Electromagnetic Information Extortion from Electronic Devices Using Interceptor and Its Countermeasure

Masahiro Kinugawa[1], Daisuke Fujimoto[2] and Yuichi Hayashi[2]

[1] National Institute of Technology (KOSEN), Sendai College, Japan,
kinugawa@sendai-nct.ac.jp

[2] Nara Institute of Science and Technology, Japan, {fujimoto,yu-ichi}@is.naist.jp

Abstract. The problem of information leakage through electromagnetic waves for various devices has been extensively discussed in literature. Conventionally, devices that are under such a threat suffer from potential electromagnetic information leakage during their operation. Further, the information inside the devices can be obtained by monitoring the electromagnetic waves leaking at the boundaries of the devices. The leakage of electromagnetic waves, however, was not observed for some devices, and such devices were not the target of the threat discussed above. In light of this circumstance, this paper discusses an "interceptor" that forces the leakage of information through electromagnetic waves, even from devices in which potential electromagnetic leakage does not occur. The proposed interceptor is a small circuit consisting of an affordable semiconductor chip and wiring and is powered by electromagnetic waves that irradiate from the outside of a device as its driving energy. The distance at which information is obtained is controlled by increasing the intensity of the irradiated electromagnetic waves. The paper presents the structure of the circuit for implementing the proposed interceptor to be used in major input–output devices and cryptographic modules, mounting a pathway designed on the basis of the construction method onto each device. Moreover, it is shown that it is possible to forcefully cause information leakage through electromagnetic waves. To detect the aforementioned threat, the paper also focuses on the changes in a device itself and the surrounding electromagnetic environment as a result of mounting an interceptor and considers a method of detecting an interceptor by both passive and active monitoring methods.

Keywords: Information Leakage · Electromagnetic Security · Cryptographic Device

1 Introduction

The performance of consumer measurement devices and the speeds of computational resources have improved, while memory device capacities have become larger in recent years, facilitating statistical analyses of data observed over a long period of time. These analyses demonstrated that, through the leakage of electromagnetic (EM) waves, information can be rapidly and easily extracted from devices without leaving any trace. Therefore, a wide range of data communication devices are under threat associated with the leakage of EM waves. Given this background, various information-containing and ubiquitous devices have been examined for the analysis and procurement of leakage signals via EM radiation, including cathode-ray tube (CRT) and liquid-crystal display (LCD) monitors [VE85, Kuh02, Kuh04, Kuh05, Kuh13, SS07, SS08, Sek10, SS13, TYF11, SJY14], touchscreen monitors [HHM+14], information printed by printers [TTY+06], key data input from keyboards

IACR Transactions on Cryptographic Hardware and Embedded Systems ISSN 2569-2925,
Vol. 2019, No. 4, pp. 62–90
DOI:10.13154/tches.v2019.i4.62-90

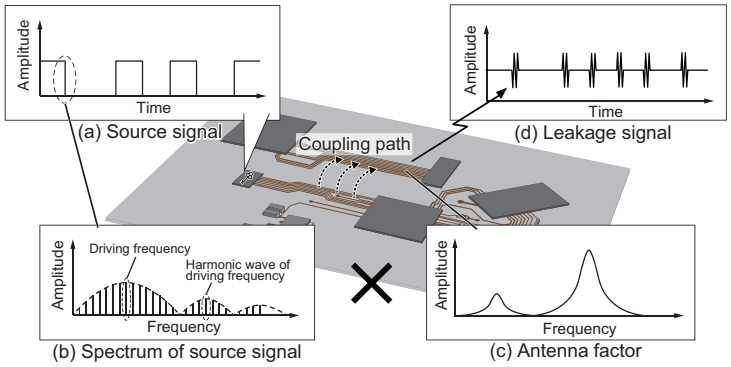


Figure 1: Electromagnetic radiation model of electronic devices

[VP09, VP10], arithmetic information in central processing units (CPUs) [ZP14, PZCW16], and secret keys in cryptographic modules [AARR02, CPM+18]. These threats are called TEMPEST/EM side-channel attacks.

EM radiation that is unintentionally generated from electronic devices has been considered in the field of EM engineering, and the mechanism of radiation can be explained by the EM radiation model shown in Figure 1 [Pau06].

The target signals to be obtained by an attacker (e.g., the drawing signals on a display, the scan signals on a keyboard, and the side channels generated during cryptographic processing) vary with time in a manner similar to the source signal shown in Figure 1. The rising and falling edges of signals include broadband signals such as the spectrum of the source signal in Figure 1. EM waves are efficiently radiated when the frequency components and the antenna characteristics composed of the physical structure of the circuit board and wiring pattern (Figure 1, antenna factor) match.

Generally, many device designers tend to design circuits assuming that signals are transmitted only along the wiring. However, in actual devices, the high-frequency components, included in the rising and falling edges of signals, are successively transmitted above the wiring owing to the coupling of the capacity and the induction in the wires. Therefore, an unpredictable structure behaves as an antenna, and EM radiation occurs. When the classified information inside the device is included in such radiation, information leakage occurs through EM waves.

However, if there exist no coupling paths or unexpected antenna structures in the device, the EM waves that contain information do not propagate until the attacker, who is at a distance. Therefore, not all devices leak information by EM waves unless critical paths or unexpected antenna structures which increase possibilities of information leakage are formed inside the devices. For these devices, it is difficult to obtain information from leaked EM waves, and TEMPEST studies only looked at devices that experience potential leakage.

Our contribution. In light of the above, an interceptor that forces information leakage from targeted devices by EM waves is proposed in this paper. The interceptor expands the range of target devices from devices that exhibit potential leakage to those that do not. We develop an interceptor based on a concept similar to that of a miniature circuit built by an inexpensive circuit element and simple wiring without a special antenna structure. The interceptor is mounted onto electronic devices.

The proposed interceptor operates only by using the EM waves of a particular frequency irradiated from the outside the device as the driving energy. Using the irradiated frequency as a carrier, the confidential information inside a device is modulated and forcibly leaked outside the device. In addition, the distance at which EM waves containing information are transmitted can be controlled by changing the irradiation intensity. Information

can thus be obtained from a standalone system that does not possess a communication line. Furthermore, the proposed interceptor leaks the waveforms of the information signals without any change in comparison with the differentiated waveform of conventional TEMPEST.

In addition, this paper explains the operation principles of the developed interceptor, and on the basis of these principles, discusses the features of the devices to which the interceptor can be applied. As specific examples, the interceptor is mounted onto input devices and cryptographic modules where highly sensitive information is exchanged, and we show how information is leaked. A detection method for verifying whether the interceptor is mounted onto a device in secrecy is also discussed.

The contributions of this paper are as follows:

- The acquisition of information is made possible by forcibly causing leakage from devices (as in essence the leakage is there in the device already, it is just not radiated out).
- 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 (in conventional TEMPEST, the range from which an attack can be performed was determined by the intensity of the EM waves radiating from devices).
- The proposed interceptor covers both analog and digital signals and leaks information outside devices by using a physical structure inside the devices, such as the antenna.
- The proposed interceptor does not require a special antenna to leak information until a certain distance. Interceptors emanate information from unintended antenna structures (e.g., the transmission lines inside the device, the cables connected to the device, etc.).
- Conventional TEMPEST measures the differentiated shape of the original signal. However, the signal leaked by the interceptor retains the original shape, and this waveform can be measured.

Related work. Although a circuit with a concept similar to that of the interceptor proposed in this study also appears in the NSA ANT catalog [Wik], actual examples are provided in the NSA Playset, which contains a radio frequency (RF) retroreflector [Oss14][Oss15], and a Green Bay Professional Packet Radio (GBPPR) project [Proa][Prob][Proc]. Their structure is similar to RF identification (RFID)[Leh12], which requires a special external antenna to communicate with outside devices. Thus, the implementation targets of these circuits are limited to certain devices, and their applications are very limited compared with those of the interceptor proposed in this study. In addition, if a special antenna is shielded with device housing made from metal as a conventional EM compatibility (EMC) countermeasure, these circuits might not work. Moreover, if an interceptor with an external antenna is implemented on a communication cable, it can be easily detected visually. In contrast, if an unintended antenna is employed, the above problem will not occur.

The possibility of an active attack using intentional EM interference is pointed out in [KA98][And08]. The concept of a TEMPEST virus shown in [And08], which modifies target devices, steals secret information, and transmits it to an outside device, is similar to an interceptor. However, the feasibility, detailed mechanisms, and examples are not shown in previous studies.

Furthermore, in an irradiation attack, the transmission power increases as the attack distance increases. As a result of the increased power, the carrier signal directly propagates from the transmit antenna (Tx) to the receive antenna (Rx). In this circumstance, the modulation index of the received wave decreases. This is a problem that occurs with or

without an external antenna. Therefore, in conventional studies, only demonstrations at short distances (less than 1 m) have been shown. In contrast, in this research, the array of antennas used for the attack is optimized, and the carrier signal is directly suppressed from the transmit antenna to the receive antenna [ESS14]. Specifically, the antenna array employs directional antennas that have null directions, for which antenna gain is a local minima. In the attack experiments, we arranged the null direction of the transmission and reception antennas to face each other. This arrangement electrically decouples both antennas. Therefore, our attack works over distances of several meters or greater.

Structure of this paper. This paper is structured as follows. Section 2 explains the features and principles of the interceptor developed in this study as well as the approach to selecting a field effect transistor (FET) with respect to the installation target. Section 3 discusses devices that exchange highly sensitive information that have been the targets of conventional TEMPEST and EM side-channel attacks. Further, this section shows that information leakage can be forced by installing the interceptor onto devices for which it is difficult to obtain information through conventional means. Section 4 discusses methods that can be used to detect whether an interceptor is attached to a device. Section 5 concludes this paper.

2 Features of the interceptor and leakage mechanism

2.1 Scenarios in which an interceptor is installed on a device

The interceptor proposed in this paper assumes installation or placement on the printed circuit board (PCB) of a target device or on a communication cable.

Another threat that assumes a similar scenario is a hardware trojan (HT) in which a malicious circuit is implemented in a system, but the targets for HTs were mainly limited to implementations inside integrated circuits (ICs) [CY10, WTP08, GM11, RWTP08, CLK11]. In contrast, the proposed interceptor consists of affordable (a few dollars) electronic components, and the degree of freedom with respect to its implementation is improved. This is because it can be implemented outside an IC owing to its ability to be easily implemented onto the circuit boards and wiring that constitute the device as well as the transmission lines for the interconnecting devices. For example, this interceptor can be easily connected to the motherboard that constitutes an information device in a similar manner to the "tiny microchip" discussed in the Bloomberg article titled "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" from early October of 2018 [Blo18]. If the targeted signals are transmitted to the outside of a device through a communication line, then such a path of communication could be appropriate for the implementation of the circuit.

Considering that the proposed interceptor consists of a small-scale circuit, the device may be implemented on circuit boards and transmission lines as a regular component during the manufacturing process by disguising it as a regular electronic component such as the capacitors and inductors that are implemented in the device (Figure 2, Figure 3). In general, information communication devices undergo EMC testing related to EM radiation (e.g. CISPR (Comité International Spécial des Perturbations Radioélectriques) 22) and immunity to EM disturbance (e.g. CISPR 16) before shipping. However, because the proposed interceptor requires to irradiate it and to measure its emission simultaneously, the interceptor may pass conventional EMC tests, which individually evaluate radiation and disturbance. Moreover, because the structure of the interceptor is simple, it can be inserted if the attacker can access the target device for a short duration after EMC testing.

The proposed interceptor has limited functionality unlike HTs that are traditionally implemented inside an IC. An HT implemented inside an IC can perform various functions such as the modification of functionality, the modification of specifications, the leakage of

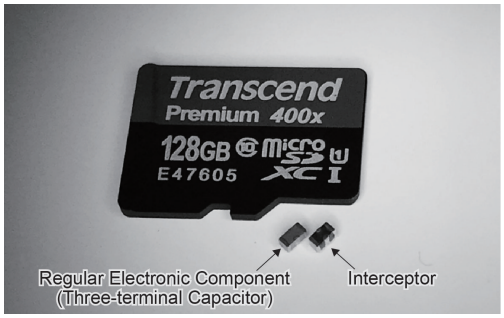


Figure 2: Interceptor disguised as a regular electronic component

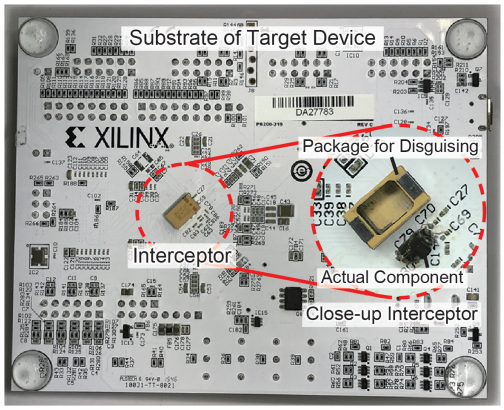


Figure 3: Interceptor implemented on a substrate by disguising it as a regular component

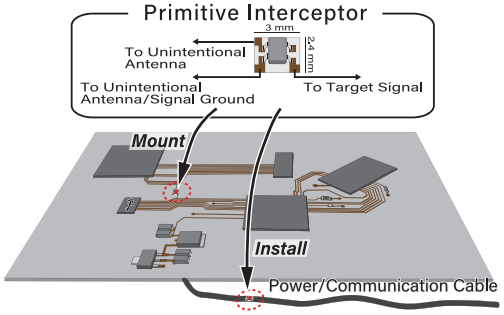


Figure 4: Conceptual diagram of the interceptor

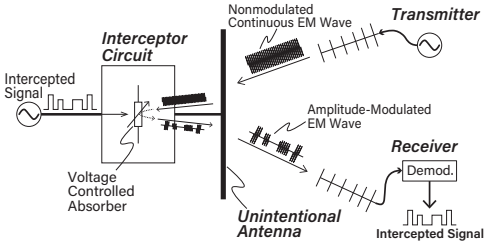


Figure 5: Principle of information leakage caused by the interceptor

information, and denial of service [TK10], but the function of the proposed interceptor is limited to the leakage of information.

2.2 Structure of an interceptor and the principles of leakage

This section discusses the circuit composition of an interceptor and its operating principles.

Figure 4 shows a conceptual diagram of the interceptor used in this study. The circuit consists of a single FET and short wiring and uses a line connected to a wiring pattern on the circuit board and to devices such as antennas (referred to as unintentional antennas henceforth). By mounting such a circuit on the targeted device, the information inside the device is leaked to the outside through EM waves. From conventional studies [Pau06, HHM+12b], the signals transmitted over a line connected to the wiring pattern and the devices on a circuit board are known to leak over the entire circuit board and connecting lines through the connection of the transmitting line with the other lines and the board itself. The interceptor can be operated by mounting it at a location where the leaked signals can be measured and unintentional antenna structures are adjacent.

Next, the principle of information leakage caused by the interceptor is explained. As shown in Figure 5, an interceptor consists of an unintentional antenna, a reflective and absorbing element with a high-frequency power, and intercepting wiring for the targeted signals. The EM waves that irradiate a device from the outside cause the unintentional antenna to have a high-frequency power. If the reflective and absorbing element with a

high-frequency power is not connected to the unintentional antenna, a reflected wave is generated depending on the magnitude of the high-frequency power. This wave is the same as the reflected wave generated when EM waves irradiate the conductor. However, when there is an element that reflects, absorbs, and changes the strength of the generated high-frequency power of the unintentional antenna, its reflected wave corresponds to the amount of power reflected by the reflective and absorbing element. Moreover, instead of an irradiated EM wave, a conductive wave can be induced from the power/communication line. In this case, the loss of the EM wave is low; therefore, it might reach targets even if there is a structure that decreases its strength over air, such as a shield.

In the proposed interceptor, a reflective and absorbing element with a high-frequency power that can be controlled by a voltage is achieved by using a FET. Additionally, by using information bearing signals from inside the device as the control voltage for the interceptor, a reflected wave where the intensity is modulated by that information bearing signal, i.e. an amplitude-modulating (AM) signal, is generated.

The specific principles of an interceptor are shown by the operation of a mixer circuit in which two signals are multiplied. A mixer circuit multiplies an intercepted signal $s_{BB}(t)$ and a high-frequency signal $s_C(t)$ induced by externally irradiated EM waves and generates an amplitude-modulated signal $s_{AM}(t) = s_{BB}(t)s_C(t)$, where $s_C(t)$ is the carrier signal and $s_{BB}(t)$ is the baseband signal. The time-varying signal $s_{BB}(t)$ is radiated outside the device as the amplitude-modulated signal $s_{AM}(t)$ through an unintentional antenna. The interceptor used in this study can be seen as a passive mixer circuit composed of a single FET.

Next, the amplitude-modulated reflected wave $s_{AM}(t)$ is received at the frequency at which this wave irradiates the device. By treating this frequency as a carrier and demodulating it, the intercepted signal $s_{BB}(t)$ can be obtained. This operation can be thought of as an attack that obtains information by combining an active attack [MOP07] and a passive [JT12] attack.

Since the strength of the carrier signal $s_C(t)$ is proportional to the intensity of the EM waves irradiating from the outside of the device, the intensity of the EM waves $s_{AM}(t)$ for leaking the intercepted information can be controlled by the irradiation intensity. In other words, the interceptor in this study can control the intensity of the radiation from the target devices, enabling intentional control of the monitoring distance [KH18], which was previously impossible for attackers with TEMPEST. This fact indicates that the attack distance can be extended by strengthening the irradiation intensity within the operating range of the FET.

For an extended attack range or an environment with a great degree of propagation attenuation, the strength of $s_{AM}(t)$ must be raised further. To do so, a resonant frequency at which the reception efficiency of the unintentional antenna is maximized is utilized. Treating $max(|s_C(t)|)$ as the maximum, the strength $s_{AM}(t)$ of the EM waves that leak information from the inside of devices can be maximized. The resonant frequencies of the unintended antenna are determined depending on the physical structure [Pau06][Mar92]. Among the physical structures, we focused on the resonant frequency determined by the dimensions of the circuit board and the length of the line attached to devices [HHM+12a]. The irradiation and monitoring of these EM waves can be conducted from the antenna through space, a current probe via a power line connected to the device, or a combination of these approaches.

2.3 Selection of a FET to match targeted information

Although it is possible to forcefully cause leakage from electronic devices through EM waves by the concept discussed above, an appropriate FET needs to be selected for the targeted device. The following are notable for the selection of the FET:

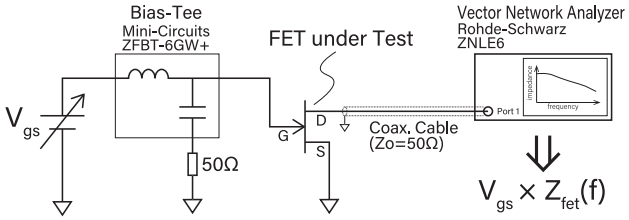


Figure 6: Impedance measurement system for the FETs of the interceptors

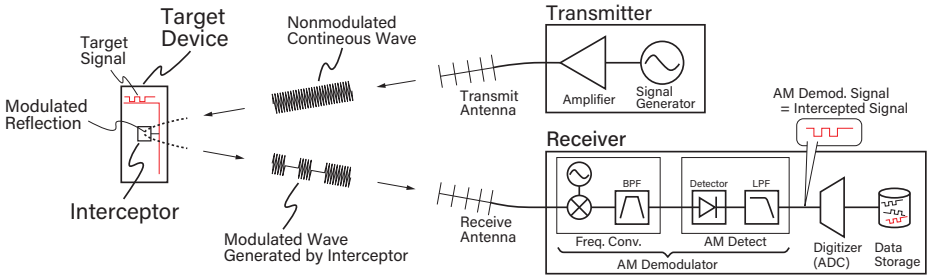


Figure 7: Transmission-and-reception system for the interceptor

- The range of voltage for the target signals
- The range of the gate–source voltage over which the drain–source impedance of the FET changes

In the next section, the conditions that each point should satisfy are discussed, and an approach for selecting the FET that constitutes an interceptor is provided.

2.3.1 Relationship that the FET impedance and the voltage of the target signal should satisfy

This section presents the selection criteria for the FET that generates the optimal amplitude-modulated signals for the interception of information by deriving the conditions for the impedance.

To design an interceptor suitable for the target signals, the drain–source impedance Z_{fet} of the FET used in the interceptor circuit needs to be variable within the voltage range of the target signals. A threshold voltage or pinch-off voltage exists in a FET as a voltage V_{gs} is applied between the gate and the source to initiate a change in Z_{fet}. This voltage is noted on the FET data sheet, but it cannot be applied to the interceptor circuit, in which a direct current (DC) potential difference does not exist between the drain and the source. Therefore, the change in the drain–source impedance as a function of the gate–source voltage needs to be measured per FET, and an appropriate FET needs to be selected.

The FET impedance Z_{fet} can be measured by using the measurement system shown in Figure 6. By varying V_{gs} and measuring Z_{fet} with a network analyzer, a graph of V_{gs} versus Z_{fet} can be obtained. The values of V_{gs} at which Z_{fet} changes need to be read from the graph, and the FET suitable for the target needs to be selected accordingly.

2.4 Driving the interceptor and the reception method for leaked signals

This section discusses the driving method of the interceptor, whose structure and principles were discussed in Section 2.2 as well as the method of obtaining leaked signals.

Driving the interceptor requires the irradiation of EM waves from outside of the device on which the interceptor is installed. The interceptor uses the EM waves to drive itself and as a carrier of modulated waves that cause information to leak to the outside by generating amplitude-modulated signals and radiating the intercepted signals. Figure 7 shows the transmission-and-reception system that radiates EM waves and receives and demodulates amplitude-modulated signals.

The transmission-and-reception system consists of a transmission system and reception system. The transmission system sends continuous sine waves as EM waves. Signals are amplified until they reach a value that can supply the power needed to drive the FET and irradiate EM waves to the devices on which an interceptor is installed. This is accomplished by using an antenna suitable for the frequency that can be easily absorbed by the intercepting device. An EM wave with a strength that is sufficiently high to activate the FET but does not destroy the device must be radiated. The maximum radiated power is limited by the radiation strength that does not destroy the device, and the reach of the re-emitted signal caused by the signal having this strength limits the maximum attack range. Moreover, an efficient frequency for irradiation can be estimated from the physical structure of the device[HHM+12a], and the transmission system should cover this frequency.

The reception system receives the amplitude-modulated signals radiated by the interceptor and reconstructs the signals. Since EM waves are received at the same frequency as that of the radiated frequency, an antenna tuned to the same frequency as the antenna used for transmission is used. Further, the dynamic range of the reception system should cover both the carrier signal and amplitude-modulated signal. In addition, the modulation index of amplitude-modulated signal may be a quantitative index that can be used to determine the quality of the acquisition of information.

The received signals are processed by converting the frequency and then digitized by an analog-to-digital converter. During signal processing, a low-pass filter appropriate for the frequency bandwidth of the target signals is applied, followed by AM demodulation, producing the intercepted signals. Data are obtained by analyzing the reconstructed intercepted signals according to the protocol. The transmission system and reception system are controlled by a personal computer (PC) that synchronizes the frequency between transmission and reception.

3 Case study

This section describes the mounting of the interceptor described in Section 2 onto a target device, which induces information leakage using EM waves. The targeted devices are mainly those that have been used as targets in past studies on TEMPEST and EM side-channel attacks for comparison between the conventional and proposed attack methods. We also evaluate the microphone of a smart speaker as a bugging device as an example of a target that does not appear in conventional research.

For each experiment, the basic circuit of the interceptor discussed in Section 2 was expanded according to the speed at which targeted information is processed to show that the timing and distance at which leakage is caused can be freely controlled.

3.1 Selection of the FET used for the interceptor based on the target signal characteristics

On the basis of the FET selection criteria discussed in Section 2.3, this experiment used the following FET for the interceptor.

Table 1 summarizes the specifications of the targeted device and internal signals. The results for the PS/2 Keyboard are not included because they might be covered by the

Table 1: Specifications of the targeted device and internal signals

Target Device	Signal Specifications		
	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)[a]	Analog	0–0.7 V	0–32.5 MHz
Audio Device (Headphone)[b]	Analog	-50–50 mV	20 Hz–20 kHz
Cryptographic Device (RSA)[c]	Analog	0.8–1.3 V	0–2.5 MHz
Smart Speaker[d]	Digital	0–3.3 V	0–2 MHz

[a]Resolution: 1024×768 pixels, Refresh Rate: 60 frames/s
[b]Apple iPhone 7 Plus with 50% Sound Volume [c]FPGA Clock Rate: 2.5 MHz
[d]Pulse Density Modulation (PDM) Microphone (Clock Rate: 2 MHz)

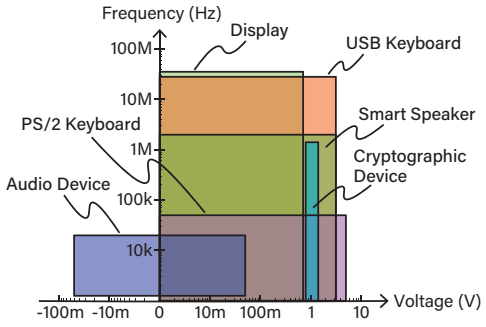


Figure 8: Internal signal classification of the target devices

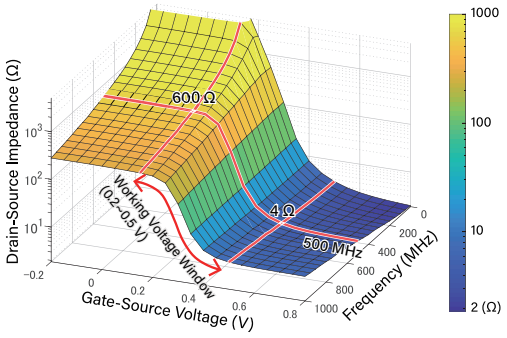


Figure 9: Drain–source impedance characteristics of the Broadcom ATF-54143 FET

results for the Universal Serial Bus (USB) keyboard. The results for the audio device (headphone) are also not included because they might be coverd by the results for smart speaker. The internal signals of a device can be classified by the amplitude and frequency, which are distributed as shown in Figure 8.

Since the signal voltage is in a positive range between 0 V and 5 V, except for side-channel signals for cryptographic devices, an enhancement-mode FET needs to be selected to expect changes in the impedance in this range. This study used a Broadcom ATF-54143 FET that satisfies such conditions. Figure 9 presents a graph that shows the relationship between the gate–source voltage, the drain–source impedance, and the frequency of the signal applied between the drain and the source of the Broadcom ATF-54143 FET, which satisfies the conditions described above.

The side-channel information leak caused by the encryption module consists of an impulse signal series with a small range of voltage fluctuation of approximately 0.3 V. Therefore, by adding a peak hold circuit to the interceptor, it is optimized with respect to AM, which is expanded to a voltage range between 0 V and 0.7 V by further amplification. Given that the fluctuation in this range of voltages is covered by the Broadcom ATF-54143 FET.

According to the specific examples of attacks using interceptors that have been described above, if the voltage and frequency range of the victim signals are within the range in Figure 8, the interceptor may work by simply optimizing the circuit constants such as the value of the resistor. If not, the attack may not succeed. This is the limit of our proposed method.

Table 2: List of experimental devices

No. in Fig.10	Equipment	Model Name
1	Log-Periodic Antenna	Ettus Research LP0410
2	Yagi–Uda Antenna	Maspro U146
3	Signal Generator	Keysight N5181B
4	Power Amplifier	R&K A000110-4040-R
5	SDR ADC/Sig. Proc. Hardware	Ettus Research USRP X310
6	SDR Radio-Frequency Frontend	Ettus Research TwinRX
7	SDR Software	GNU Radio 3.7.12

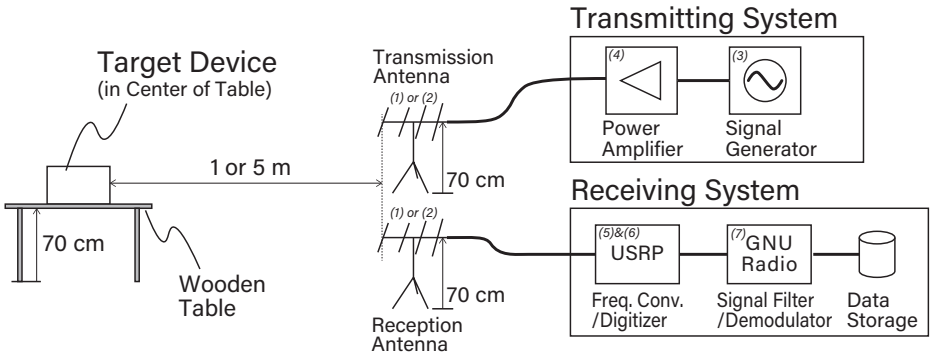


Figure 10: Common experimental system components and layout

3.2 Transmission-and-reception system used in the experiment

Following the driving force behind an interceptor and the reception method for leaked signals, as discussed in Section 2.4, this section describes the transmission-and-reception system. Table 2 lists the experimental devices, and Figure 10 shows the system components and layout. The specifications of the entire transmission-and-reception system are listed in Table 3.

The transmission system consists of a signal generator, an amplifier, and a transmission antenna. The signal generator generates sine waves that serve as an arbitrary frequency and startup power for the interceptor. The generated sine waves are amplified to 40 dB by an amplifier and input into the transmission antenna.

The reception system consists of a reception antenna and software-defined radio (SDR). The reception antenna can also be used as a transmission antenna by using a circulator, but this approach is flawed, given the fact that the reception sensitivity decreases. For this reason, given the fact that the ultrahigh frequency (UHF) antenna is small, this experiment used a structure in which the transmission and reception antennas are separated. Compared to the 19-inch rack, 4-unit volume, and 20-kg weight of the conventional TEMPEST receiver (Dynamic Sciences R-1550A) [Sci], the setup for this experiment is miniature (27.7 cm $\times$ 21.8 cm $\times$ 3.8 cm) and lightweight (1.7 kg). Further, digital signal processing can be used to filter and remove noise without the use of additional devices.

3.3 Experimental procedure

In the experiment, the distance with respect to the target device mounted with an interceptor is varied, and the changes in the quality of the received signals with the distance are observed. Additionally, to compare the leaked signals obtained by conventional TEMPEST

Table 3: Specifications of the transmission-and-reception system

Parameter	Value
Frequency Range	400–1000 MHz
Maximum Transmit Power	40 dBm
Antenna Factor (LP0410)[b]	18.2 dB/m
Antenna Factor (U146)[b]	13.6 dB/m
Method of Self-Interference Suppression	Isolation Using a Directional Antenna
Self-Interference Suppression	>30 dB (400–1000 MHz)
Receive Gain Range of SDR	0–95 dB
Receive Bandwidth of SDR	80 MHz
ADC Sampling Rate of SDR	200 MHz
ADC Resolution of SDR	14 bits
1 LSB Voltage of SDR (RX Gain = 0 dB)[a]	3.9 mV

[a]Measured value at 500 MHz [b]Calculated value at 500 MHz

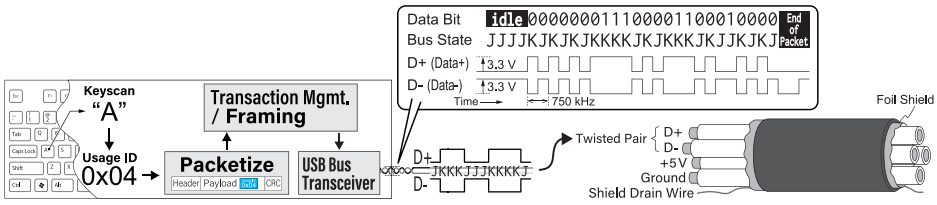


Figure 11: Functions and communication signals of a USB keyboard

and the signals obtained by the proposed method, leaked EM waves were also measured for devices not mounted with an interceptor. In this experiment, conventional TEMPEST uses a cable with a shield cut to evaluate the signals leaked under the same conditions when the interceptor is installed. Moreover, conventional TEMPEST is performed at the frequency where the received power is maximum [HHT+16]. Note that conventional TEMPEST attacks do not work against potentially leak-free devices. Therefore, even if the shield is cut, it is difficult to obtain information using conventional TEMPEST unless the frequency containing the information causes resonance on the cable and the signal is not radiated outside the device. The experimental setup of the conventional TEMPEST is identical to that in Figure 10.

3.4 USB keyboard (digital input device)

A USB keyboard was used as the target. Similar to a PS/2 keyboard, a USB keyboard is a commonly used input device. Unlike a PS/2 keyboard, the signals treated inside the device are digital signals of several megabits per second. A USB keyboard was separately evaluated since the methods for mounting the interceptor and detecting signals are different.

3.4.1 Signals inside the targeted USB keyboard

The targeted USB keyboard sends key input information to the USB host through the following procedure. First, the states of the keys over the key matrix are monitored and recorded by a built-in microcomputer. Next, the key code of the key that is pressed at the moment is returned in response to the read request from the USB host. The transmitted data are the key code values assigned to each key. Figure 11 shows the key input information sent from the keyboard and a schematic of the communication signals.

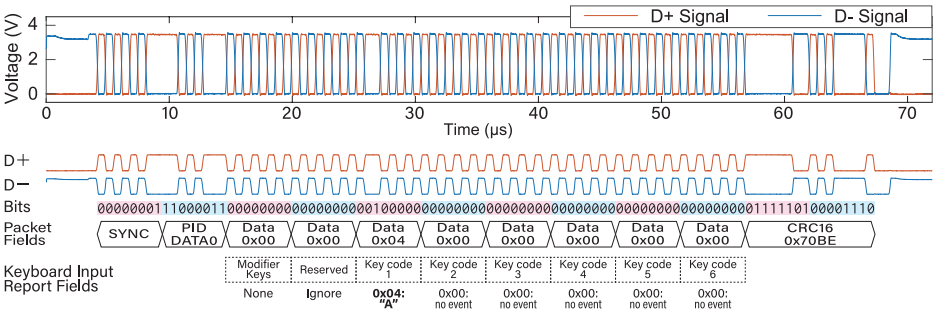


Figure 12: USB signaling and packet format of the USB keyboard

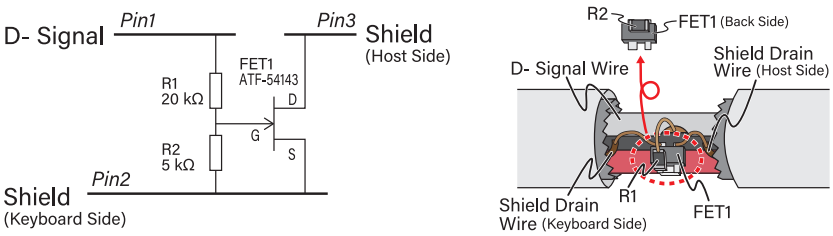


Figure 13: Circuit and wiring diagram of the interceptor for the USB keyboard

The USB host is connected with a data bus of differential signals and a four-core shielded cable. The differential data signals consist of Data+ (D+) and Data- (D-) communication lines. The voltages of these communications lines transition between 0 and 3.3 V and transmit bit information through the potential difference between D+ and D-. There are no clock signals, and a clock sync takes place between the USB host and the USB target through a synchronization pattern transmitted ahead of the data. For a USB keyboard, the bit rate uses the low-speed mode and is 1.5 Mbps.

A key code, which is the key input information, is transmitted as a data packet as a response to a data request by a token packet from the USB host. The payload of the data packet is 12-byte data with a unit of 8 bits, as shown in Figure 12. Figure 12 shows the data packet transmitted while the "A" key is pressed. When a single key is entered, the data are set to the Key Code 1 field. When multiple keys are simultaneously entered, a maximum of six keys are set to the fields for Key Codes 1–6.

3.4.2 Circuit of the interceptor and its implementation

Figure 13 shows the circuit diagram of the interceptor used in the experiment and its implementation method. This circuit consists of a FET and resistors.

To intercept key input information with the interceptor, it is sufficient to obtain either one of the D- or D+ signals, as D- and D+ are complementary. The interceptor in this experiment was structured such that signal information was transmitted outside the device by intercepting the D-signal. The resistances of R1 and R2 are determined to implement a resistive voltage divider that restricts the peak gate-to-source voltage to 0.6 V.

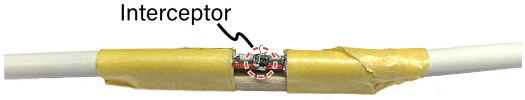


Figure 14: Interceptor installed in the USB cable of the USB keyboard

Table 4: Experimental parameters for intercepting the USB signal of the USB keyboard

Distance	Frequency	Tx Power	Rx Gain	TX & RX Antenna
1 m	690 MHz	30 dBm	58 dB	LP0410
5 m	633 MHz	40 dBm	40 dB	U146

Figure 14 shows the state in which the interceptor built in this experiment is mounted in the cable. The FET is small in size and can be covered easily by the cable jacket; thus, its presence can be hidden.

This experiment induced information leakage by connecting each pin to the communication line of the USB cable. Pin 1 is connected to the D- signal line, Pin 2 is connected to the shield drain wire on the keyboard side, and Pin 3 is connected to the shield drain wire on the USB host side. Shield drain wires function as unintentional antenna. Amplitude-modulated signals are generated by multiplying the alternating current (AC) signals generated between Pins 2 and 3 by irradiating EM waves and communication signals from the keyboard inputs from Pin 1 using the FET. Radiation outside the device occurs, as these signals are transmitted to the unintentional antenna. Moreover, through AM demodulation outside the device, the data signals generated by key inputs can be obtained.

3.4.3 Experimental environment

The experimental environment setup is shown in Figure 10, and the parameters used are listed in Table 4. As explained in the previous section, EM waves irradiated the target device, and the modulated signal was received.

In this section, the unintentional antenna is implemented by the USB cable, keyboard, and PC. The total length of this unintended antenna is 2 m, and the antenna structure can be regarded as a dipole antenna. Therefore, the resonance occurs when the condition

$$f_n = \frac{c}{2L/(2n-1)} \quad (n = 1, 2, 3, ...) \tag{1}$$

is satisfied, where f_n is the resonance frequency of the antenna, n is the order of resonance, c is the light speed and L is the total length of the unintended antenna. The resonance frequency of this antenna can be obtained from Equation 1 as 75, 225, 375, 525, and 675 MHz. Among these frequencies, we employed the frequency around 675 MHz that is suitable for the frequency characteristics of the antenna used for the attack.

Given that the data signals were square waves with a maximum frequency of 750 kHz, the bandwidth used for demodulation was 50 MHz, which included a third-order harmonic. Therefore, bits were readable as square waves from the temporal waveforms after demodulation. The bandwidth was limited up to the third-order harmonic to reduce the calculation cost during signal processing and measurements in real time.

3.4.4 Acquisition of information using the interceptor

Next, the possibility of leaking information from a USB keyboard mounted with an interceptor is specifically considered. In the following experiment, a waveform in which the letter “A” is continuously typed is monitored.

Figure 15 shows the original waveform of the data signals. The data signals could not be monitored with the conventional TEMPEST and without an interceptor, as shown in Figure 16 (similar in the other case studies). Figure 17 shows the result after demodulation of the received signals and two-value processing using the hysteresis threshold value when

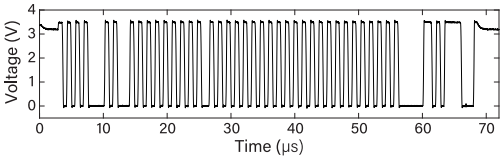


Figure 15: Original USB signal of the USB keyboard

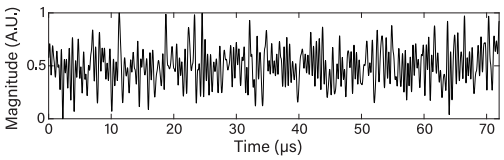


Figure 16: Conventional TEMPEST result for the USB keyboard

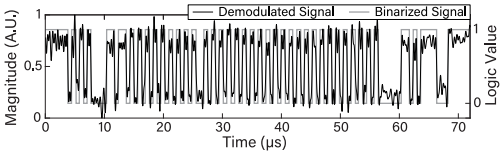


Figure 17: Signal of the USB keyboard intercepted at a distance of 1 m

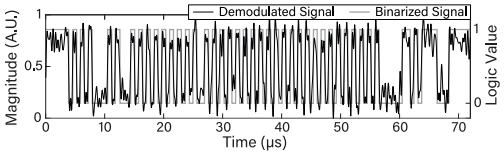


Figure 18: Signal of the USB keyboard intercepted at a distance of 5 m

the distance between the target onto which the interceptor was mounted and the receive antenna was 1 m. We can demodulate the obtained signal and recover the original bit sequence. Figure 18 shows the result when the distance between the target and the antenna was increased to 5 m, the output intensity of the EM waves was increased, and reception and demodulation processing similar to the case for a distance of 1 m were performed. As with the case for a distance of 1 m, the result was such that bit restoration was possible.

3.5 Cryptographic devices (analog signal)

In this section, the secret key of a Rivest–Shamir–Adleman (RSA) cryptographic device is obtained by mounting an interceptor onto it, forcing the radiation of side-channel information outside the device, and performing a simple EM analysis (SEMA) [AARR02, MOP07].

3.5.1 Targeted side-channel signal

Regarding the side-channel signals, this experiment focused on the core voltage fluctuation caused by the operation of a field-programmable gate array (FPGA; Xilinx Artix-7 XC7A35T-L1CSG324I). In the side-channel signals, the squaring operation appears as a large amplitude, and multiplication appears as a small amplitude (Figure 19). As for the correspondence between the bit of the secret key and the core voltage waveform where the secret key is treated as the repeated bit pattern discussed above, a squaring operation whose amplitude is large is performed when the bit is 0. A multiplication operation whose amplitude is small is performed after the squaring operation when the bit is 1. Using this feature, the secret key can be extracted on a bitwise basis.

The aforementioned side-channel signals consist of a series of impulse signals, and their source of generation is the transient current caused by the operation of the complementary metal–oxide–semiconductor (CMOS) gate that constitutes the FPGA. Figure 20 shows an expanded diagram of the temporal waveform of the impulse signal series. The secret key data of the RSA cryptographic device is included in the envelope of this impulse signal series. For this reason, the envelope line was intercepted from the side-channel signals at the interceptor for the cryptographic module, and the envelope signals are leaked as an amplitude-modulated signal outside the device.

The specifications of the RSA cryptographic device implemented onto the FPGA and the data, key, and input data are as follows. The left to right binary method was used for the algorithm. The key length was 1024 bits. Some chosen plaintext was used as the input data, where the least significant bit (LSB) was 1 and everything else was input as 1-,

Table 5: Experimental parameters for intercepting the side-channel signal

Distance	Frequency	Tx Power	Rx Gain	TX & RX Antenna
1 m	497 MHz	20 dBm	48 dB	LP0410
5 m	497 MHz	20 dBm	56 dB	LP0410

which represents 0. The key value repeated an 8-byte pattern of 0x0123456789abcdef 16 times, a value at which changes in bit pattern were easily monitored.

3.5.2 Circuit of the interceptor and its implementation

Figure 21 shows the circuit and wiring diagrams of the interceptor. Because this interceptor circuit is implemented on a power source plane of the cryptographic module, it is able to gain DC power in addition to the side-channel signals. For this reason, this circuit operates by gaining power to drive the circuit from the target power source. As shown in the circuit diagram in Figure 21, signal processing at the circuit consists of side-channel signal extraction from the power source plane, amplification of the extracted side channel signals, a peak hold circuit, and a FET as the variable impedance element that operates the unintentional antenna constructed by the PCB and interceptor as the transmission-and-reception antenna.

Owing to this signal processing, the period of the intercepted signals is decreased to the processing cycle time of the cryptographic module, which allows the frequency bandwidth required for reception to be narrowed and enables a low configuration for the sampling rate by the analog/digital converter of the SDR. This shows that the implementation of a function greater than AM onto the interceptor circuit lowers the difficulty of attack.

To simplify the experiment, an interceptor and an antenna independent of the cryptographic module were used. However, highly dense mounting is easily attainable, and miniaturization to the size shown in Figure 22 is possible, allowing mounting onto the existing circuits of the target. An antenna line is attached to the interceptor, but this antenna line can be omitted by coupling with the power line or communication line.

3.5.3 Experimental environment and parameters

As for other experiments, the environment was set up as shown in Figure 10, and the values listed in Table 5 were used as the parameters for the experiment.

The unintentional antenna in this section is implemented by the PCB of the target and the interceptor. The total length of this unintended antenna is 0.7 m. From Equation 1, the resonance frequency is calculated as 214 MHz, 643 MHz, and 1.07 GHz. Among these, we focus on 643 MHz, which matches the frequency characteristics of the antenna used for the attack, and irradiate around this frequency.

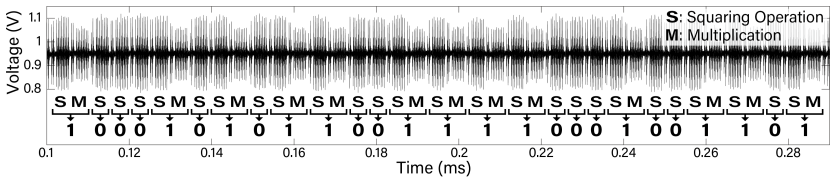


Figure 19: Waveform characteristics of the side-channel signal in the cryptographic device circuit and the method for extracting its secret key

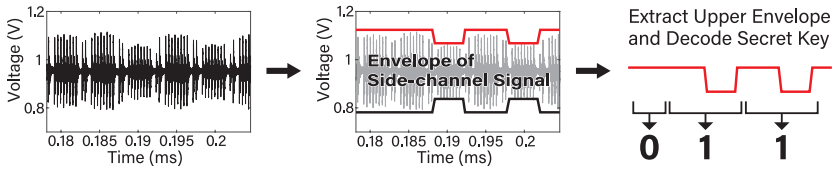


Figure 20: Envelope extraction technique

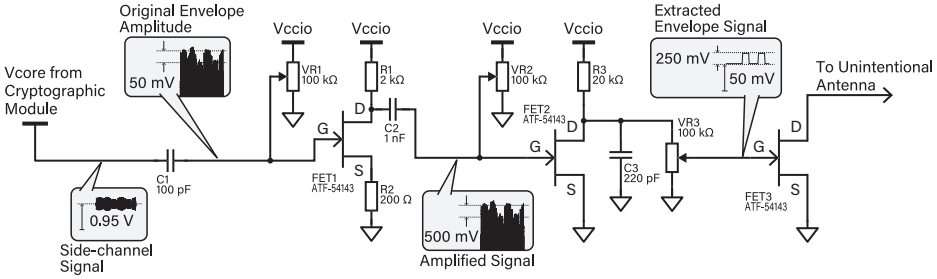


Figure 21: Circuit and wiring diagram for intercepting the side-channel signal of the cryptographic device and the signal processing flow

Given that the clock period of the cryptographic module is 5 μs, the bandwidth for demodulation was set at 2 MHz, which is equal to 10 samples per the clock period.

3.5.4 Acquisition of information using the interceptor

Next, the possibility of intercepting the side-channel signals from the cryptographic module mounted with an interceptor is considered. The side-channel signals monitored over the cryptographic processing board used in the experiment are shown in Figure 23.

As with conventional TEMPEST, the side-channel signals could not be monitored when the device without an interceptor was not irradiated with EM waves were not irradiated, as shown in Figure 24. Figure 25 (Demodulated Signal) shows the side-channel signals, and Figure 25 (Binarized Signal) shows the waveform converted into a two-value form by defining a threshold value when the distance between the target mounted with the interceptor and the receive antenna was 1 m. Every waveform that corresponds to the bits of the secret key could be observed in Figure 25 (Binarized Signal and RSA Key). Figure 26 (Demodulated Signal) shows the result when the distance between the target and the antenna was increased to 5 m and the reception gain of the SDR was increased (and not the output power from the antenna). Figure 26 (Binarized Signal) shows the waveform that was converted into a two-value form at a threshold. Every waveform that corresponds

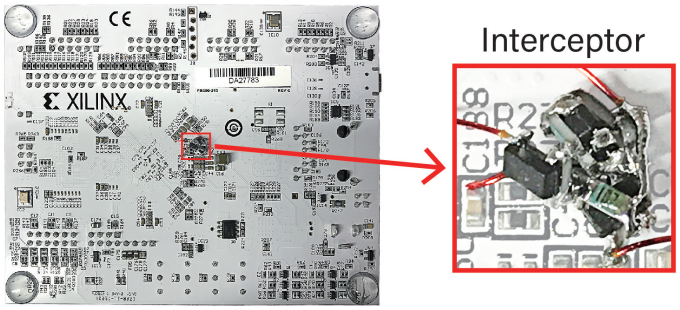


Figure 22: Miniaturized interceptor on the cryptographic device

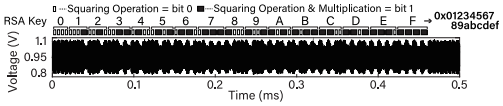


Figure 23: Original side-channel signal of the cryptographic device and the extracted secret key in the RSA cryptographic device

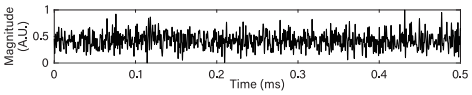


Figure 24: Conventional TEMPEST result for the cryptographic device

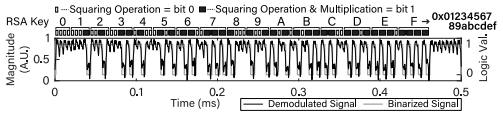


Figure 25: Signal of the cryptographic device intercepted at a distance of 1 m and the extracted secret key in the RSA cryptographic device

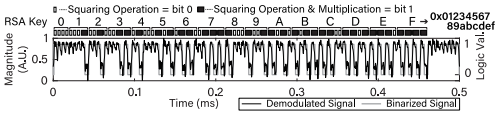


Figure 26: Signal of the cryptographic device intercepted at a distance of 5 m and the extracted secret key in the RSA cryptographic device

to the bits of the secret key could also be observed in Figure 26 (Binarized Signal and RSA Key). In light of the above, the experiment showed that intercepted side-channel signals could be received at a greater distance.

In this section, attacks were performed using AM modulation and demodulation; however, for Differential Power Analysis (DPA) style attacks, it is necessary to measure the amplitude fluctuation precisely according to the input. Therefore, other modulation methods (e.g., frequency modulation) must be utilized for increasing signal fidelity.

3.6 VGA display

In this section, we targeted a PC display that was one of the major targets in the TEMPEST studies [VE85, Kuh02, Kuh04, Kuh05, Kuh13, SS07, SS08, Sek10, SS13, TYF11, SJY14].

3.6.1 Targeted video signals

The targeted display is a flat panel display used for PCs. Figure 27 shows an outline of the drawing operation. This experiment targeted analog RGB signals. An analog RGB signal consists of tricolor luminance signals (R, G, and B), a horizontal sync (HSYNC) signal, and a vertical sync (VSYNC) signal.

The targeted RGB signal is a 700 mV peak-to-peak analog signal. The luminance was expressed as continuous voltage value, where the minimum luminance was expressed as 0 V and the maximum luminance was 700 mV. Pixel information was leaked outside the device by intercepting the changes in the voltage. Table 6 summarizes the VGA signal parameters used in the experiment.

The luminance signals of the analog RGB signals are broadband signals ranging from DC to harmonic signals. The resolution used in this experiment was in the bandwidth of 0–32.5 MHz, and a coaxial cable with limited damping of harmonic signals (a characteristic

Table 6: Signal parameters of the analog RGB (VGA) signal

Parameter	Value
Resolution	1024 × 768 pixels
VSYNC Freq.	59.8 Hz
HSYNC Freq.	48.2 kHz

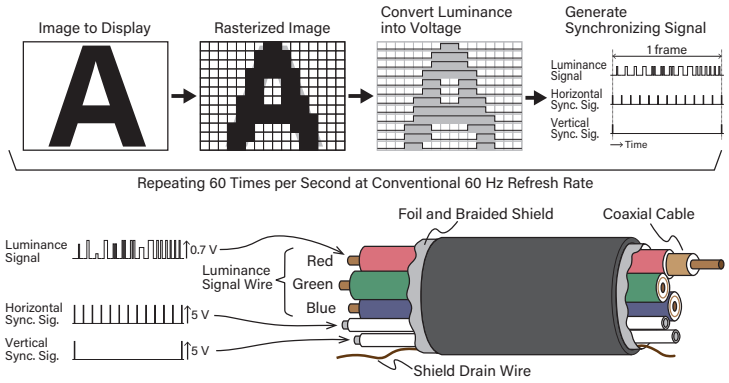


Figure 27: Drawing operation and video signal of the display

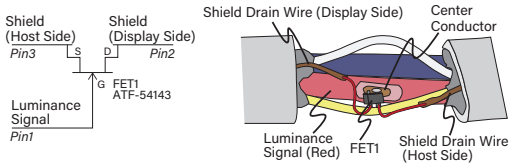


Figure 28: Drawing operation and video signal of the circuit diagram and wiring diagram of the interceptor for the analog RGB video signal on the VGA cable

impedance of 75 Ω) was used for signal transmission. A coaxial cable exists for each RGB luminance signal inside the VGA cable. This experiment was structured such that a red luminance signal is intercepted and transmitted outside the device.

3.6.2 Circuit of the interceptor and its implementation

Figure 28 shows the circuit diagram of the interceptor used in the experiment and the implementation method. This circuit only consists of a FET.

Figure 29 shows the state in which an interceptor built in this experiment is mounted in the cable. The FET is small in size and can be easily covered by the cable jacket; thus, its presence can be hidden.

In this experiment, information leakage is induced by connecting each pin to the communication line of the VGA cable. Pin 1 is connected to the central conductor of the coaxial cable that transmits the red luminance signal, Pin 2 is connected to the shield drain wire on the display side, and Pin 3 is connected to the shield drain wire on the PC side. Amplitude-modulated signals for red luminance are generated by multiplying the high-frequency signals generated between Pins 2 and 3 by irradiated EM waves and the red luminance signal from the Pin 1 input using the FET. Radiation outside the device occurs as these signals are transmitted to the unintentional antenna. Moreover, through

Figure 29: Interceptor installed in the VGA cable

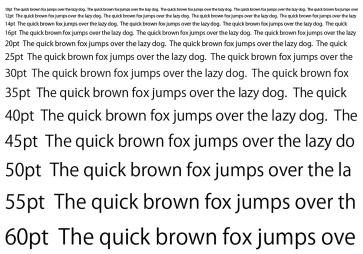


Figure 30: Test pattern

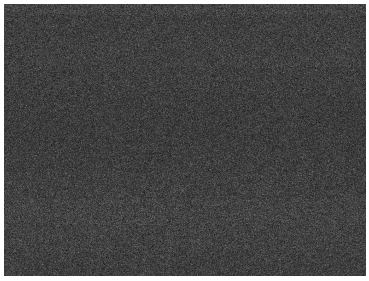


Figure 31: TEMPEST result

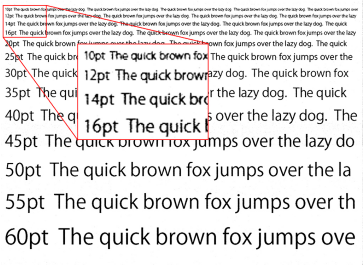


Figure 32: Image intercepted at a distance of 1 m

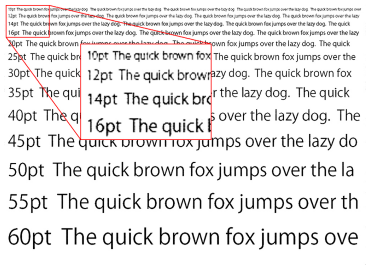


Figure 33: Image intercepted at a distance of 5 m

Table 7: Experimental parameters for intercepting the video signal

Distance	Frequency	Tx Power	Rx Gain	TX & RX Antenna
1 m	406.2 MHz	30 dBm	49 dB	U146
5 m	697 MHz	40 dBm	64 dB	U146

AM demodulation outside the device, the changes in the red luminance can be obtained, and videos can be obtained by reconstructing the raster scans back to images.

3.6.3 Experimental environment

As with the other experiments, the environment was set up as shown in Figure 10, and the values listed in Table 7 were used as parameters for the experiment.

The unintentional antenna in this section is implemented by the VGA cable, the PC and the display. The total length of this unintended antenna is 2.3 m. From Equation 1, the resonance frequency is calculated as 62.5 MHz, 188, 313, 438, 563, and 688 MHz. Among these, we focus on 438 MHz and 688 MHz, which matches the frequency characteristics of the antenna used for the attack, and irradiate around this frequency.

Given that data signals targeted in this experiment are analog signals with a maximum frequency of 0–32.5 MHz, the occupied bandwidth after modulation is 65 MHz. For this reason, the demodulation bandwidth was set higher at 100 MHz so that the luminance information can be reconstructed at the pixel level.

3.6.4 Acquisition of information using the interceptor

Next, the possibility of leaking video information from a VGA cable mounted with an interceptor is considered. In the following experiment, the reception waveform is monitored when Figure 30 is displayed.

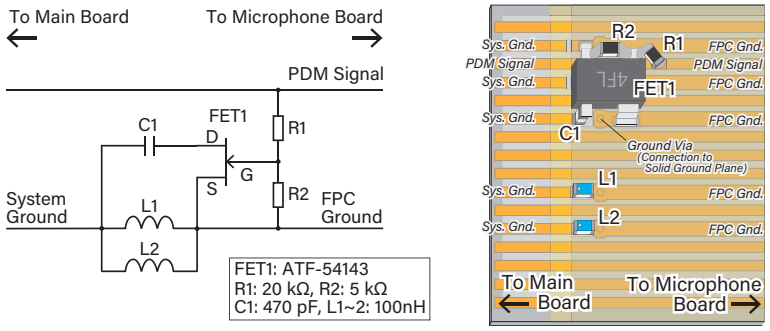


Figure 34: Circuit and wiring diagram of the interceptor for the audio device

As with conventional TEMPEST, video could not be monitored when a device without an interceptor was not irradiated with EM waves, as shown in Figure 31. Figure 32 shows the reconstructed image result after the demodulation of the received signals when the distance between the target mounted with the interceptor and the receive antenna was 1 m. Video where words could be identified in a similar fashion as the original video was observed is shown in Figure 33. As with the case in which the distance between the target and the antenna was 1 m, words could be identified as with the original data, even when the distance between the target and the antenna was increased to 5 m and the output intensity of the EM waves was increased (Figure 33).

3.7 Audio Device

This section considers the interception of sound information. Specifically, a smart speaker is targeted.

3.7.1 Targeted sound signal

A smart speaker interprets wake words such as "OK Google," "Alexa," or "Hey Siri" on the basis of the surrounding sound acquisition and invokes the speech recognition process. Further, the surrounding sound is always monitored to extract wake words. Therefore, in the case of installing an interceptor on such a device, the sound around the device can be intercepted from a distance.

Microelectromechanical systems (MEMS) microphones are generally used for speech acquisition because of their low power consumption, performance, and size. In this example, we consider the interception of the surrounding speech from the output signal of an MEMS microphone. The output signal of an MEMS microphone is the digital signal using pulse density modulation (PDM). The voltage range of this signal is around 0–3.3 V, which is the same as a general single-end digital signal on the board. In addition, the signal input to the microphone is a chirp signal in the range of 20 Hz–20 kHz.

The speech output device used in the experiment was a tablet PC, and chirp signals were released from the external speaker connected to tablet PC. The distance between the smart speaker with an interceptor and the speaker that output the chirp signals was 1 m. We monitored whether the chirp signals can be intercepted outside the device while changing the volume by 50% from 0%–100%.

3.7.2 Circuit of the interceptor and its implementation

An MEMS microphone is directly mounted on the printed circuit board (PCB) of the smart speaker. Therefore, the unintentional antenna must consist of the electrical element or wiring near the output signal of the MEMS microphone. In this section, a flexible printed

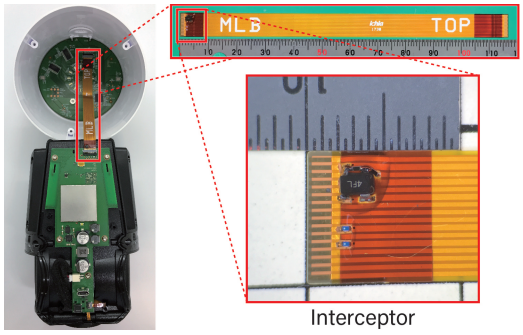


Figure 35: Interceptor installed in the enclosure of the smart speaker

Table 8: Experimental parameters for intercepting the audio signal

Distance	Frequency	Tx Power	Rx Gain	TX & RX Antenna
1m	649.7 MHz	10 dBm	68 dB	U146
5m	644.7 MHz	30 dBm	60 dB	U146

circuit (FPC), which works as a PCB-to-PCB cable, is used as an unintentional antenna. The FPC has a solid ground plane to reduce unwanted EM emission. If the ground plane is isolated from the system ground at the attack frequency, it efficiently receives high frequency power when EM waves at the resonant frequency are irradiated. Figure 34 shows the circuit diagram of the implemented interceptor and the implementation method. The voltage level of the target PDM signal is divided by the resistor to a voltage level at which the FET of interceptor efficiently operates. The ground plane of the FPC, which works as an unintentional antenna, is connected with the drain of the FET of the interceptor by a capacitor.

Moreover, to prevent distortion of the PDM signal caused by the installed interceptor, the resistance between the interceptor and the PDM signal must be high. Moreover, to prevent a change in the ground plane potential caused by installing an interceptor, the inductance between the ground plane and the system ground must be small so that only the high-frequency signal can be blocked.

Figure 35 shows the state in which the interceptor built in this experiment was mounted onto the smart speaker. The size of the circuit element for the interceptor was small and could be easily installed into the space inside the smart speaker so that its presence can be hidden.

3.7.3 Experimental environment and parameters

As with the other experiments, the environment was set up as shown in Figure 10, and the values listed in Table 8 were used as parameters for the experiment.

The unintentional antenna in this section is implemented by the PCB of the target and the FPC. The total length of this unintended antenna is 23 cm. From Equation 1, the resonance frequency is calculated as 652 MHz, 1.96 GHz, and 3.26 GHz. Among these, we focus on 652 MHz, which matches the frequency characteristics of the antenna used for the attack, and irradiate around this frequency.

Given that the PDM signals were square waves with a maximum frequency of 2 MHz, the bandwidth used for demodulation was 10 MHz, which included a third-order harmonic. Thus, bits were readable as square waves from the temporal waveforms after demodulation. The bandwidth was limited up to the third-order harmonic to reduce the calculation cost

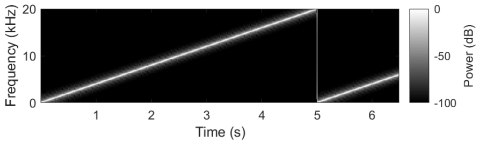


Figure 36: Spectrogram of the original audio data

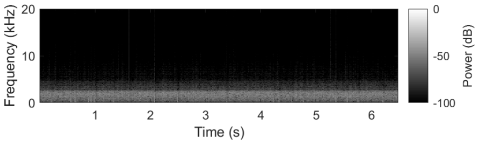
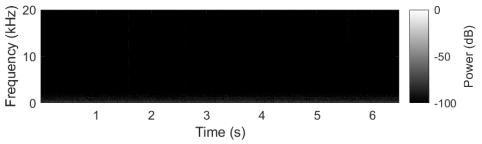
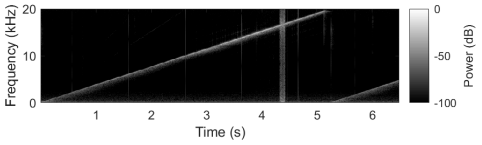


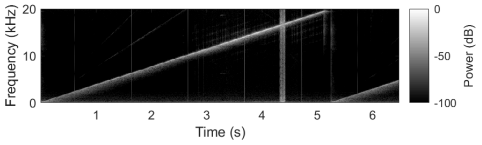
Figure 37: Spectrogram of the conventional TEMPEST result



(a) Volume level: 0 %

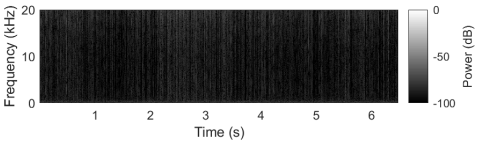


(b) Volume level: 50 %

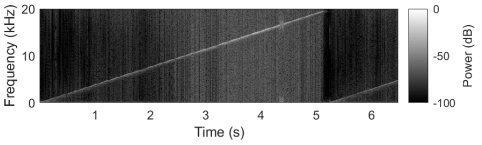


(c) Volume level: 100 %

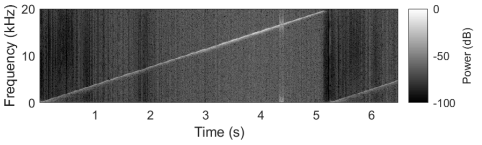
Figure 38: Results for the intercepted audio signal at a distance of 1 m



(a) Volume level: 0 %



(b) Volume level: 50 %



(c) Volume level: 100 %

Figure 39: Results for the intercepted audio signal at a distance of 5 m

during signal processing and measurements in real time.

3.7.4 Acquisition of information by the interceptor

Next, the possibility of leaking speech information from a smartspeaker mounted with an interceptor is specifically considered. The spectral changes over time for the chirp signals used in the experiment are shown in the spectrogram in Figure 36.

As with conventional TEMPEST, the chirp signals could not be monitored at any volume when a device without an interceptor was not irradiated with EM waves, as shown in Figure 37. Figure 38 shows spectrograms of speech extracted from demodulated reception signals when the distance between the target mounted with the interceptor and the receive antenna was 1 m. The fundamental waves of the original signals could be observed at every volume except volume 0 % in Figure 38. Figure 39 shows spectrograms of demodulated speech from the received signals when the distance between the target and the antenna was increased to 5 m. The fundamental waves of the chirp signals could be observed at every volume in Figure 39.

3.8 Summary of experiments

This section showed that forcefully leaking information is possible through EM waves by mounting the interceptor proposed in Section 2 onto any device, which handles high/low-

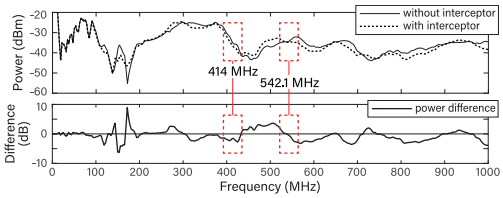


Figure 40: Comparison of the frequency response to differentiate between the normal case (not modified) and that modified with the interceptor

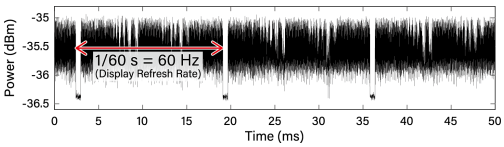


Figure 41: Temporal variation in the radiated EM wave power at 542.1 MHz

speed analog/digital signals. In the experiment, observations were acquired at a distance as far as 5 m, but it is possible to obtain information at a farther distance by increasing the transmission power of the antenna. The interceptor used in this experiment was handmade, but its size may be further reduced and improved in terms of precision through techniques such as the implementation of a circuit board.

4 Detection method for the interceptor

The interceptor used in this study was driven by the power from the EM waves applied from the outside. It modulated information from inside a device and radiated it outside the device. The EM waves used for the irradiation attack exceed EMC regulations. A mechanism that stops operation when such EM waves are irradiated can be a countermeasure. As a concrete example of a countermeasure, a monitor that can measure the voltage fluctuation inside a device caused by intentional EM interference can be installed[ZS18][FHB+18]. However, as the monitoring of wide frequency bands is difficult, it is necessary to estimate the frequency used for the attack. For example, low-immunity frequencies (i.e., frequencies at which EM waves are easily induced inside a device) are considered as monitoring candidates.

Moreover, the presence of an interceptor may be verified by detecting the difference between the case in which EM waves are irradiated and the case in which such waves are not irradiated. Figure 40 shows a graph that compares the spectrum between the case in which EM waves irradiate a device mounted with an interceptor and the case in which such waves do not irradiate the device. The interceptor considered in this study was implemented on an analog VGA cable of a display, as explained Section 3.6. Figure 40 shows that a difference is observed between 414 MHz, a frequency at which the waves are applied from the outside to start the interceptor (shown in Section 3.1), and 542.1 MHz. Figure 41 also shows a graph of the temporal variation by focusing on the frequency for which there was a difference. The obtained results show that luminance signals repeated at a period of 60 Hz went through AM demodulation while using the frequency of 542.1 MHz as a carrier, thus leaking information outside the device. The presence of a mounted interceptor can be detected by scanning the device periodically by the method described above. The spectrum of radiated EM waves changes if the interceptor is activated by the irradiated EM waves. Therefore, we can detect attacks by observing the chance of the radiation spectrum, even if the target signal is unknown.

The interceptor may also be detected by continuously observing the radiated spectrum alone. The proposed interceptor induces EM waves of a specific frequency that are applied outside the device into the device and uses these waves as the driving power and as a carrier of modulated waves that cause information leakage. The addition of such a circuit that improves the sensitivity to EM waves decreases the immunity of the device and is equivalent to making changes to its equivalent circuit and frequency characteristic [Pau06]. As a result, the EM wave spectrum irradiated from the device changes [HHM+12a].

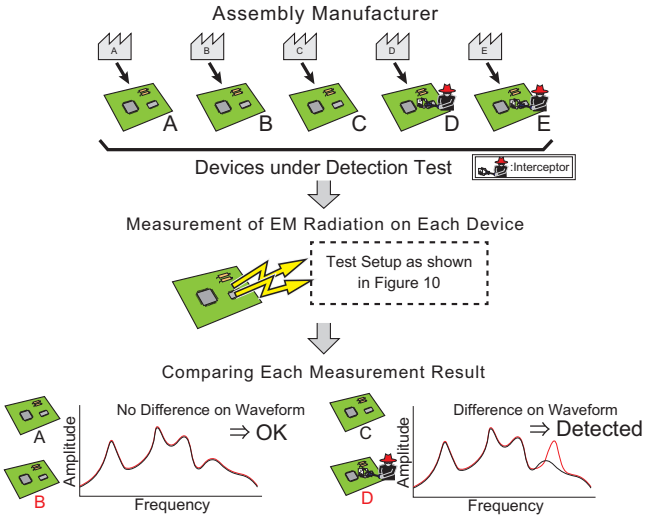


Figure 42: Framework for the HT insertion prevention of a board

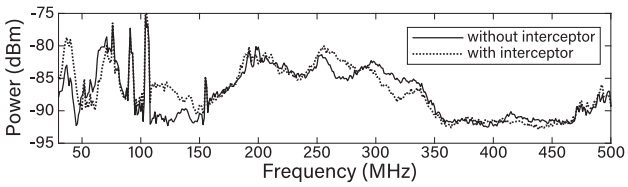


Figure 43: Comparison of the radiation power spectrum to differentiate between the normal case (not modified) and that modified with the interceptor

In order to measure the difference between EM waves with/without an interceptor, a board without an interceptor is required. For this purpose, it is better to use multiple manufacturers to assemble the board. This idea has already been proposed as a framework for HT insertion prevention for ICs, and we applied the idea to a board, as shown in Figure 42. Note that the framework used here is different from that in IC split fabrication [XFT15, VDS+14] and assumes the use of multiple manufacturers for board manufacturing. In a device with an interceptor, the equivalent circuit of the device changes significantly. This is a large change compared to the change caused by the manufacturing variance in the equivalent circuit. Additionally, changes in the equivalent circuit of the device affect the spectrum of the radiated EM waves. Therefore, by observing the radiated spectrum of the instrument, it is possible to distinguish devices "with" and "without" interceptors.

Figure 43 shows the radiation spectrum observed from the device in the case where there "was" an interceptor and the case where there "was not" an interceptor. A difference in the spectrum is observed between these cases; thus, it is possible to detect whether an interceptor was mounted by a specific manufacturer/manufacturers.

Another potential method of detection is to prevent the induction of EM waves applied from the outside to drive the HT into the device. Components for EMC and noise suppression as well as measures against intentional EM disturbances are examples of effective methods for this approach [Rad14, K.716, K.816a].

Furthermore, the propagation of interfering EM waves into a device can be regarded as a phenomenon in which the direction of propagation of the EM waves leaking from the device is in the opposite direction owing to the EM reciprocity theorem. For this reason, the application of ITU-T Recommendations K.84, K.87, and K.115 [K.811, K.816b, K.115]

to the problem of reducing information leakage by leaking EM waves may also be a viable measure against the threat discussed in this paper.

5 Conclusions

This paper focused on the threat of information leakage through EM waves. Conventionally, devices targeted by such a threat are those with the potential leakage of EM waves during their operation, and the information inside the device was obtainable by monitoring the leaking EM waves near the device. In contrast, the leakage of EM waves was not potentially observed for some devices, and such devices were not a target of the threat discussed above.

In light of this, this paper proposed an interceptor that forces leakage even in devices that do not suffer potential EM leakage. The proposed interceptor consisted of an inexpensive FET and wiring without a special antenna structure and can be mounted onto manufactured devices. The driving energy can be supplied via EM waves outside the device, rendering an individual power supply unnecessary. Additionally, leakage occurs only when a signal with a specific frequency irradiates the device, making the detection of leakage from the device by anyone other than the attacker difficult. Furthermore, an increase in the intensity of the irradiated EM waves enables control of the distance at which information can be obtained. The intercepted result captures information signals without any change in comparison with the differentiated waveform of conventional TEMPEST.

The study showed that it is possible to force information leakage through EM waves by using a USB keyboard as a digital signal target and a cryptographic module as an analog signal target to ensure data confidentiality and completeness, which is realized by mounting an interceptor onto these devices. Further, such leakage can be monitored from a distance using the devices by increasing the intensity of the irradiated EM waves. Moreover, a signal that satisfies the conditions listed in Section 3.1 might be covered by the interceptor to force information leakage.

To detect the aforementioned threat, we focused on the changes in the device itself and the surrounding EM environment as a result of mounting an interceptor and considered a method of detecting a malicious circuit that causes such a threat by using both passive and active monitoring methods.

Acknowledgments

This research was partly supported by JSPS KAKENHI under Grant Numbers JP18KT0050, JP18K18053, JP18K18050, the Telecommunications Advancement Foundation, and SECOM Science and Technology Foundation. And we would like to thank Prof. Youngwoo Kim and ISE laboratory students for valueable advice.

References

[AARR02] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, and Pankaj Rohatgi. The em side?channel (s). In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 29–45. Springer, 2002.

[And08] Ross Anderson. *Security engineering*, chapter 17, pages 523–546. John Wiley & Sons, 2008.

[Blo18] Bloomberg Businessweek. The big hack: How china used a tiny chip to infiltrate u.s. companies. https://www.bloomberg.com/news/features/2018-

10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies, 2018.

[CLK11] John Clark, Sylvain Leblanc, and Scott Knight. Risks associated with usb hardware trojan devices used by insiders. In *2011 IEEE International Systems Conference*, pages 201–208. IEEE, 2011.

[CPM+18] Giovanni Camurati, Sebastian Poeplau, Marius Muench, Tom Hayes, and Aurélien Francillon. Screaming channels: When electromagnetic side channels meet radio transceivers. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 163–177. ACM, 2018.

[CY10] Liqun Chen and Moti Yung. *Trusted Systems*, volume 6802 of *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, 2010.

[ESS14] Evan Everett, Achaleshwar Sahai, and Ashutosh Sabharwal. Passive self-interference suppression for full-duplex infrastructure nodes. *IEEE Transactions on Wireless Communications*, 13(2):680–694, 2014.

[FHB+18] Daisuke Fujimoto, Yuichi Hayashi, Arthur Beckers, Josep Balasch, Benedikt Gierlichs, and Ingrid Verbauwhede. Detection of iemi fault injection using voltage monitor constructed with fully digital circuit. In *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, pages 753–755. IEEE, 2018.

[GM11] Zheng Gong and Marc X Makkes. Hardware trojan side-channels based on physical unclonable functions. In *IFIP International Workshop on Information Security Theory and Practices*, pages 294–303. Springer, 2011.

[HHM+12a] Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Analysis of electromagnetic information leakage from cryptographic devices with different physical structures. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):571–580, 2012.

[HHM+12b] Yuichi Hayashi, Naofumi Homma, Takaaki Mizuki, Haruki Shimada, Takafumi Aoki, Hideaki Sone, Laurent Sauvage, and Jean-Luc Danger. Efficient evaluation of em radiation associated with information leakage from cryptographic devices. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):555–563, 2012.

[HHM+14] Yuichi Hayashi, Naofumi Homma, Mamoru Miura, Takafumi Aoki, and Hideaki Sone. A threat for tablet pcs in public space: Remote visualization of screen images using em emanation. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 954–965. ACM, 2014.

[HHT+16] Yuichi Hayashi, Naofumi Homma, Yohei Toriumi, Kazuhiro Takaya, and Takafumi Aoki. Remote visualization of screen images using a pseudo-antenna that blends into the mobile environment. *IEEE Transactions on Electromagnetic Compatibility*, 59(1):24–33, 2016.

[JT12] Marc Joye and Michael Tunstall. *Fault analysis in cryptography*. Springer-Verlag Berlin Heidelberg, 2012.

[K.115] ITU-T K.115. Mitigation methods against electromagnetic security threats, 2015.

[K.716] ITU-T K.78. High altitude electromagnetic pulse immunity guide for telecommunication centres, 2016.

[K.811] ITU-T K.84. Test methods and guide against information leaks through unintentional electromagnetic emissions, 2011.

[K.816a] ITU-T K.81. High-power electromagnetic immunity guide for telecommunication systems, 2016.

[K.816b] ITU-T K.87. Guide for the application of electromagnetic security requirements – overview, 2016.

[KA98] Markus G Kuhn and Ross J Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*, pages 124–142. Springer, 1998.

[KH18] Masahiro Kinugawa and Yuichi Hayashi. Range of information leakage from iot devices with hardware trojans. In *2018 IEEE International Symposium on Electromagnetic Compatibility and 2018 IEEE Asia-Pacific Symposium on Electromagnetic Compatibility (EMC/APEMC)*, pages 118–118, May 2018.

[Kuh02] Markus G Kuhn. Optical time-domain eavesdropping risks of crt displays. In *Proceedings 2002 IEEE Symposium on Security and Privacy*, pages 3–18. IEEE, 2002.

[Kuh04] Markus G Kuhn. Electromagnetic eavesdropping risks of flat-panel displays. In *International Workshop on Privacy Enhancing Technologies*, pages 88–107. Springer, 2004.

[Kuh05] Markus G Kuhn. Security limits for compromising emanations. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 265–279. Springer, 2005.

[Kuh13] Markus G Kuhn. Compromising emanations of lcd tv sets. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):564–570, 2013.

[Leh12] Harvey Lehpamer. *RFID design principles*, chapter 5. Artech House, 2012.

[Mar92] Michel Mardiguian. *Controlling radiated emissions by design*. Springer, 1992.

[MOP07] Stefan Mangard, Elisabeth Oswald, and Thomas Popp. *Power analysis attacks: Revealing the secrets of smart cards*. Springer US, 2007.

[Oss14] Michael Ossmann. The nsa playset: Rf retroreflectors. In *DEF CON*, 2014.

[Oss15] Michael Ossmann. The nsa playset: A year of toys and tools. In *BlackHat*, 2015.

[Pau06] Clayton R Paul. *Introduction to electromagnetic compatibility*, volume 184. John Wiley & Sons, 2006.

[Proa] GBPPR Project. Gbppr project. http://www.qsl.net/n9zia/.

[Prob] GBPPR Project. Gbppr tawdryyard experiments. http://67.225.133.110/~gbpprorg/mil/photoanglo/tawdryyard/index.html.

[Proc] GBPPR Project. Gbppr vision #26: Overview of the nsa's tawdryyard radar retro-reflector. https://youtu.be/KDQxDxiflyo.

[PZCW16] Milos Prvulovic, Alenka Zajić, Robert L Callan, and Christopher J Wang. A method for finding frequency-modulated and amplitude-modulated electromagnetic emanations in computer systems. *IEEE Transactions on Electromagnetic Compatibility*, 59(1):34–42, 2016.

[Rad14] William Radasky. Electromagnetic warfare is here. http://spectrum.ieee.org/aerospace/military/electromagnetic-warfare-is-here, IEEE Spectrum, 2014.

[RWTP08] Reza M Rad, Xiaoxiao Wang, Mohammad Tehranipoor, and Jim Plusquellic. Power supply signal calibration techniques for improving detection resolution to hardware trojans. In *Proceedings of the 2008 IEEE/ACM International Conference on Computer-Aided Design*, pages 632–639. IEEE Press, 2008.

[Sci] Dynamic Sciences. Dynamic sciences r-1550a. http://www.dynamicsciences.com/client/show_product/33.

[Sek10] Hidenori Sekiguchi. Information leakage of input operation on touch screen monitors caused by electromagnetic noise. In *2010 IEEE International Symposium on Electromagnetic Compatibility*, pages 127–131. IEEE, 2010.

[SJY14] Tae-Lim Song, Yi-Ru Jeong, and Jong-Gwan Yook. Modeling of leaked digital video signal and information recovery rate as a function of snr. *IEEE Transactions on Electromagnetic compatibility*, 57(2):164–172, 2014.

[SS07] Hidenori Sekiguchi and Shinji Seto. An evaluation method of the display image reconstructed by electromagnetic emanation. In *EMC Europe Workshop 2007*, pages abs–133. EMC Europe, 2007.

[SS08] Hidenori Sekiguchi and S Seto. Proposal of an information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer. In *2008 IEEE Instrumentation and Measurement Technology Conference*, pages 1859–1863. IEEE, 2008.

[SS13] Hidenori Sekiguchi and Shinji Seto. Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage. *IEEE Transactions on Electromagnetic Compatibility*, 55(3):547–554, 2013.

[TK10] Mohammad Tehranipoor and Farinaz Koushanfar. A survey of hardware trojan taxonomy and detection. *IEEE design & test of computers*, 27(1):10–25, 2010.

[TTY+06] Toshihide Tosaka, Kazumasa Taira, Yukio Yamanaka, Atsuhiro Nishikata, and Mitsuo Hattori. Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer. In *2006 17th International Zurich Symposium on Electromagnetic Compatibility*, pages 630–633. IEEE, 2006.

[TYF11] Toshihide Tosaka, Yukio Yamanaka, and Kaori Fukunaga. Method for determining whether or not information is contained in electromagnetic disturbance radiated from pc display. *IEEE Transactions on Electromagnetic Compatibility*, 53(2):318–324, 2011.

[VDS+14] Kaushik Vaidyanathan, Bishnu P. Das, Ekin Sumbul, Renzhi Liu, and Larry Pileggi. Building trusted ics using split fabrication. In *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 1–6. IEEE, May 2014.

[VE85] Wim Van Eck. Electromagnetic radiation from video display units: an eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985.

[VP09] Martin Vuagnoux and Sylvain Pasini. Compromising electromagnetic emanations of wired and wireless keyboards. In *USENIX security symposium*, pages 1–16, 2009.

[VP10] Martin Vuagnoux and Sylvain Pasini. An improved technique to discover compromising electromagnetic emanations. In *2010 IEEE International Symposium on Electromagnetic Compatibility*, pages 121–126. IEEE, 2010.

[Wik] Wikipedia. NSA ANT catalog — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=NSA%20ANT%20catalog.

[WTP08] Xiaoxiao Wang, Mohammad Tehranipoor, and Jim Plusquellic. Detecting malicious inclusions in secure hardware: Challenges and solutions. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust*, pages 15–19. IEEE, 2008.

[XFT15] Kan Xiao, Domenic Forte, and Mark Mohammed Tehranipoor. Efficient and secure split manufacturing via obfuscated built-in self-authentication. In *2015 IEEE International symposium on hardware oriented security and trust (HOST)*, pages 14–19. IEEE, 2015.

[ZP14] Alenka Zajić and Milos Prvulovic. Experimental demonstration of electromagnetic information leakage from modern processor-memory systems. *IEEE Transactions on Electromagnetic Compatibility*, 56(4):885–893, 2014.

[ZS18] Mark Zhao and G Edward Suh. Fpga-based remote power side-channel attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 229–244. IEEE, 2018.