August 26th, 2019
CHES, Atlanta, U.S

Electromagnetic Information Extortion from Electronic Devices Using Interceptor, Its Countermeasure

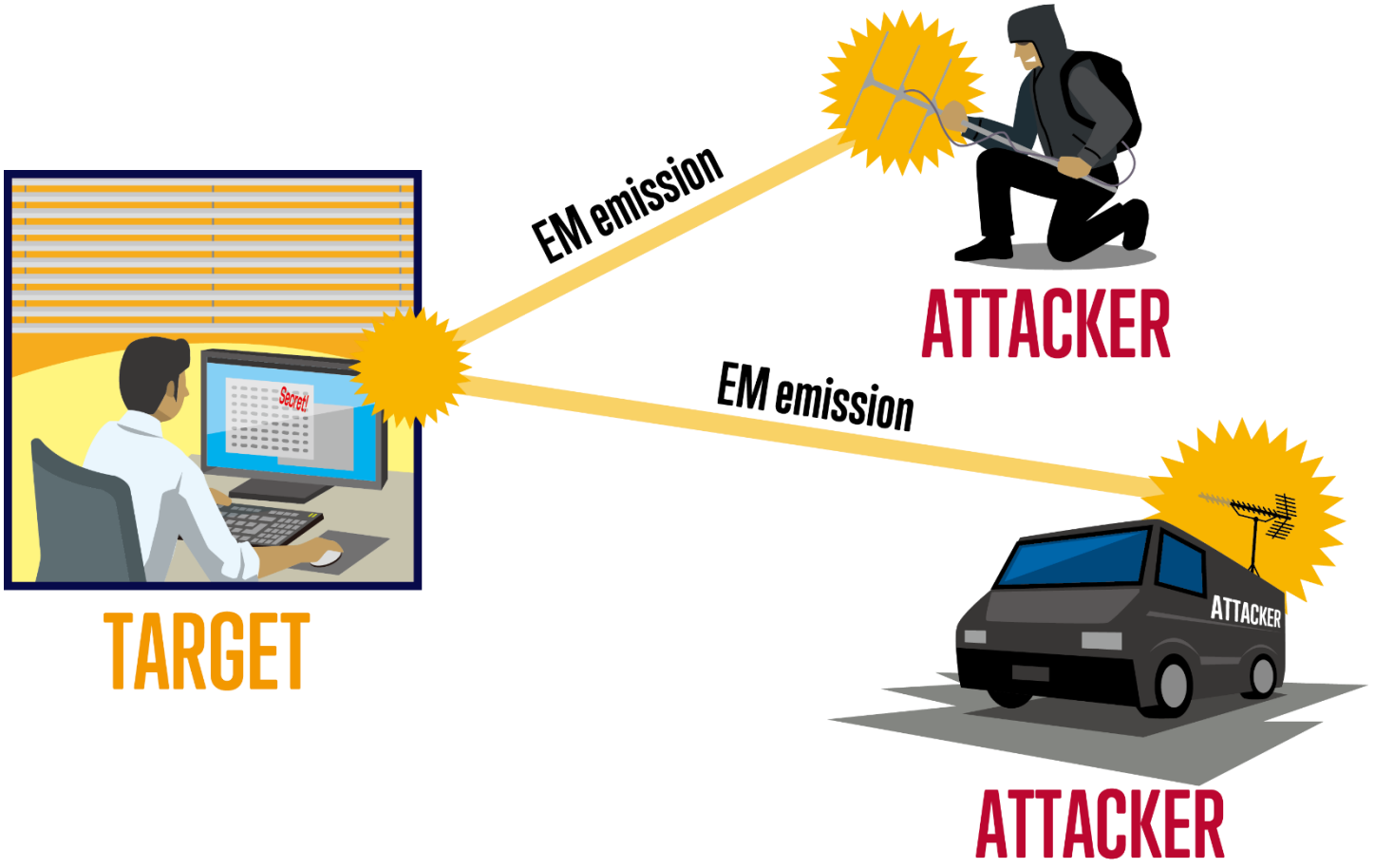
Masahiro **Analog** Kinugawa
Daisuke **Digital** Fujimoto
Yuichi EM Hayashi

NIT, Sendai College

Nara Institute of Science and Technology NAIST

NAIST

Conventional EM information leakage threat



Demo

https://youtu.be/nL2wM-4xRkI

https://youtu.be/FHaKnzb--a8

Y. Hayashi, et al. “A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation, " 21st ACM CCS

Targets of EM information leakage

Touch Panel of ATM

Desktop/Laptop PC

www.panasonic.co.jp

Display (CRT/LCD)

www.nec.co.jp

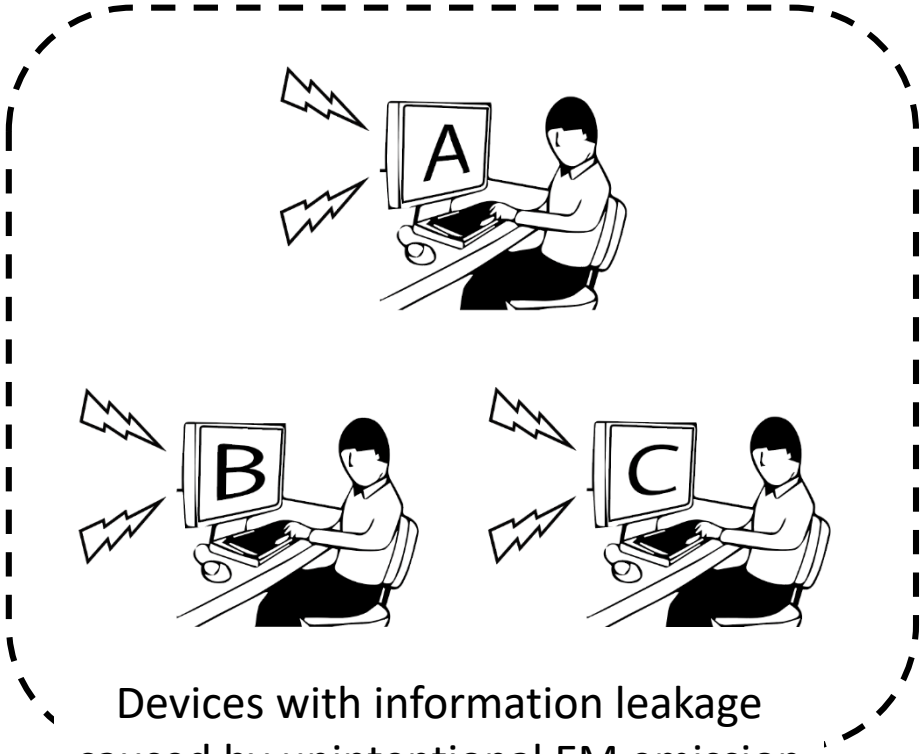
Printer

Cryptographic modules

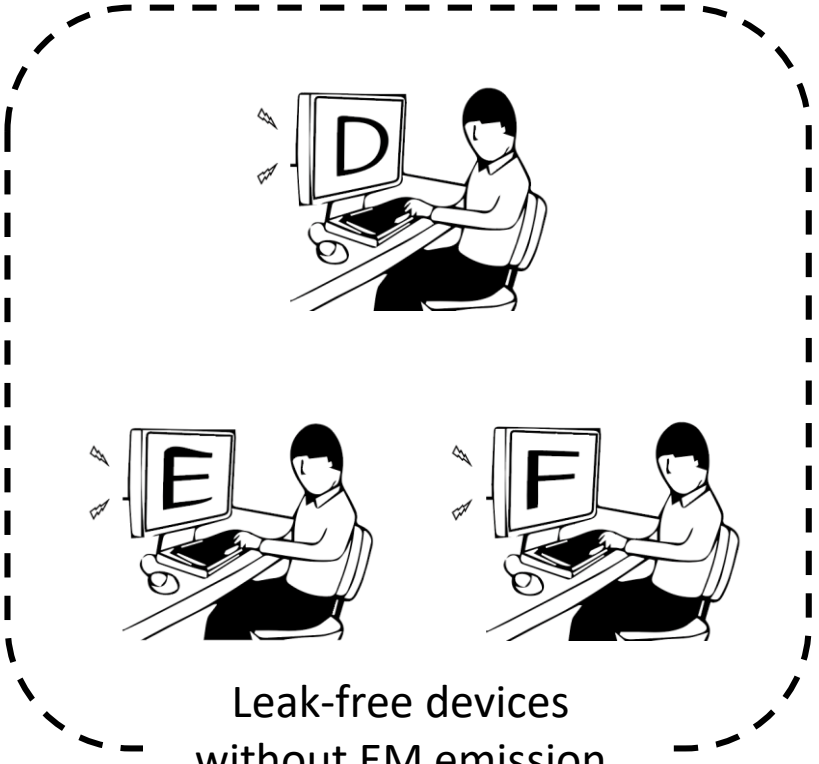
Keyboards

Touch screen devices

Is the EM attack feasible against every electrical device?



Devices with information leakage caused by unintentional EM emission



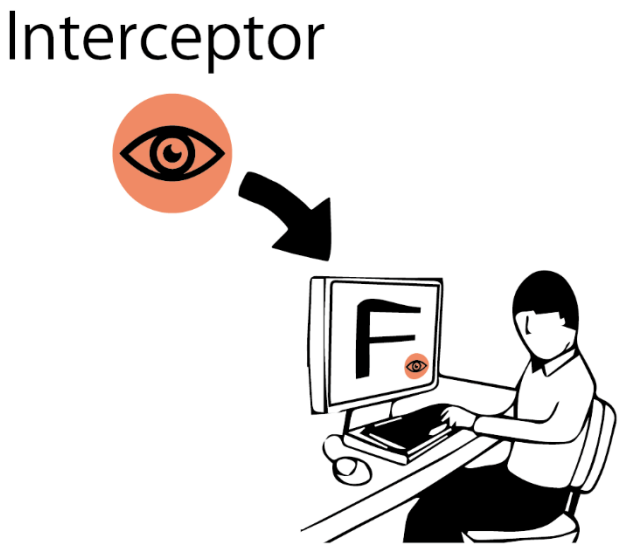
Leak-free devices without EM emission

In conventional attacks, attackers focused on devices with unintentional EM emission. So, devices without EM emission had been out of the scope of threats.

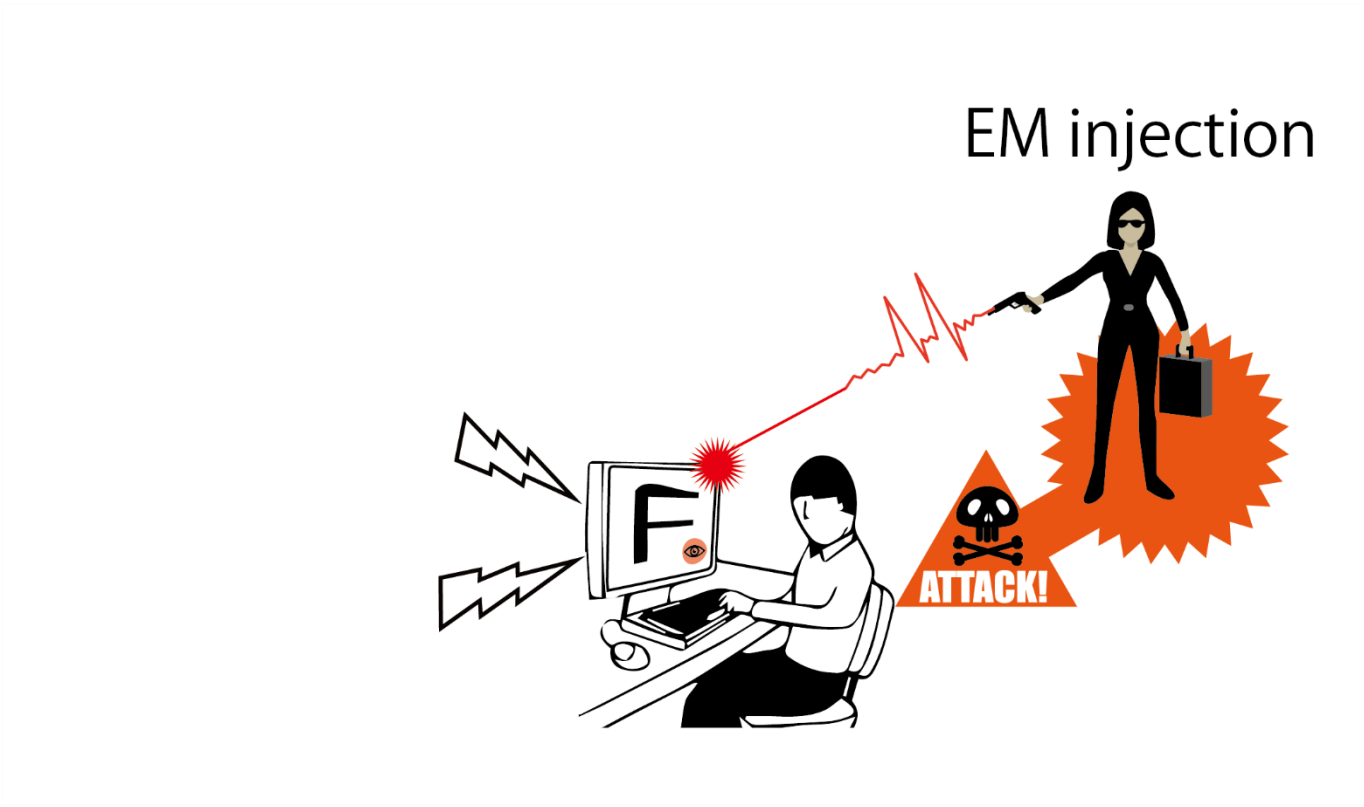
EM information extortion from electronic devices using interceptor

Threats against potentially leak-free devices

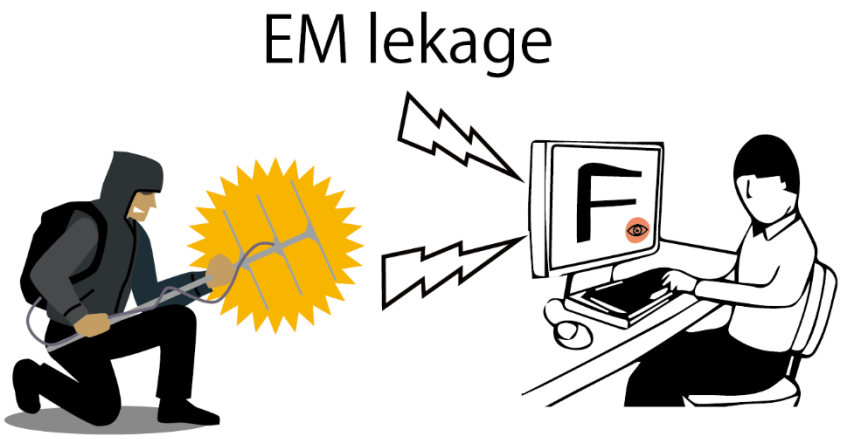
Threats against potentially leak-free devices



Threats against potentially leak-free devices



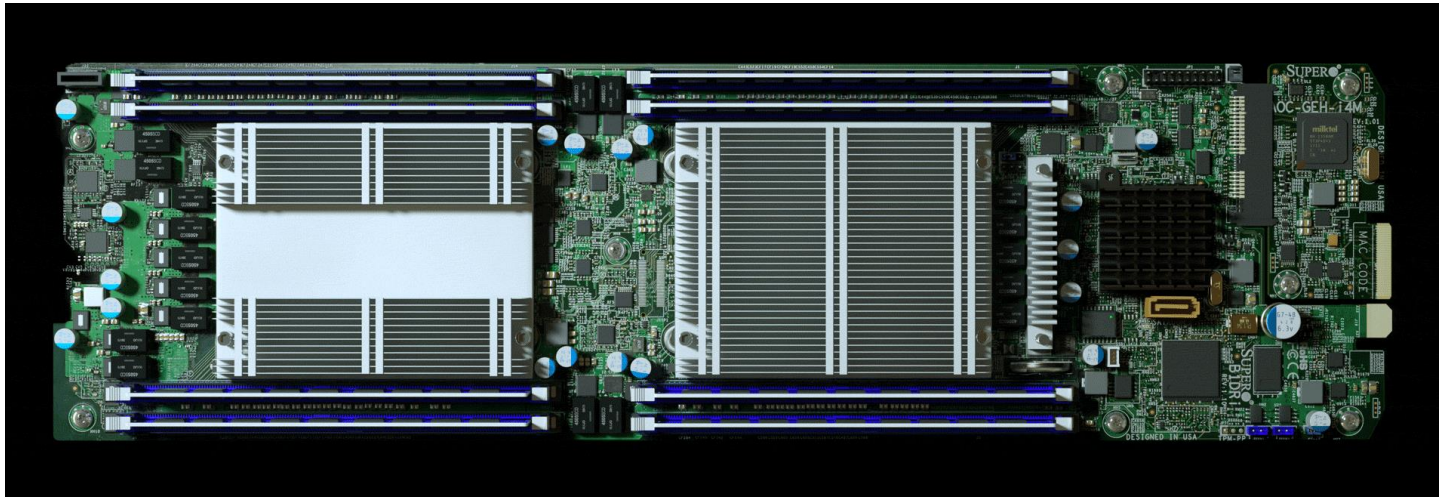
Threats against potentially leak-free devices

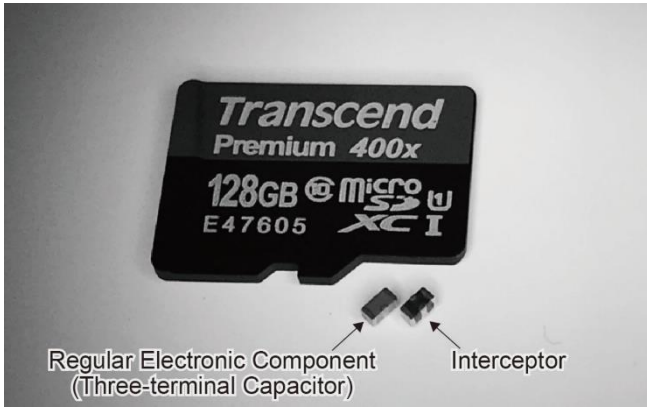


Using interceptor, active/passive attack, there is the possibility that information can be leaked from potentially leak-free devices.

Operation principle of interceptor installed on peripheral circuits of IC and transmission line

Concept of interceptor





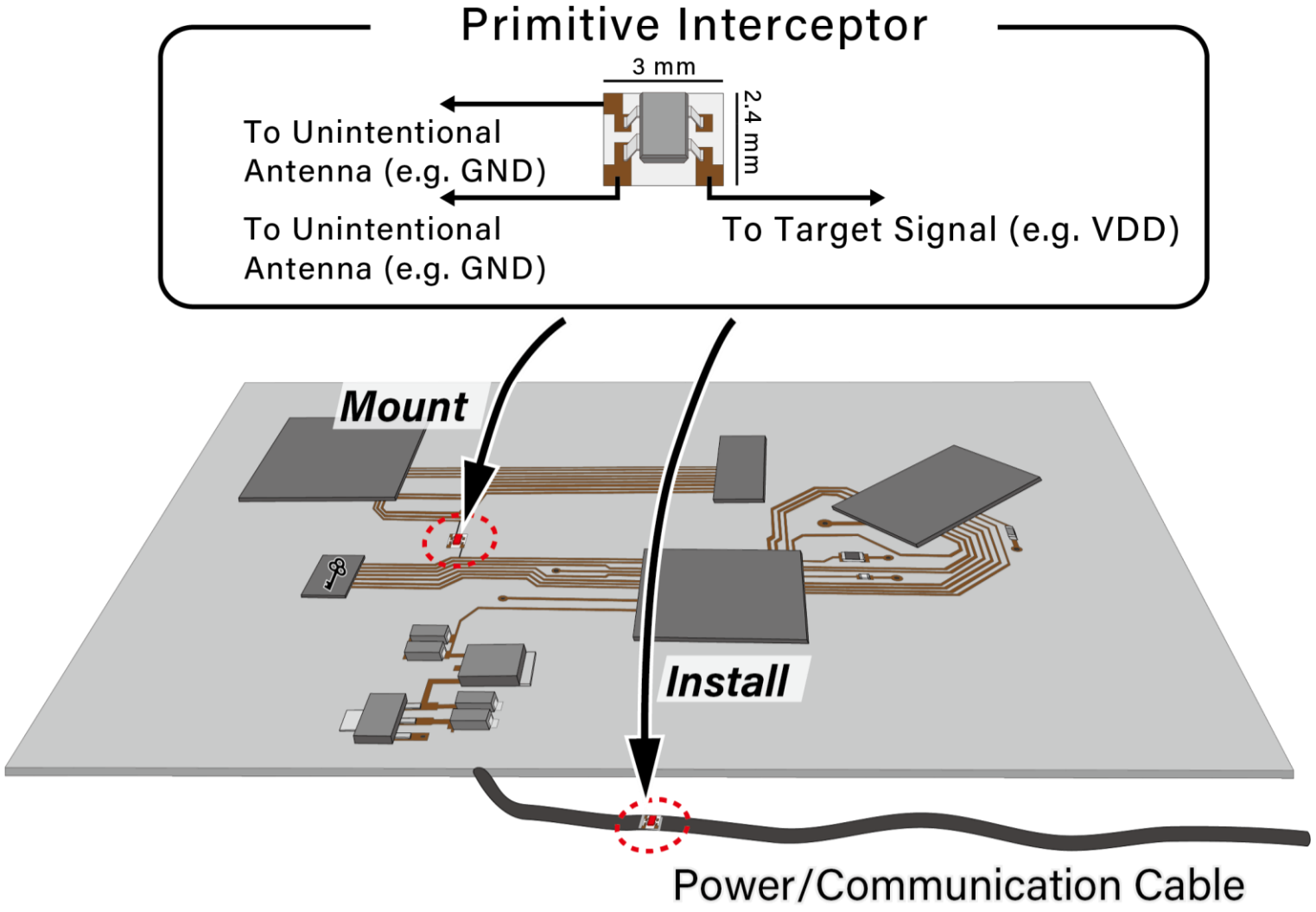
Interceptor

https://www.bloomberg.com/news/

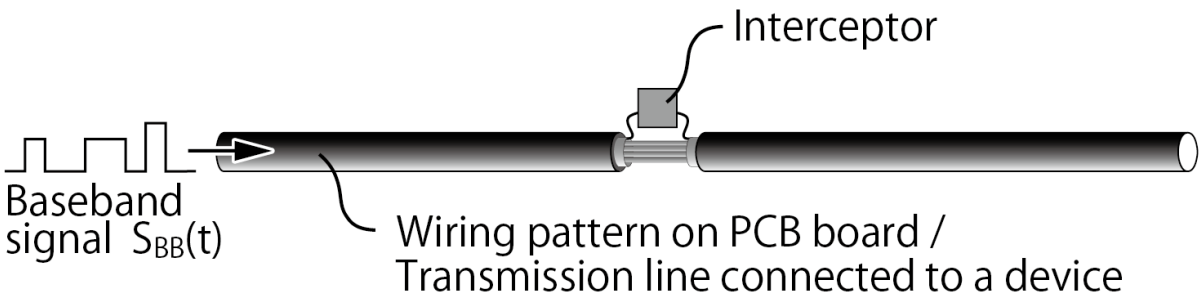
Function of interceptor

- The acquisition of information is made possible by **forcibly causing leakage** from devices
- **Leakage** is only measurable from a **distance during the irradiation** of EM waves from devices, and the **range of leakage** is adjustable by the **irradiation intensity**
- Interceptors cover both **analog** and **digital** signals
- Interceptors emanate information from **unintended antenna** structures
- Signals leaked by the **interceptor retain the original shape**, and this waveform can be measured (Conventional TEMPEST measures the differentiated shape of the original signal)

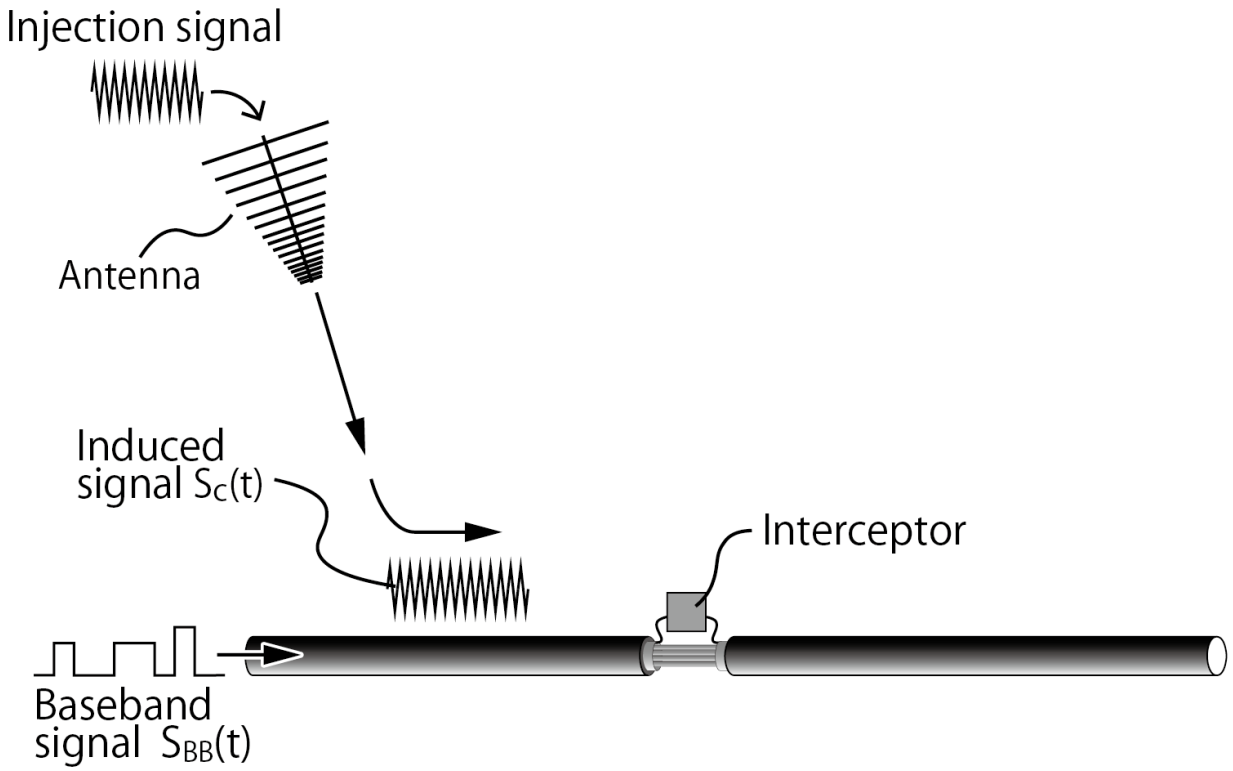
Installation of interceptor



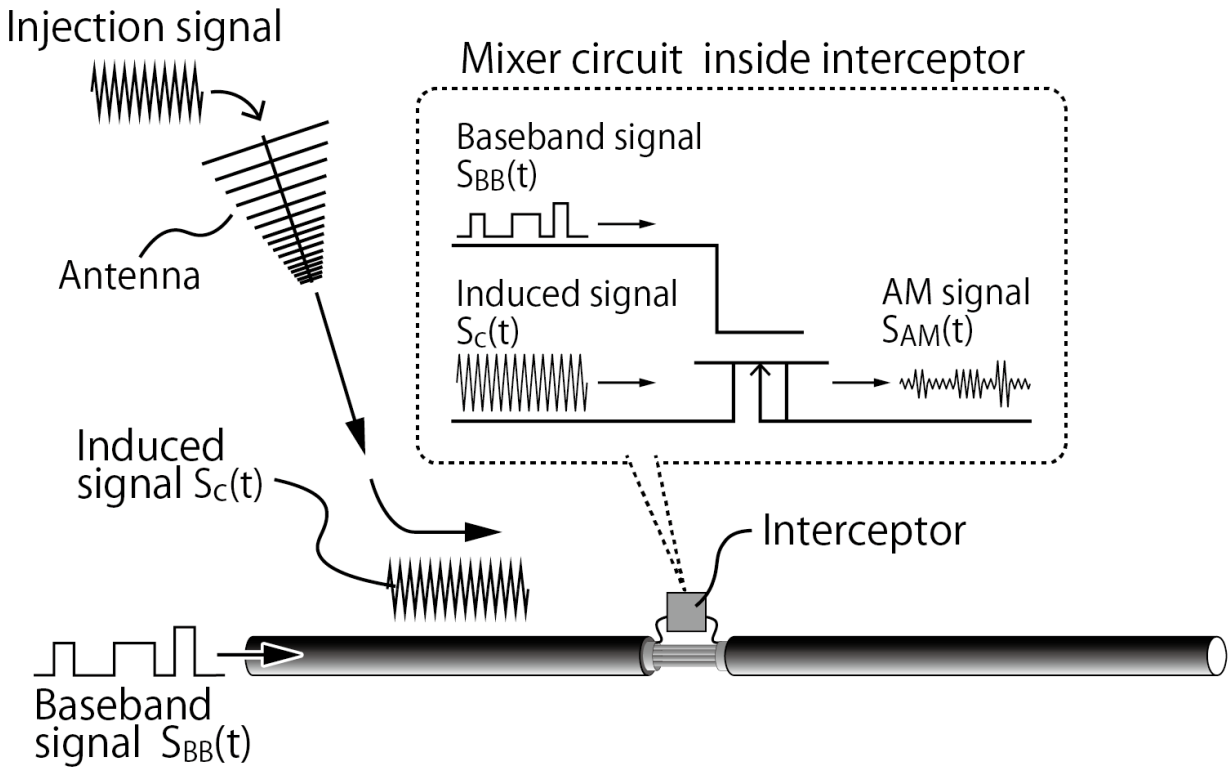
Information leakage caused by interceptor installed on peripheral circuits of IC and transmission line



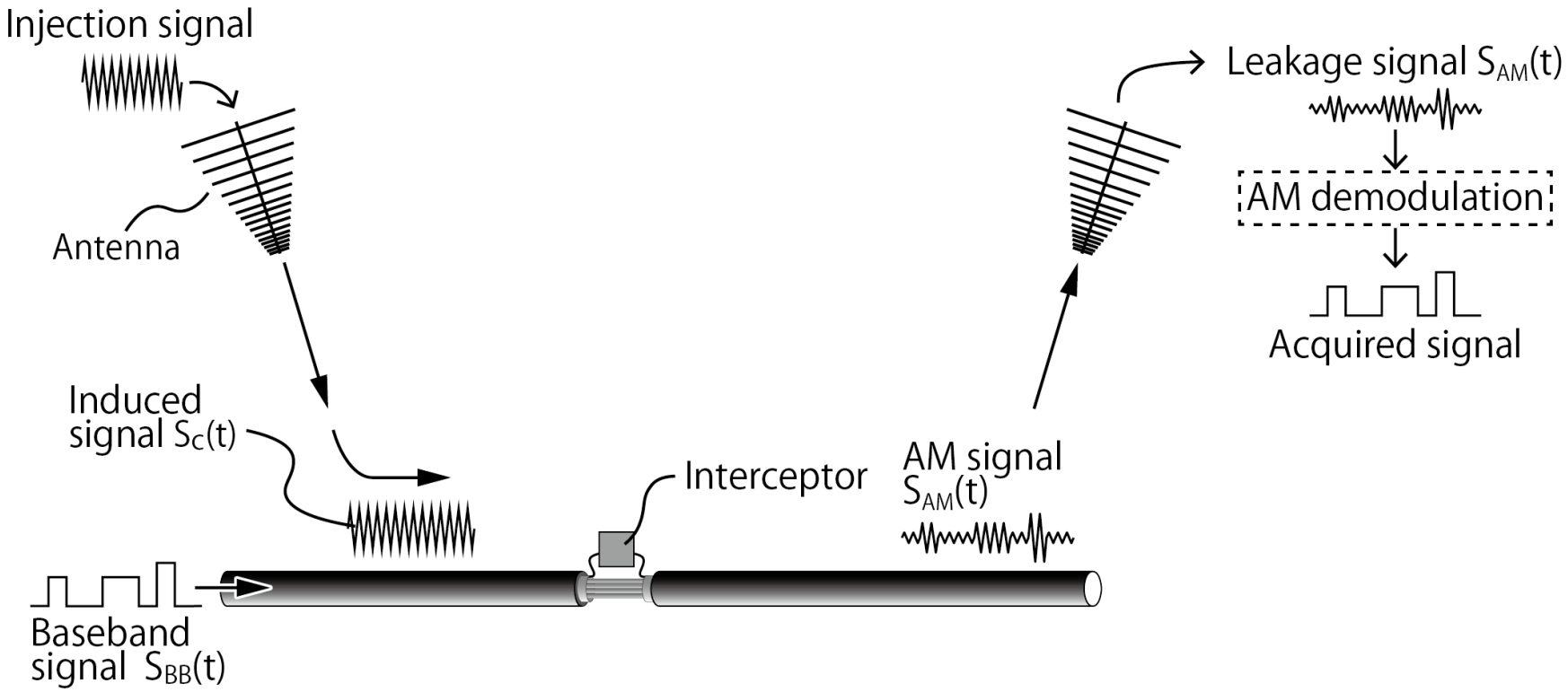
Information leakage caused by interceptor installed on peripheral circuits of IC and transmission line



Information leakage caused by interceptor installed on peripheral circuits of IC and transmission line

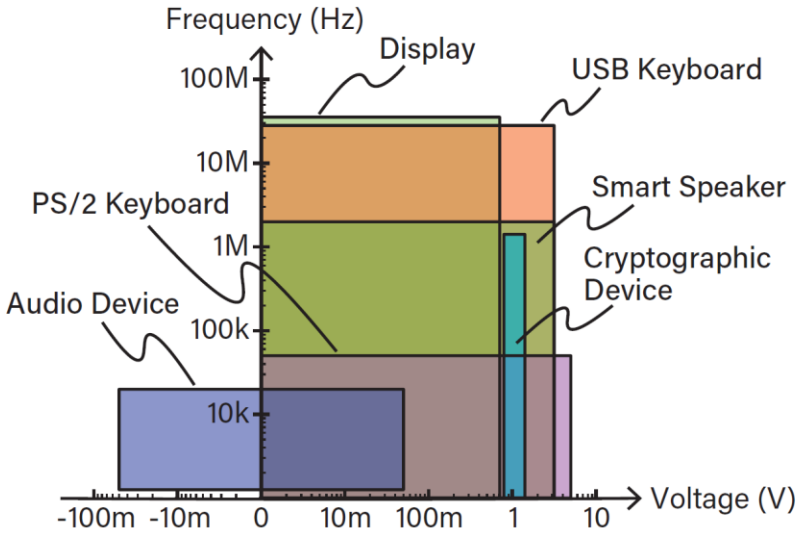


Information leakage caused by interceptor installed on peripheral circuits of IC and transmission line



Selection of MOSFETs matching the target signal

Target Device	Type	Voltage	Bandwidth
Keyboard (PS/2)	Digital	0～5.0 V	0～41.5 kHz
Keyboard (USB)	Digital	0～3.3 V	0～27.5 MHz
Display (VGA)	Analog	0～0.7 V	0～32.5 MHz
Audio Device (Headphone)	Analog	-50～50 mV	20 Hz～20 kHz
Cryptographic Device (RSA)	Analog	0.8～1.3 V	0～2.5 MHz
Smart Speaker	Digital	0～3.3 V	0～2 MHz

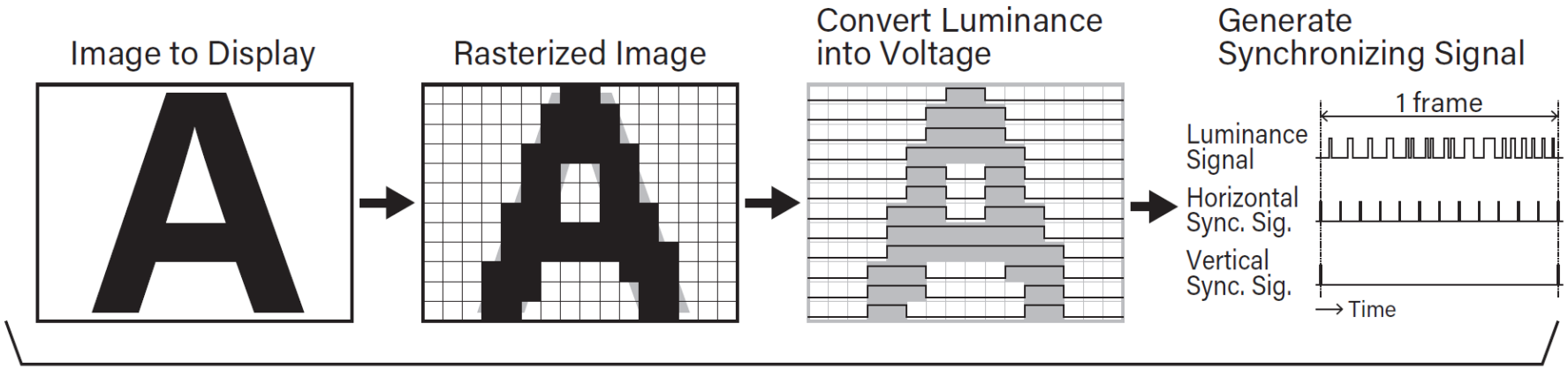


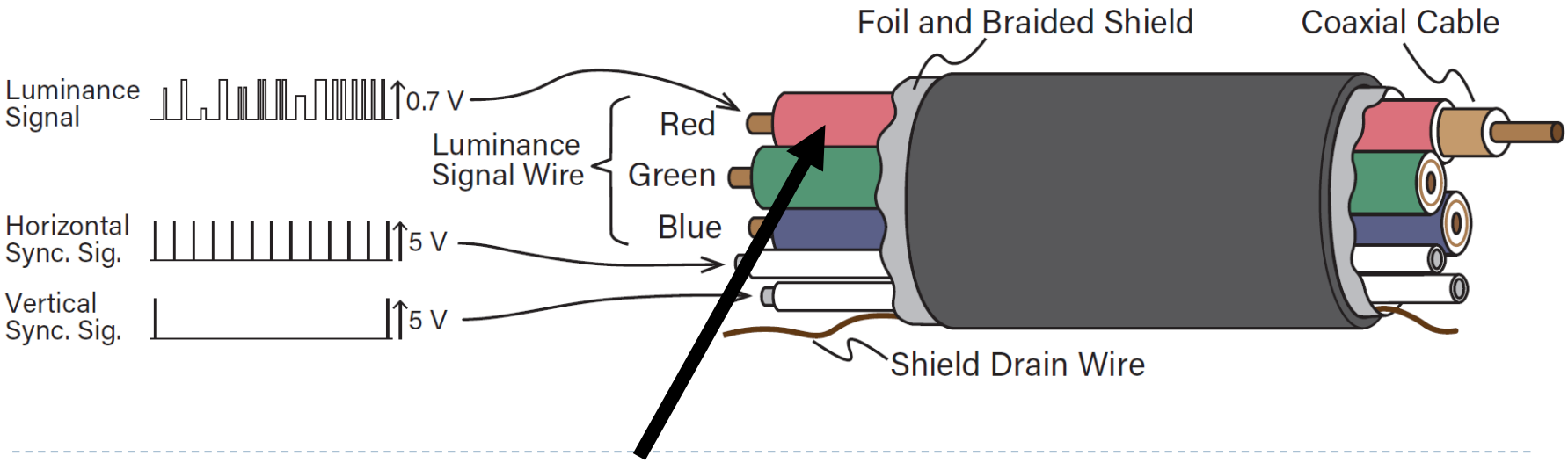
MOSFET is the core component of interceptor.

This selection can be determined by the **frequency** and **voltage** of the target signal.

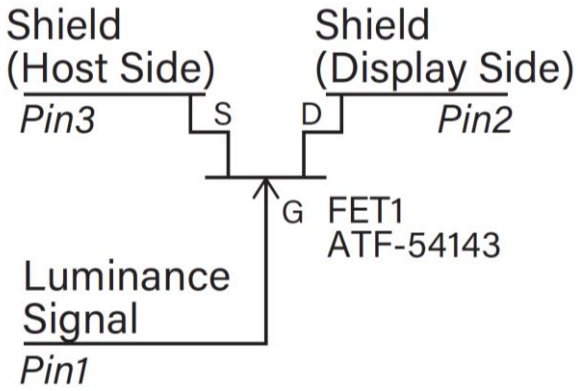
EM leakage from a display

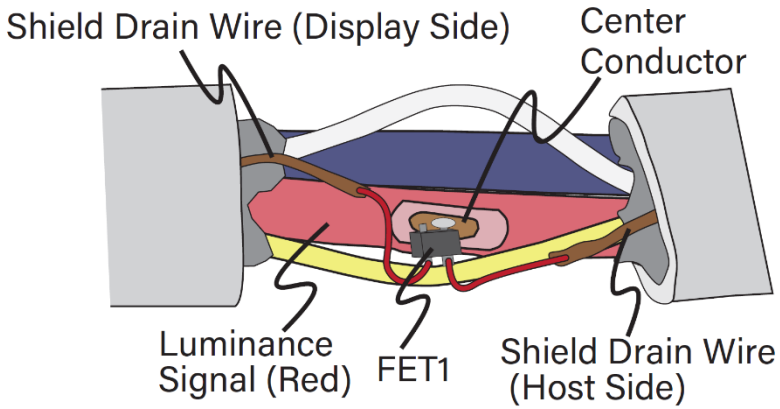
Target signal



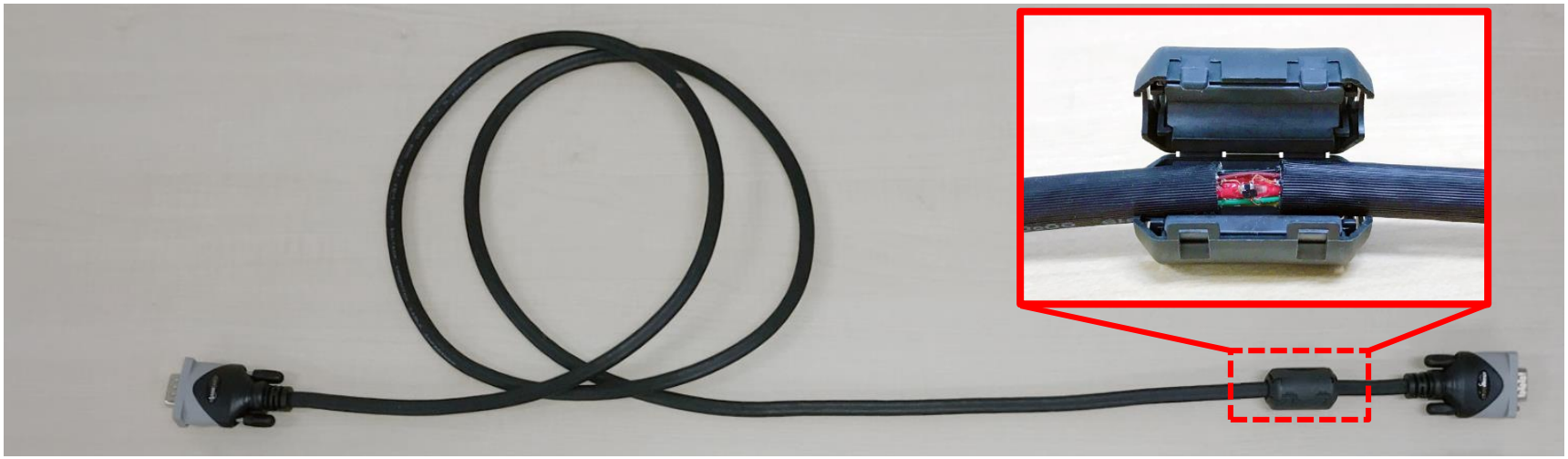


Installation of Interceptor





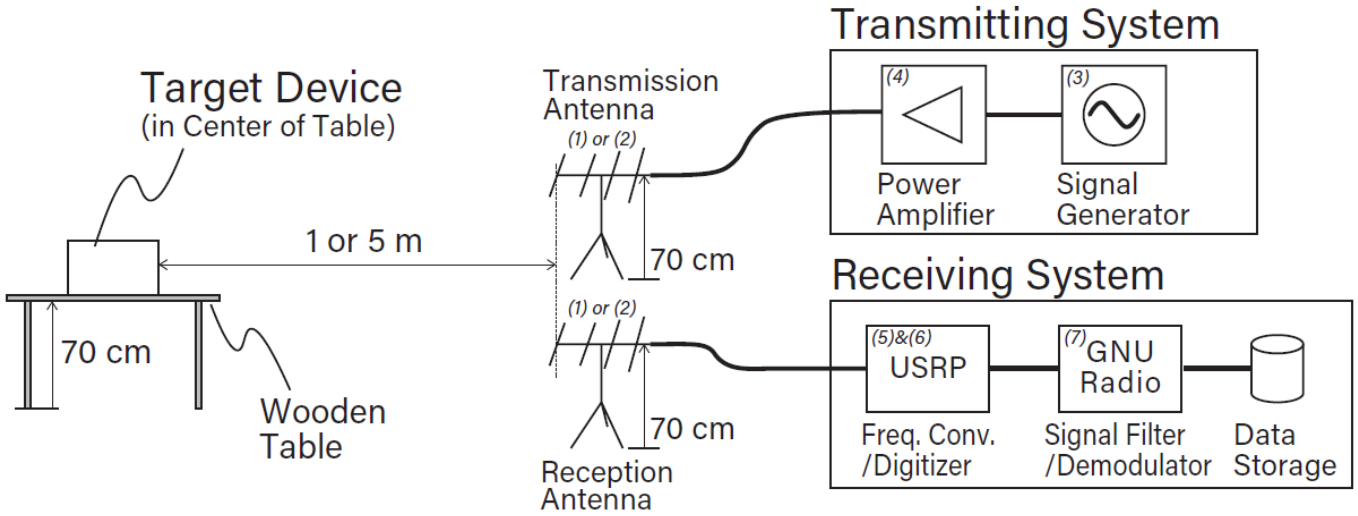
Circuit configuration of interceptor

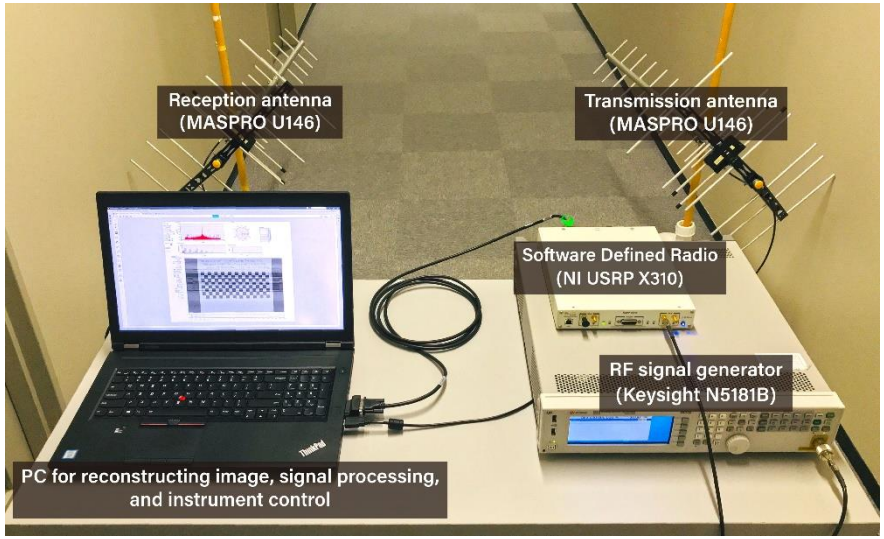


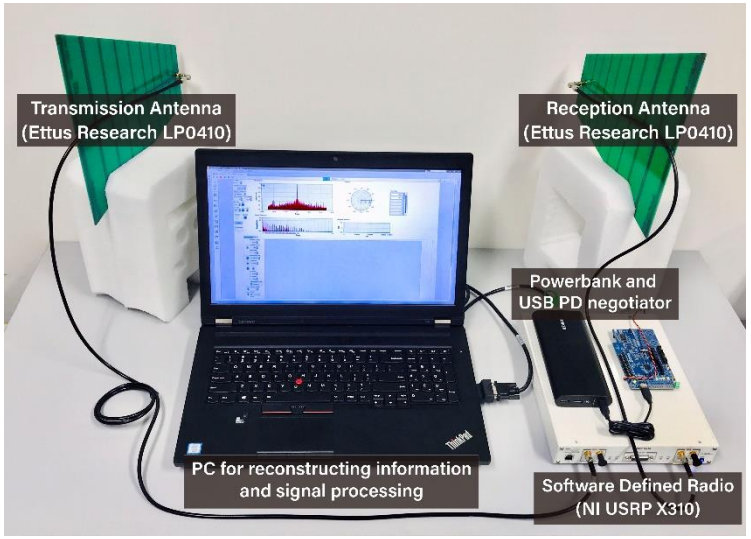
Demo

https://youtu.be/yFVdnhb28bo

Experimental system components and layout





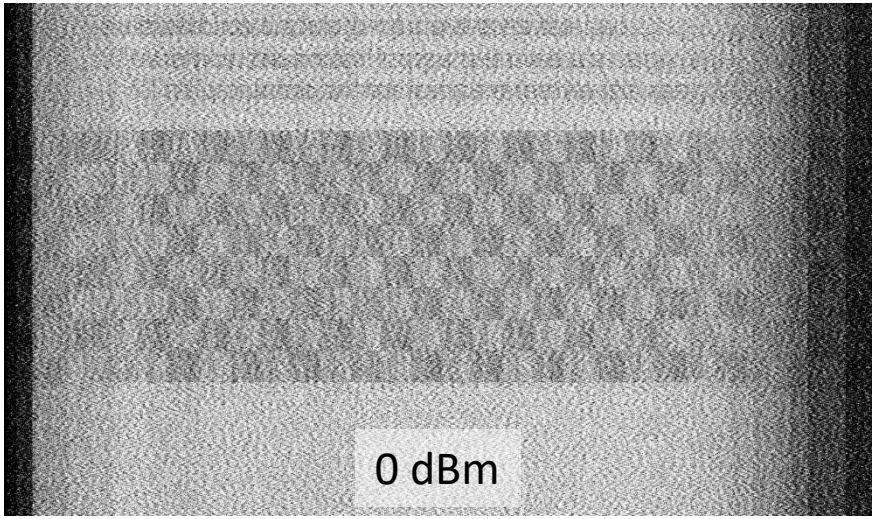


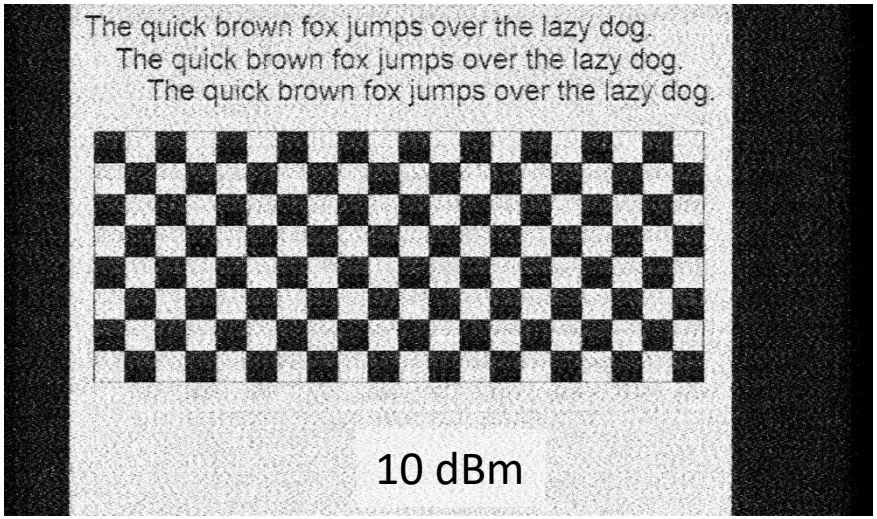
Stationary setup

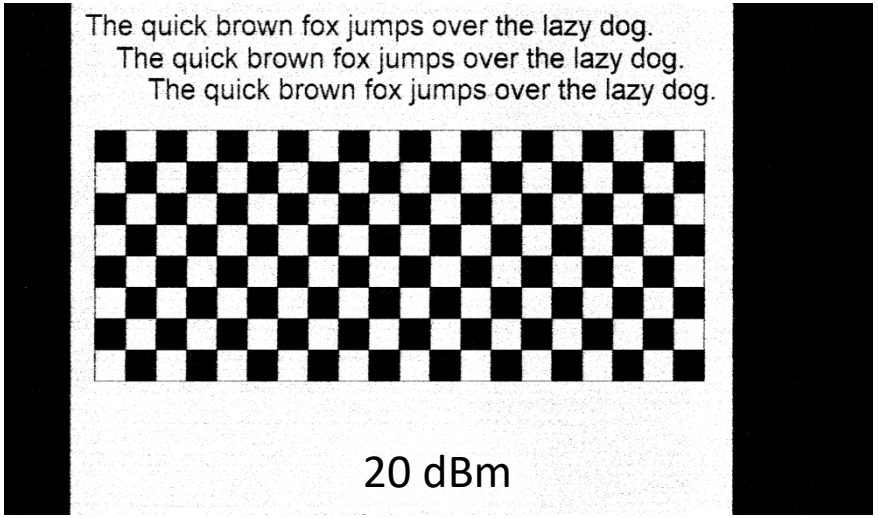
Portable setup

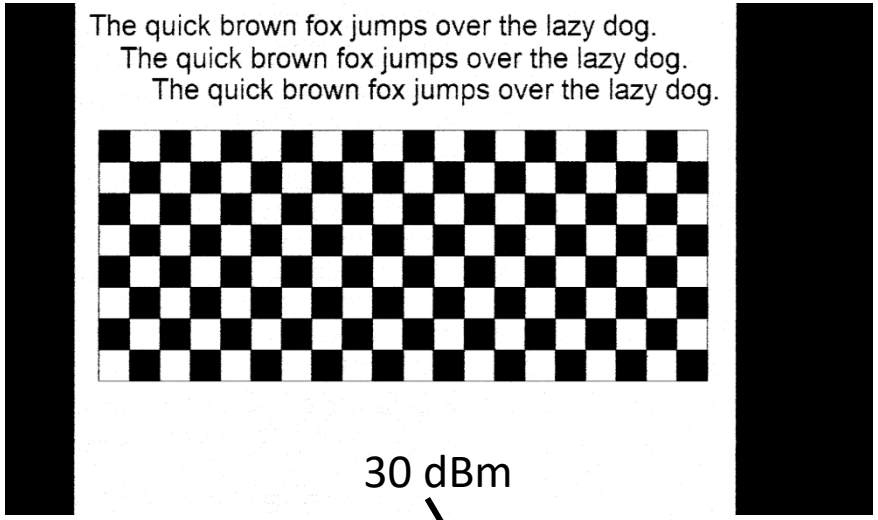
Demo

Leakage control by EM irradiation strength





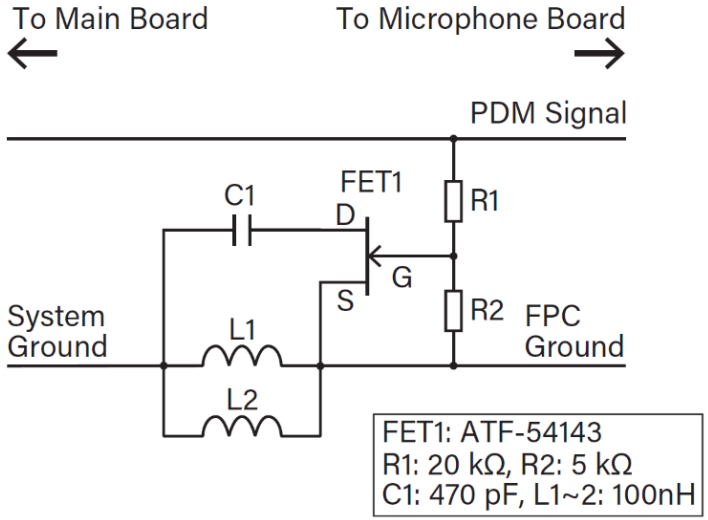


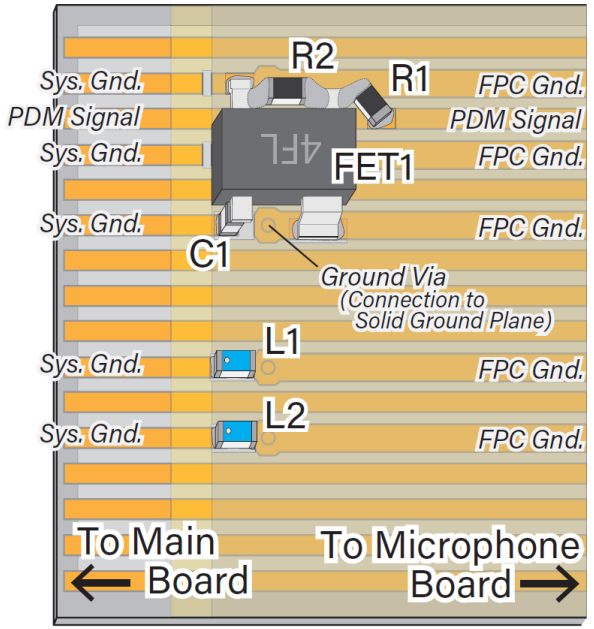


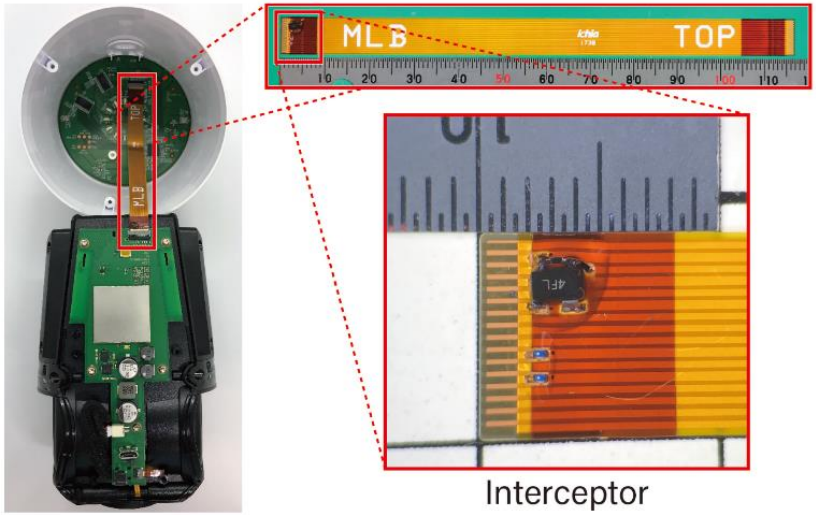
EM irradiation strength

EM leakage from a smart speaker

Interceptor installation against smart speaker





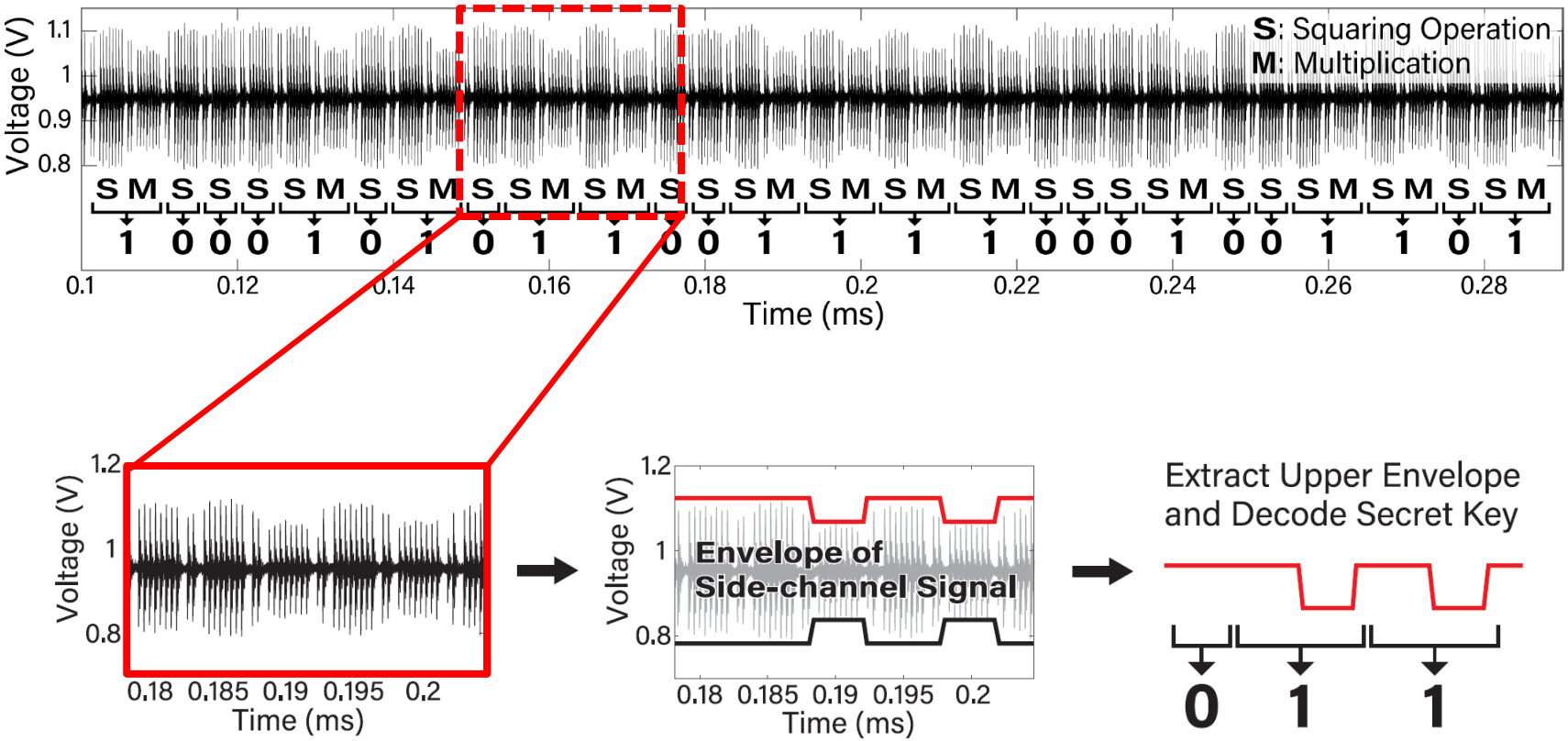


Smart speakers always pick up ambient sounds, so attacker can monitor the surrounding sounds of smart speakers by observing EM leakage.

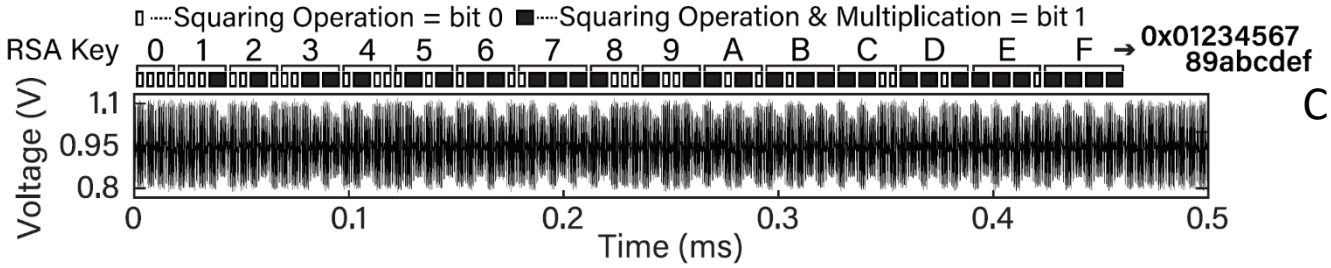
Demo

EM leakage from a cryptographic module

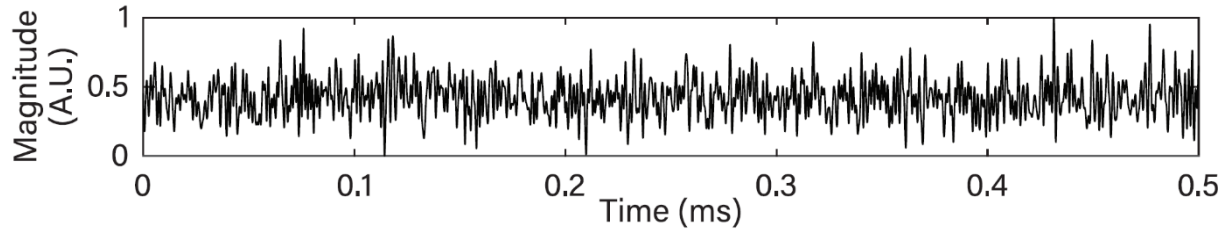
Interceptor installation against crypt module (RSA)



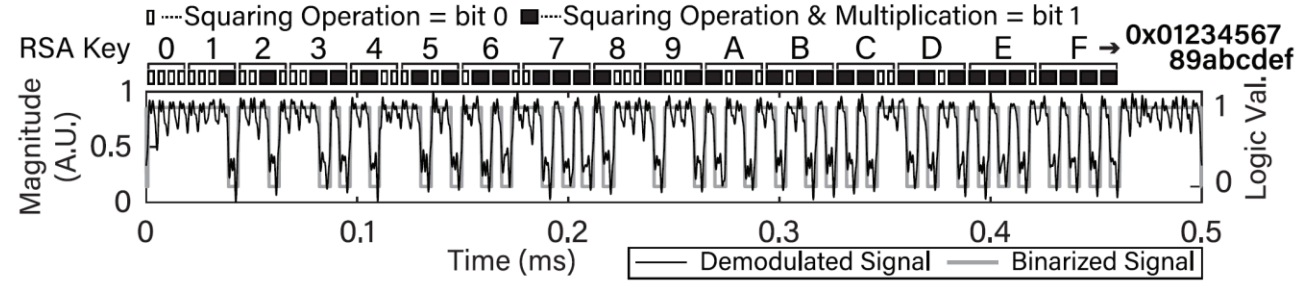
EM leakage signal from crypt module (RSA)



Change of internal signal at key input (original)



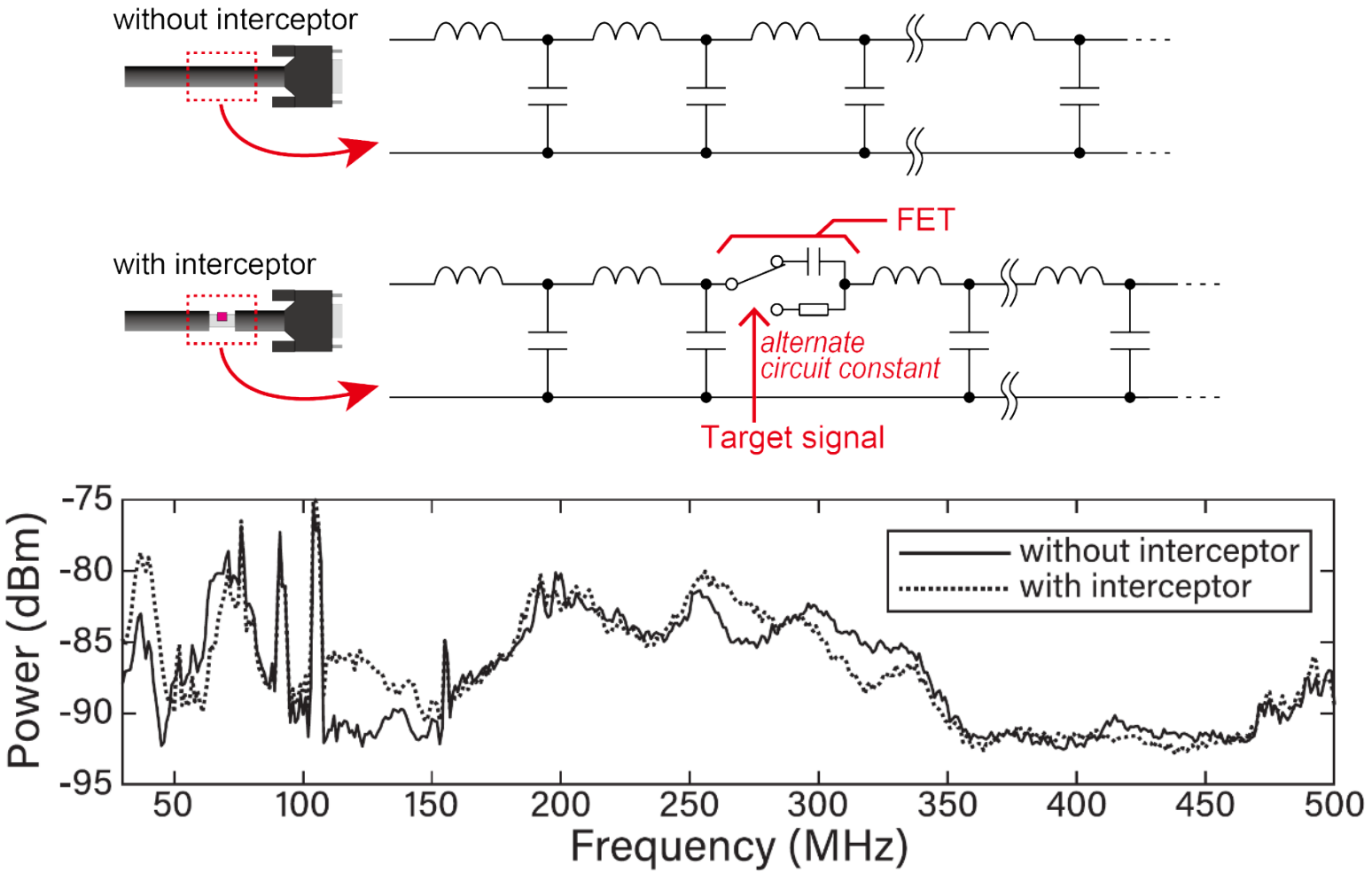
Observed leakage signal without EM injection



Observed leakage signal with EM injection (5 m)

Detection method of interceptor

Interceptor detection using passive sensing



Conclusion

Some devices have weak EM emission and potentially leak free. So, these devices have been excluded from this kind of threats in conventional EM attacks.

It was shown that interceptors can cause information leakage from potentially leak-free devices forcibly. It was also shown that the timing, distance, and intensity of leakage can be controlled by using interceptors.

In addition, we showed the interceptors have the potential to be detected by passive or active sensing methods.