP CS10	Mem.	BLE	28.7-57.1	30/30	18.3-28.6 57.2-99	30/30	3
19	IKBC W200	Mech.	BLE	✗	-	86-100	30/30	3
20	Keycool K-9	Mech.	USB	✗	-	37.2-62.3 74.9-96.1	30/30	5
21	Lenovo K4800S	Mem.	USB	93-100	30/30	38.9-44.8 76.6-90	30/30	2
22	Lenovo MK23	Mem.	BLE	33.6-42 77.6-100	30/30	17.3-33.5 42-77.5	30/30	2
23	Lenovo K104	Mech.	USB	✗	-	35-45 70.5-87.9 95-100	30/30	2
24	Lenovo EKB-536A	Mem.	USB	38.7-45.2 88.0-96.8	30/30	✗	-	-
25	Logitech MK235	Mem.	BLE	73-100	30/30	18-48	30/30	3

#	Specification			DoS		Keystroke Injection		
	Vendor and Model	Structure	Protocol	Fre.	Succ.	Fre.	Succ.	Targeted Keys
26	Logitech MK275	Mem.	BLE	39.2-98.2	30/30	19.1-37.6	30/30	4
27	Logitech MK220	Mem.	BLE	37.7-43.3 49.4-100	30/30	17.1-37.6 43.4-49.3	30/30	4
28	Logitech G610	Mech.	USB	✗	-	96.9-97.8	30/30	3
29	Microsoft 850	Mem.	BLE	36.3-52.2 75.4-100	30/30	52.3-75.3	30/30	3
30	Microsoft 900	Mem.	BLE	32.4-46.5 82.6-100	30/30	32.4 82.6	30/30	1
31	Philips SPK6234	Mem.	USB	98.8	30/30	✗	-	-
32	Philips SPT6103	Mem.	BLE	29.5-57 63-100	30/30	17.5-29.5 57-63.2	30/30	3
33	Philips SPK6212B	Mem.	USB	79.1-100	29/30	10-79	30/30	4
34	Rapoo K150	Mem.	USB	66.1-100	30/30	✗	-	-
35	Rapoo X125S	Mem.	USB	74.1-100	30/30	✗	-	-
36	Rapoo 8050T	Mem.	BLE	19.3-20	30/30	20.1-100	30/30	1
37	Razer RZ03-0146	Mem.	USB	✗	-	10-100	30/30	3
38	Razer RZ03-0147	Mem.	USB	✗	-	10-100	30/30	3
39	Thunderobot KG3089R	Mech.	USB	✗	-	62-89	30/30	4
40	Thunderobot KG3104R	Mech.	USB	✗	-	38-39.8 91-100	30/30	2
41	Thunderobot KM400	Mem.	BLE	87-100	30/30	✗	-	-
42	Xiaomi HZJP01YM	Mech.	USB	✗	-	10-100	30/30	5
43	Xiaomi WXJS01YM	Mem.	BLE	42-85	29/30	10-40 86-100	30/30	3
44	Xiaomi JXJP01MW	Mech.	USB	✗	-	33.3-33.7	30/30	1
45	A4TECH FK13P	Mem.	USB	33.4 41.9	30/30	22-33 34-38.4	30/30	2
46	CoolSpeed	Mem.	USB	30.1-42.8 68.1-100	30/30	19.6-30.0 42.9-68.0	30/30	2
47	Hiz	Mem.	USB	87.9-90	30/30	29.6-43.3	30/30	3
48	IBM	Mem.	USB	38.1-42.2 74-77 83.1-100	30/30	26.9-38 42.3-45.5 77.1-83	30/30	3
49	Rapoo K10	Mem.	USB	27.6-45.7 67.3-100	30/30	✗	-	-
50	Sunread SKB886S	Mem.	USB	✗	-	✗	-	-

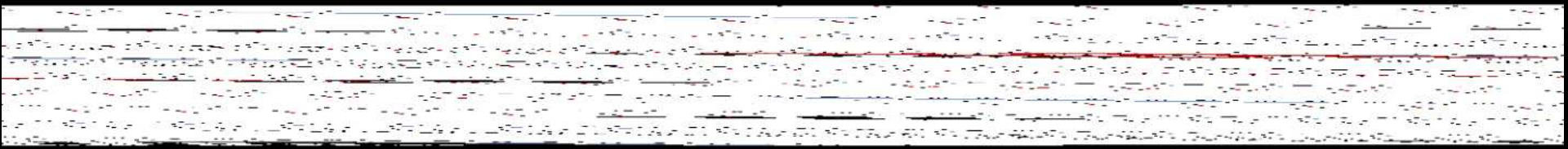
Impact Factors: Evaluation Metrics

- *Success Rate (SR)* is the percentage of attacks that successfully achieve the targeted attack outcomes.
- *Actions per Minute (APM)* is the number of injected keystrokes per minute to evaluate the injection speed.

Evaluation: Impact of Injection Distance

Injection Distance	DoS Attack (Success Rate)			Keystroke Injection (Action per Minute)			
	Dell KB216t	Lenovo EKB-536A	Rapoo K150	Human (Max)	Razer RZ03-0147	Thunderobot KG3104R	Xiaomi HZJP01YM
0 mm	100%	100%	100%	< 1000	6804.0	23612.4	3962.6
10 mm	100%	100%	100%		4448.2	19453.8	2403.0
20 mm	42%	62%	100%		2951.8	10475.2	1635.6
30 mm	0	0	100%		1017.8	2632.2	393.8

GhostType attacks can inject keystrokes up to 30 mm



Impact of Table Material

Table Material (10 mm)	DoS Attack (Success Rate)			Keystroke Injection (Action per Minute)			
	Dell KB216t	Lenovo EKB-536A	Rapoo K150	Human (Max)	Razer RZ03-0147	Thunderobot KG3104R	Xiaomi HZJP01YM
Solid Wood	100%	100%	100%	< 1000	3808.2	18464.8	2311.2
Acrylic Sheet	100%	100%	100%		4248.4	16901.4	2336.0
MDF	100%	100%	100%		4492.2	17310.4	2423.0
Glass	100%	100%	100%		4035.8	14964.6	2375.4

GhostType attack works on common table materials

Impact of Table Thickness

Table Thickness (Acrylic sheet)	DoS Attack (Success Rate)			Keystroke Injection (Action per Minute)			
	Dell KB216t	Lenovo EKB-536A	Rapoo K150	Human (Max)	Razer RZ03-0147	Thunderobot KG3104R	Xiaomi HZJP01YM
10 mm	100%	100%	100%	< 1000	4248.4	16901.4	2336.0
15 mm	100%	100%	100%		3570.0	11105.0	1828.6
20 mm	100%	100%	100%		2509.2	7781.2	1064.6
25 mm	70%	0	100%		4035.8	14964.6	2375.4

GhostType attack can be conducted under the common table top

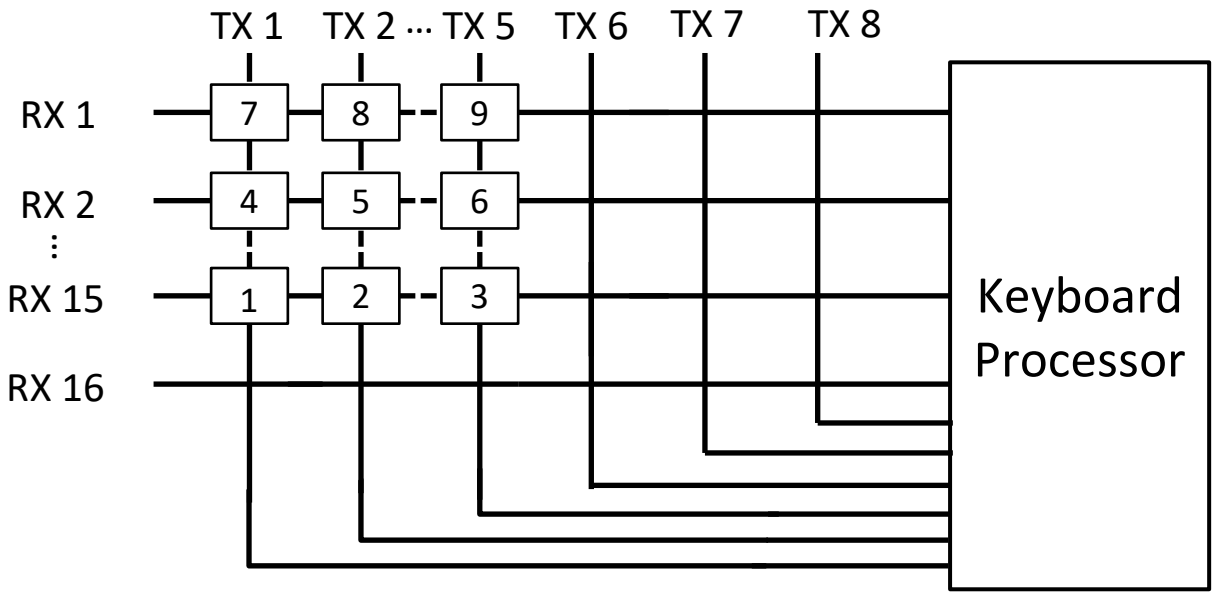
Hidden Keys

How hidden key occurs?

Hardware layout designer

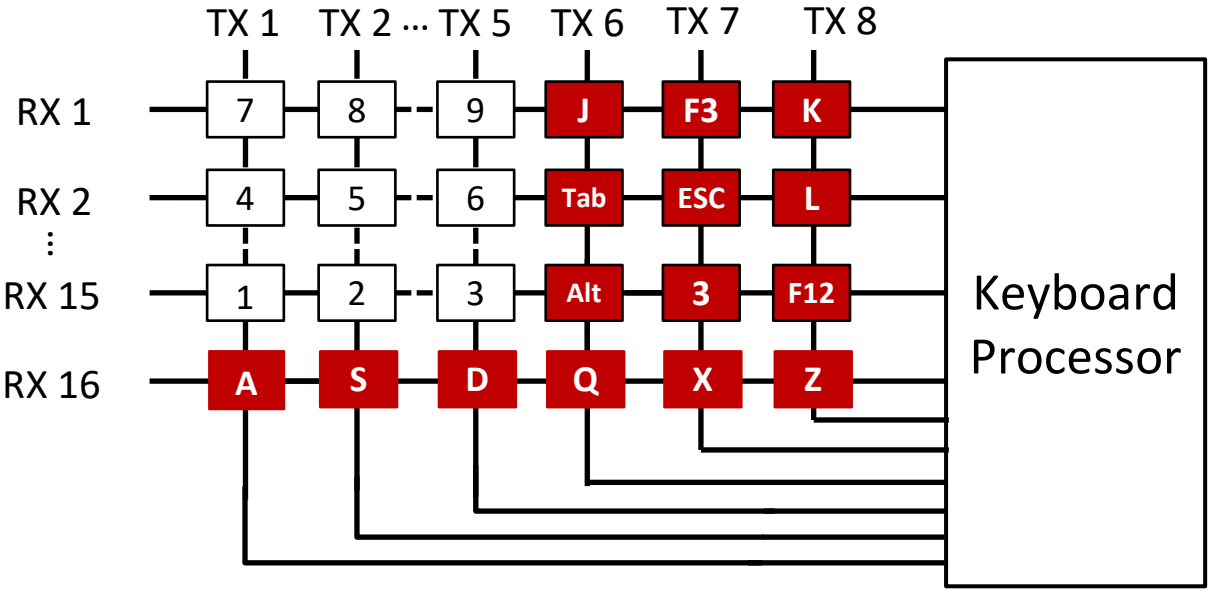
Firmware designer

How hidden key occurs?



Hardware layout designer

How hidden key occurs?

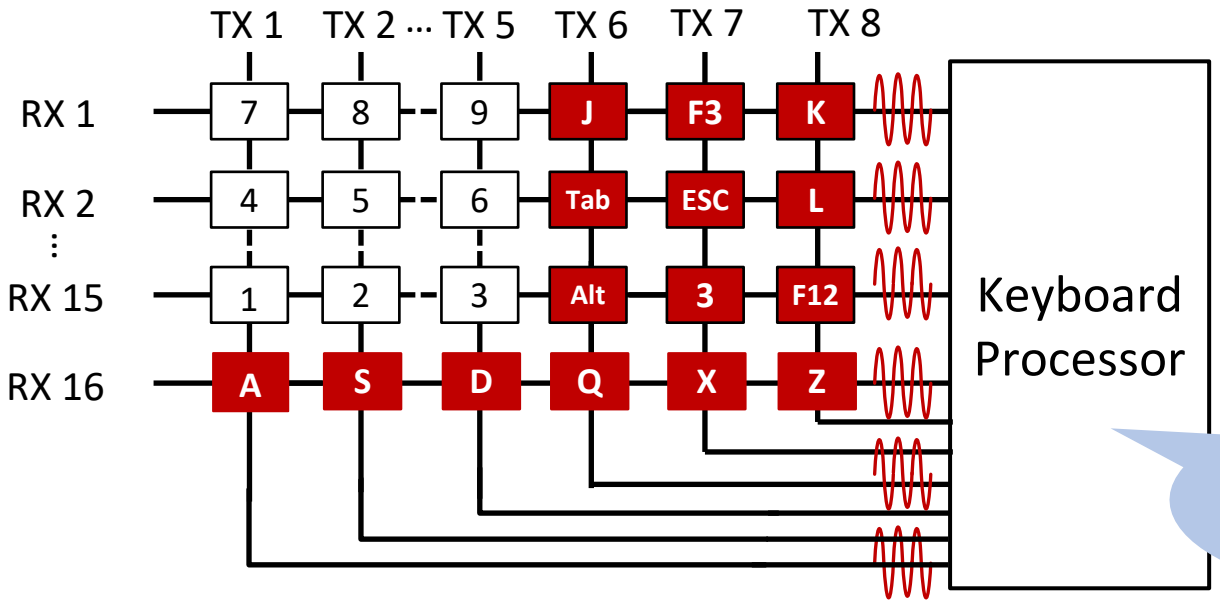


Firmware designer

Hidden keys exist in keyboard firmware

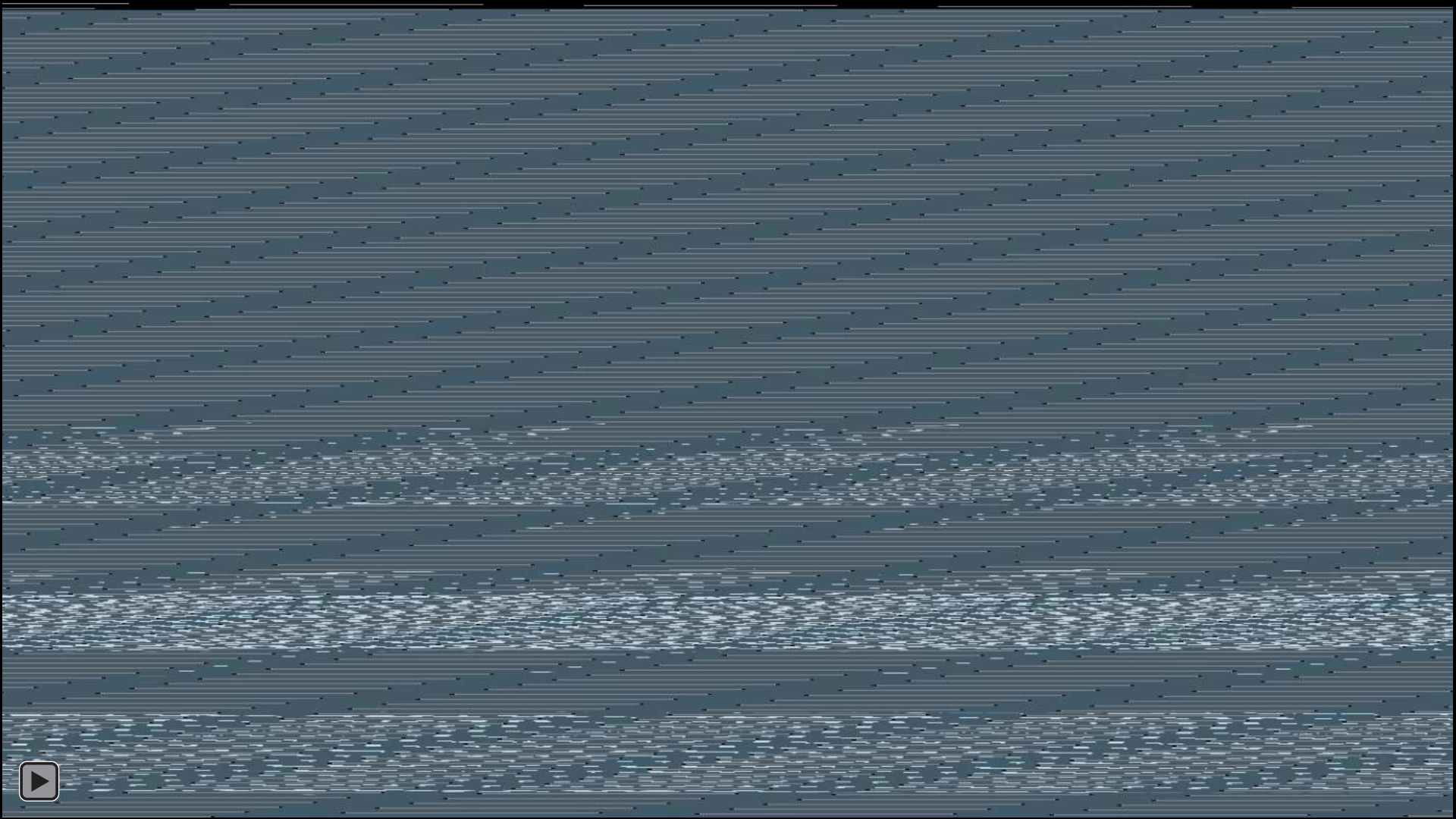
How hidden key occurs?

Adversary



Hidden keys

Hidden keys can be injected with EMI



Discussion: countermeasures

- *Shield* Keyboards with metal materials
- Enhance the *keystroke sensing mechanism*
- Remove the non-existent keys from the *keyboard firmware*

Future work

- Given the keystroke vulnerability, analyze *the impact on the system*

- Investigate vulnerabilities in *high-security applications* such as ATM public terminals

Conclusion

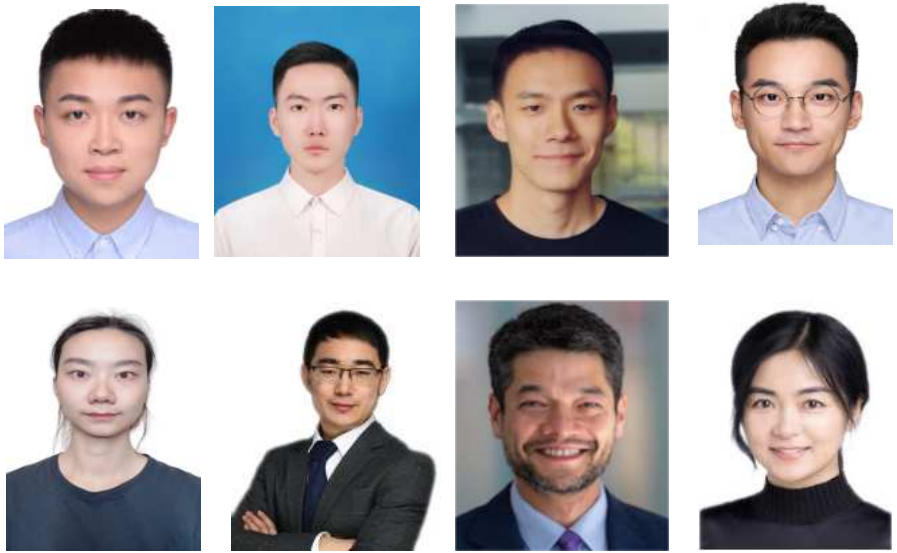
- Review *the first analog attack against keyboards* can bypass digital countermeasures

- Validate the feasibility of *contactless keystroke injections with EMI*.

- Assess the vulnerabilities on *50 off-the-shelf keyboards* and propose countermeasures.

GhostType: The Limits of Using Contactless Electromagnetic Interference to Inject Phantom Keys into Analog Circuits of Keyboards

Thanks for listening! Q&A



Qinhong Jiang

qhjiang@zju.edu.cn

https://jackjiang313.github.io/

Paper

Demo