Echo TEMPEST: EM Information Leakage Induced by IEMI for Electronic Devices

Shugo Kaji, *Student Member, IEEE*, Daisuke Fujimoto, *Senior Member, IEEE*, Masahiro Kinugawa, *Member, IEEE*, and Yuichi Hayashi, *Senior Member, IEEE*

***Abstract*—Electromagnetic (EM) information leakage encourages attacks, wherein the attackers passively capture and analyze EM waves that are unintentionally generated by devices. Generally, devices with weak EM emission intensities are not targeted. However, even these devices would be subject to attacks if it becomes possible to actively sense the electrical changes that occur within them when information is processed. This article demonstrates the feasibility of the information leakage threat induced by the active sensing of input impedance changes in the input/output (I/O) circuit of an integrated circuit (IC). Specifically, the changes in the input impedance when information was transmitted from the IC, were measured by irradiating the EM waves from outside the target device. This article labels the threat as Echo TEMPEST. The experiment validated Echo TEMPEST with an evaluation board that simulated the I/O circuit of the IC, UART modules, and USB keyboards. It was also demonstrated that attackers could control the distance (obtained information from the target device), depending on the intensity of the irradiated EM waves. Furthermore, we discussed countermeasure methods focusing on the conditions for executing Echo TEMPEST.**

***Index Terms*—Eavesdrop, electromagnetic emanations, electromagnetic information leakage, hardware security, information security, intentional electromagnetic interference, TEMPEST.**

I. Introduction

PREVIOUSLY, measures for ensuring the security of devices with access to confidential information had isolated them from the Internet and other public networks, thereby eliminating the path for executing attacks [1].

However, when information is processed inside an electronic device, it generates electrical signals, such as current and voltage, which vary with time. These time-varying signals unintentionally generate electromagnetic (EM) waves that radiate from the device. If an attacker captures such radiated EM waves, the device's confidential information is leaked [2], [3]. In particular, input/output (I/O) information of human-oriented devices (e.g., displays, keyboards, printers, and audio) is not encrypted, and an attacker can obtain it by capturing and analyzing the radiated EM waves.

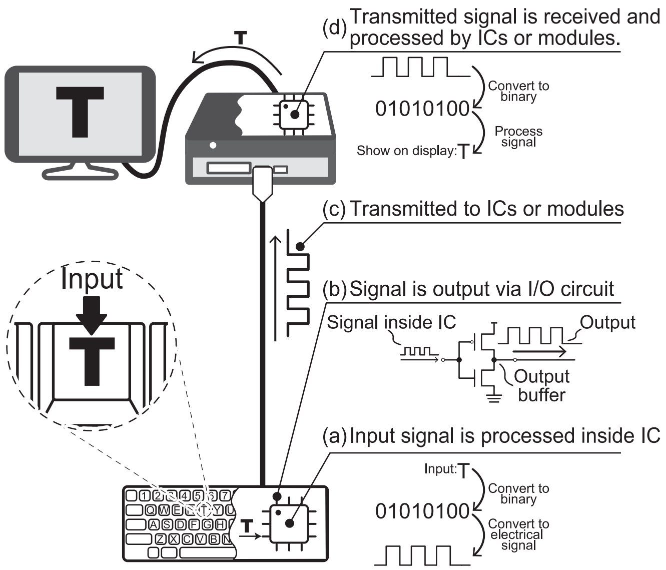

(d) Transmitted signal is received and processed by ICs or modules.
T
Convert to binary
01010100
Process signal
Show on display: T
(c) Transmitted to ICs or modules
(b) Signal is output via I/O circuit
Signal inside IC
Output
Output buffer
Input
T
(a) Input signal is processed inside IC
Input: T
Convert to binary
01010100
Convert to electrical signal

Fig. 1. Diagram of a mechanism by which input/output (I/O) information, which is the target of electromagnetic information leakage, is processed inside the device and propagated as an electrical signal. (a) User's input signals or signals inside the device are processed inside the integrated circuit (IC). (b) Signal is output to the transmission line as an electrical signal through the IC's I/O circuit. (c) Signals output from the I/O circuit are transmitted to the ICs or modules for the next processing. (d) Transmitted electrical signals are received and processed by the ICs or modules.

Until now, attacks, known under the code name TEMPEST [4], against information devices by capturing the radiated EM waves have been discussed only in the fields of military and diplomacy. Discussions related to commercial products [5], [6], [7], [8], [9], [10], [11], [12], [13] began after the possibility of such an attack was demonstrated by the Dutch researcher Wim van Eck in the early 1980s [14].

Fig. 1 illustrates the information processing and electrical signal propagation of I/O devices. Electrical signals are the main target of information leakage caused by the capture of radiated EM waves (EM information leakage). Radiated EM waves are generated in the process indicated in Fig. 1(a)–(d) or their mixed signals based on the mechanism shown in Fig. 2 [15], [16].

The above-cited threat of EM information leakage is a passive attack in which the attacker captures EM waves radiated from the device against the designer's intention. It is difficult for

Manuscript received 3 November 2022; accepted 12 February 2023. Date of publication 3 April 2023; date of current version 13 June 2023. This work was supported by the JSPS KAKENHI under Grant JP19H01104, Grant JP21K19772, Grant JP22K12031, and Grant JP22H04999. *(Corresponding author: Shugo Kaji.)*

Shugo Kaji, Daisuke Fujimoto, and Yuichi Hayashi are with the Nara Institute of Science and Technology, Ikoma 630-0192, Japan (e-mail: kaji.shugo.kp0@is.naist.jp; fujimoto@is.naist.jp; yu-ichi@is.naist.jp).

Masahiro Kinugawa is with the University of Fukuchiyama, Fukuchiyama 620-0886, Japan (e-mail: kinugawa@fukuchiyama.ac.jp).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TEMC.2023.3252636.

Digital Object Identifier 10.1109/TEMC.2023.3252636

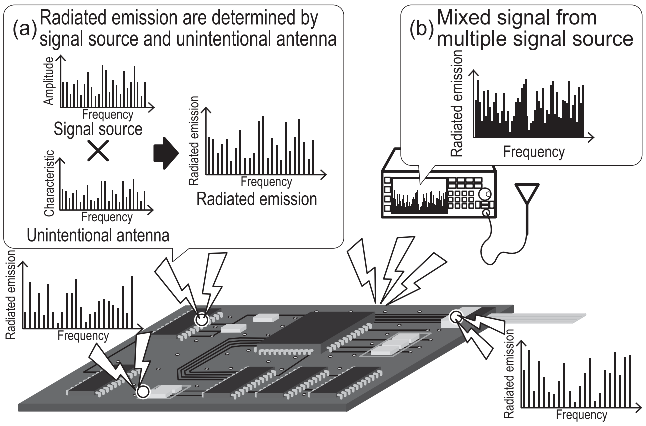


Fig. 2. Diagram of a mechanism by which electrical signals inside the device radiate as EM waves. (a) Process by which signals inside a device are radiated as EM waves through the device's unintentional antenna and (b) EM waves are a mixture of multiple signals measured outside the device.

attackers to control the intensity of the radiated EM waves. Therefore, radiated EM waves were captured with lightweight and miniaturized measurement setups [8], [17], [18], antennas with high gain, and instruments with wide resolution bandwidths [19], [20], depending on the attack scenario. Contrastingly, EM waves radiating from devices with a weak EM emission intensity may be below the background noise in the device's vicinity [21]. Therefore, these devices are potentially resistant to the threat of EM information leakage, and were not considered in previous studies [21], [22].

However, the electrical signal states and characteristics of the circuits change when information is processed inside the device (see Fig. 1). Therefore, if the changes in the device's electrical characteristics can be actively sensed using EM waves from outside the device, it is possible to obtain the same or additional information, which was captured from the radiated EM waves in previous studies. If active sensing is possible from outside the device, then attackers can control the distance (obtained information from the target device), depending on the intensity of the irradiated EM waves used for sensing. When such a threat is feasible, devices that were not targeted by conventional EM information leakage threats owing to the weak intensity of EM emission will also need countermeasures.

In this article, we define the threat of EM information leakage via "the signals generated by active sensing using irradiated EM waves (*Echo*)" as Echo TEMPEST and investigate the feasibility of the new threat against real devices.

The contributions of this article are as follows.

1) It is possible to obtain information using EM waves inside the device by actively sensing the changes in the electrical features that occur when processing the information inside the device.
2) The distance that can be obtained information from the target device can be controlled depending on the intensity of the irradiating EM waves used for active sensing.
3) Information can be obtained by actively sensing a device that is not targeted by the threat of conventional EM information leakage owing to the weak intensity of EM emission.

The rest of this article is organized as follows. Section II presents the electrical features, which contain the information transmitted from the device targeted by Echo TEMPEST, and the principle of capturing the electrical features. Section III presents the possibility of obtaining information from the device using the evaluation board with the extracted circuit to generate the *Echo*, based on the principle of Echo TEMPEST. Section IV validates Echo TEMPEST using real devices that have not been confirmed to obtain information using the conventional EM information leakage method. Furthermore, this section shows the possibility of controlling the distance, which can be obtained information from the device, depending on the intensity of the irradiated EM waves. Section V discusses countermeasure methods that focus on the conditions for executing Echo TEMPEST. Finally, Section VI concludes this article.

II. Electrical Features to be Measured for Executing Echo TEMPEST and Method for Obtaining Information by Active Sensing

This section describes the electrical features to be measured by active sensing to obtain transmitted information from the device. Additionally, a method for obtaining information from the *Echo* generated by active sensing of the electrical features from outside the device is described.

A. *Electrical Features to be Measured for Obtaining Information From the Device*

In previous studies, time-varying electrical signals, depending on the I/O information, had been considered as leakage sources. They judged the EM information leakage by capturing the radiated EM waves based on the mechanism shown in Fig. 2.

The I/O information of the device, which is the target of the EM information leakage, is processed inside the IC and then transmitted as electrical signals from the I/O circuit of the IC, as shown in Fig. 1. The I/O circuit of the IC is implemented with output buffers to match the current and voltage values between the ICs, synchronizing the timing of electrical signals to be transmitted and received, and improving the noise immunity [23], [24]. Therefore, the output signals are transmitted from the IC via the output buffer.

Focusing on the output buffer, because the switching state of the transistor inside the output buffer changes according to the output signal, "the input impedance of the output buffer measured from outside the IC (input impedance)" changes based on the value of the output signal. Based on the information being processed, there is change in the internal state of the active elements and the circuit in which the active elements are combined. These changes affect the input impedance and other electrical features. Therefore, if the attacker can measure these electrical features from outside the device by active sensing, the *Echo* generated inside the device is equivalent to the information in the radiated EM waves used by the conventional EM information leakage method.

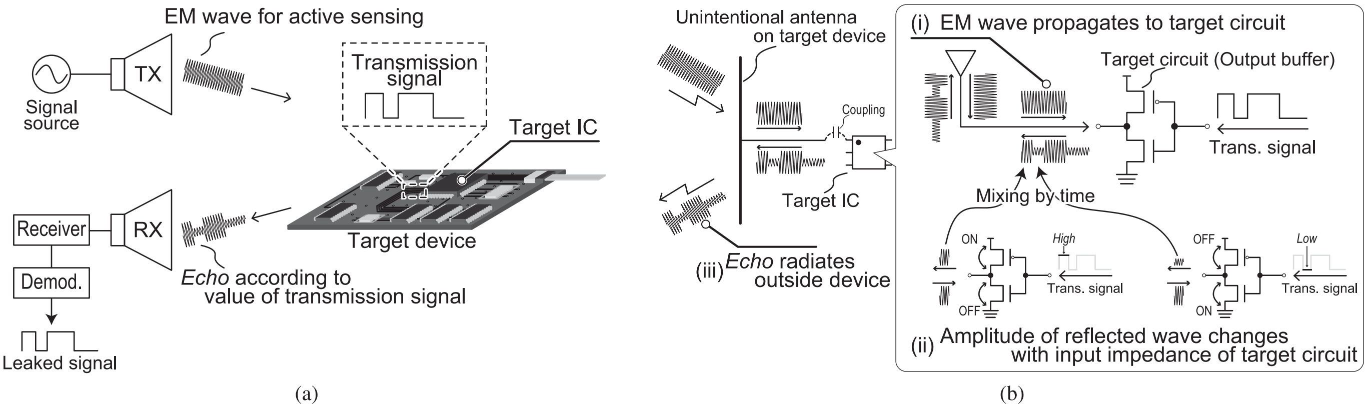

EM wave for active sensing
Signal source
TX
Transmission signal
Target IC
Receiver
RX
Demod.
Leaked signal
Target device
Echo according to value of transmission signal
(a)
Unintentional antenna on target device
Coupling
Target IC
(iii) Echo radiates outside device
(i) EM wave propagates to target circuit
Target circuit (Output buffer)
Trans. signal
Mixing by time
ON
OFF
High
Low
Trans. signal
(ii) Amplitude of reflected wave changes with input impedance of target circuit
(b)

Fig. 3. Conceptual diagram of Echo TEMPEST. (a) Flow of Echo TEMPEST. (b) Process of generating *Echo* by active sensing. (i) Irradiated EM waves propagate to the target circuit. (ii) Absorption and reflection of the propagated EM waves occur due to the change in input impedance value based on the transmitted signal from the target circuit. (iii) Amplitude-modulated (AM) waves generated by the time variation of the input impedance of the target circuit are radiated outside the device as *Echo*.

B. Principle of Echo TEMPEST

Fig. 3(a) shows the flow of Echo TEMPEST. The information is leaked by receiving the *Echo* generated by the device owing to the irradiated EM waves. The *Echo* generated by active sensing is caused by the device's unintentional antenna, which receives the irradiated EM waves from outside the device, and a circuit structure that absorbs and reflects the propagated EM waves inside the device [see Fig. 3(b)].

The EM waves irradiated from outside the device propagate inside the device through an unintentional antenna, such as cables connected to the device and traces on the PCB, and reach "the circuit that processes information that is the target of information leakage (target circuit)" [see Fig. 3(b)(i)]. The EM waves that propagate to the target circuit are partly absorbed into the circuit and partly reflected, depending on the value of the input impedance of the target circuit, which varies over time in accordance with the processed information [see Fig. 3(b)(ii)]. The reflected EM waves follow a path in the opposite direction to the incident waves and radiate outside the device as the *Echo*. Therefore, the *Echo* is generated as amplitude-modulated (AM) waves, with the irradiated EM waves as the carrier wave and the output signal of the target circuit as the modulated wave [see Fig. 3(b)(iii)]. Based on the abovementioned principle, the output state of the target circuit is contained in the *Echo*, and the IC's output information can be estimated by capturing and AM demodulating the radiated *Echo*.

Furthermore, the intensity of the *Echo* radiated from the target device depends on the intensity of the irradiated EM wave used for active sensing. It is possible to control the intensity of the radiated *Echo* by increasing the intensity of the irradiated EM waves to the range that the circuit comprising the output buffer of the I/O circuit can operate as usual.

III. Demonstration of Echo TEMPEST With a Simple Experimental System

In this section, we create an evaluation board that extracts the output buffers of the I/O circuits of the ICs, which is the target circuit for Echo TEMPEST. We measured the reflection of EM waves propagated from the target circuit with different amplitudes, depending on the value of the output signal of the target circuit. We then show that the information can be obtained based on the principle described in Section II.

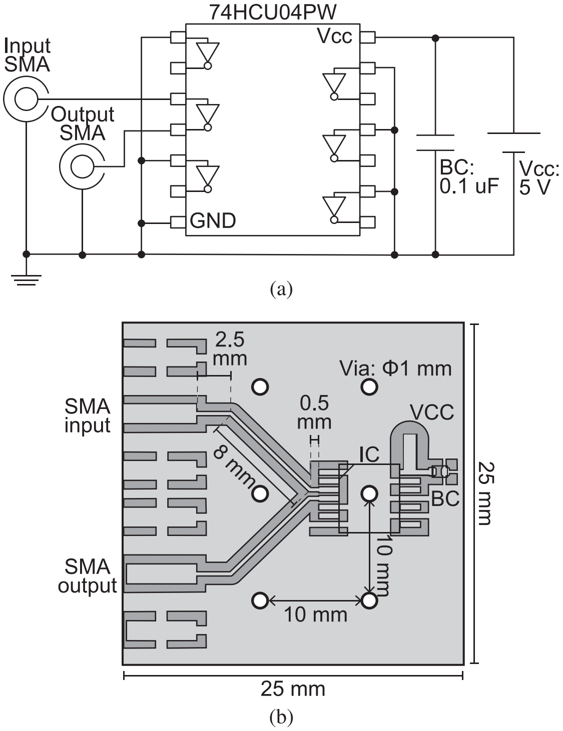


Fig. 4. Device under test (DUT) with the inverter element mounted. (a) Circuit diagram of the DUT. (b) Mounting layout of the DUT.

A. Evaluation Board Using an Inverter Element

This section describes the device under test (DUT) that implements an inverter element with a structure equivalent to the output buffer of the I/O circuit of the IC as the target circuit. Fig. 4 shows the circuit diagram and the mounting layout of the DUT.

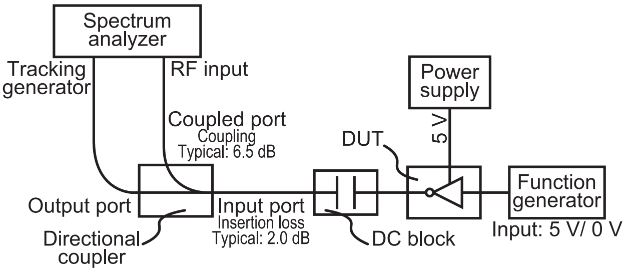


Fig. 5. Input impedance measurement setup based on the value of the inverter element's output signals.

TABLE I
MEASUREMENT SETUP AND PARAMETERS FOR DUT

Experiment equipment	
Spectrum analyzer	Rohde & Schwarz, FSV
Directional coupler	Mini-Circuits, ZFDC-6-23-S+
DC block	Mini-Circuits, BLK-18-S+
Stabilized power supply	Texio, PA18-2B
Function generator	NF, WF1968
DUT inverter IC	NXP, 74HCU04PW
DUT substrate	Sanhayato, No. 35R
Experimental parameters	
DUT input	0 / 5 V
RBW	1 MHz
Sweep points	32 001 points
Tracking generator output	–20 dBm
Frequency	20–2000 MHz

The circuit shown in Fig. 4(a) comprises an inverter element (NXP, 74HCU04PW) and a 0.1 μF bypass capacitor (BC). The SMA connectors were mounted as signal I/O terminals. The input ports of the inverter element not used in this experiment were grounded to the ground (GND).

Fig. 4(b) shows the mounting layout of the circuit shown in Fig. 4(a). The I/O ports of the inverter element were connected to the SMA connectors through the wiring with a trace width of 0.4 mm on the PCB using FR-4. The 1 mm diameter vias shared GNDs on both sides of the DUT. However, to measure the input impedance for a wide bandwidth based on the value of the output signals of the inverter element, the wire impedance was not matched the I/O impedance of the inverter element at a specific frequency.

B. Measurement of the Input Impedance Based on the Value of the Inverter Element's Output Signals

Fig. 5 and Table I show the measurement setup and parameters of the input impedance based on the value of the output signals of the inverter element.

In this experiment, a spectrum analyzer connected to a directional coupler and tracking generator were used as the measurement setup. The power supply of the DUT was stabilized power supply set at 5 V. The input and output of the DUT are connected to the function generator and input port of the directional coupler, respectively. A direct current (DC) block was inserted between the directional coupler and the DUT to prevent dc from DUT entering into the spectrum analyzer and tracking generator.

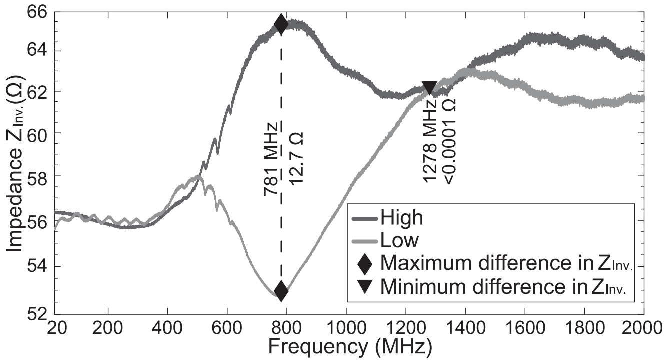


Fig. 6. Input impedance measurement result based on the output signal value of the inverter element. The input impedance values of the DUT are indicated as $Z_{\text{inv.}}$.

Next, the measurement parameters were explained. In this experiment, we used high (5 V) and low (0 V) inputs to the DUT to eliminate the transient response of the input impedance based on the value of the output signals of the inverter element. The measurement frequency range of the spectrum analyzer was set to 20–2000 MHz, according to the frequency range of the directional coupler. The spectrum analyzer and tracking generator's other parameters were set to 1 MHz RBW, 32 001 sweep points, and −20 dBm output.

The input impedance of the inverter element was calculated from the reflection coefficient, with the characteristic impedance of the measurement setup set at 50 Ω. In this experiment, the spectrum analyzer calibrated the directional coupler's input port before connecting the DUT to measure the reflected waves according to the value of the output signals of the inverter element. The responses were measured using the normalizing function of a spectrum analyzer to focus on the change in input impedance based on the value of the output signals of the inverter element.

The measurement results of the input impedance based on the value of the output signals of the inverter element are shown in Fig. 6. In Fig. 6, the input impedance values of DUT are denoted as $Z_{inv.}$. A maximum input impedance difference of 12.7 Ω was observed at 781 MHz, depending on the value of the output signals of the inverter element. Additionally, a minimum input impedance difference of less than 0.0001 Ω was observed at 1278 MHz.

C. Experimental Evaluation of Echo Generation According to Changes in Value of Inverter Element's Input Impedance

In this section, we demonstrate that a change in the input impedance generates an *Echo* based on the value of the output signals of the inverter element, and the transmitted information can be obtained. Fig. 7 and Table II show the measurement setup and parameters, respectively.

In this experiment, the EM waves generated by the signal generator were input into the output terminal of the DUT. The EM waves were propagated to the inverter element with low loss through coaxial cables. Furthermore, a spectrum analyzer measured the *Echo* through a directional coupler at the same

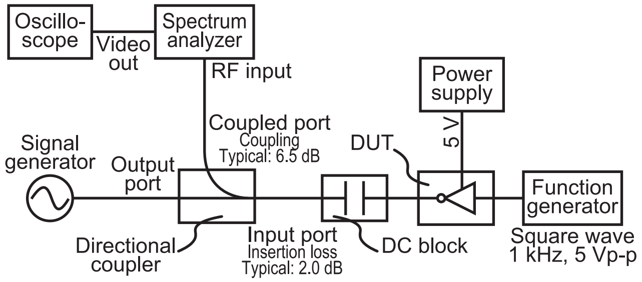
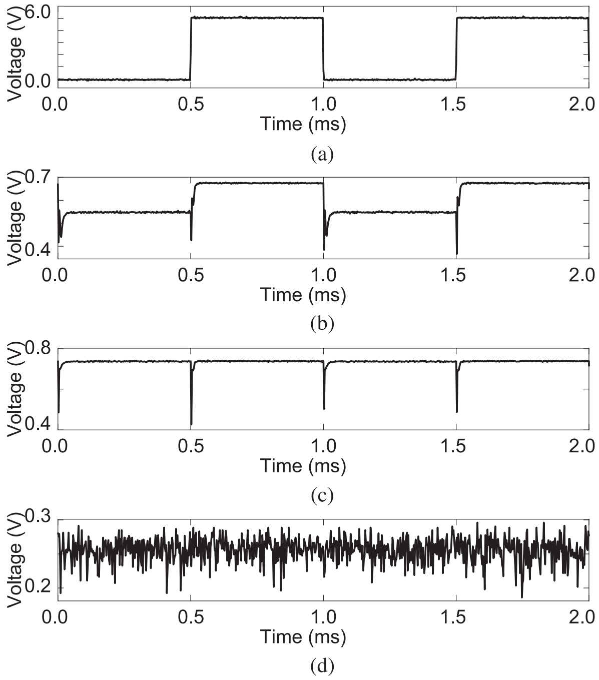


Fig. 7. *Echo* measurement setup generated by the change in the input impedance based on the output signal value of the inverter element.

TABLE II
EVALUATION SETUP AND PARAMETERS FOR TO VERIFY THE GENERATION OF *ECHO*

Experiment equipment	
Spectrum analyzer	Rohde & Schwarz, FSV
Directional coupler	Mini-Circuits, ZFDC-6-23-S+
DC block	Mini-Circuits, BLK-18-S+
Stabilized power supply	Texio, PA18-2B
Function generator	NF, WF1968
Signal generator	Keysight, N5181
DUT inverter IC	NXP, 74HCU04PW
DUT substrate	Sanhayato, No. 35R
Experimental parameters	
DUT input	1 kHz, 5 V_{p-p}, 2.5 V offset
RBW	5 MHz
Sweep points	32 001 points
Signal generator output	–30 dBm
Signal generator frequency	781 MHz 1278 MHz



(a)

(b)

(c)

(d)

Fig. 8. AM demodulated results of the measured *Echo* when EM waves were propagated to the output terminal of the DUT. (a) Waveform was output from the DUT. (b) AM demodulated waveform of the measured *Echo* when the EM waves with 781 MHz were propagated to the output terminal of the DUT. The waveform shows the amplitude of the *Echo* fluctuated according to the value of the inverter element's output signal. (c) AM demodulation waveform of the measured the *Echo* when EM waves with 1278 MHz propagated to the output terminal of the DUT. The waveform shows that the amplitude of the *Echo* did not fluctuate based on the output signal value of the inverter element. (d) *Echo* was not generated when 781 MHz was measured without propagating EM waves.

frequency as that of the propagated EM waves. The measured EM waves were AM demodulated using zero-span mode on a spectrum analyzer. The AM demodulated waveforms were input into the oscilloscope. The frequencies of the propagated EM waves were selected as 781 and 1278 MHz. These are the frequencies at which the input impedance difference, which is based on the value of the output signals of the inverter element, were the maximum and minimum in the previous section. At this time, 5 V_{p-p} square waves at 1 kHz were input to the input terminal of the DUT from a function generator.

Fig. 8 shows the output signal of the DUT, and the AM demodulation results that measured the *Echo* when EM waves with frequencies of 781 and 1278 MHz were propagated to the output terminal of the DUT. Fig. 8(a) shows the measured waveform of the output signal of the DUT, which is a 5 V_{p-p} square waves with 1 kHz. Fig. 8(b) shows the AM demodulation waveform of the measured *Echo* when EM waves with 781 MHz propagated to the DUT. It was confirmed that the amplitude of the *Echo* changes according to the high/low output signal of the inverter element. Fig. 8(c) shows the AM demodulation waveform of the measured *Echo* when EM waves with 1278 MHz propagated to the DUT. The amplitude remained constant, independent of the value of the output signal of the inverter element, and the amplitude fluctuation of the *Echo*, as shown in Fig. 8(b), was not observed. Fig. 8(d) shows the result at 781 MHz without propagating EM waves. This result indicates that *Echo* was not generated. In contrast, we also confirmed that the *Echo* was generated according to the DUT's output signal when the EM waves were propagated with other frequencies (approximately 510–1200 MHz) that had a difference in the input impedance in the previous section.

From these results, we confirmed that a change in the input impedance generates an *Echo* according to the value of the output signal of the inverter element. Therefore, we showed the possibility of obtaining transmitted information from the IC by propagating EM waves to the IC's output buffer, which has a circuit structure equivalent to that of the inverter element.

The falling signals measured at 0.5, 1.0, and 1.5 ms in Fig. 8(b) and (c) were due to the transient input impedance fluctuation caused by the timing of the changes in the inverter element's output signal. Thus, it is also possible to estimate the timing of the output signal change and the information transmitted from the falling signals. However, this section focuses on the amplitude fluctuation of the *Echo* caused by the input impedance change according to the value of the output signal of the inverter element evaluated in the previous section. Hence, we have excluded these fluctuations from our discussion.

IV. Evaluation of Echo TEMPEST Using Real Devices

This section demonstrates that Echo TEMPEST can be executed using real devices. First, we describe the method for obtaining information using active sensing. Subsequently, two

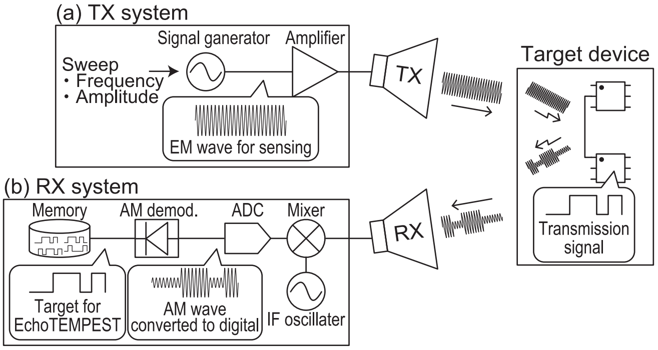


Fig. 9. Transmitter (TX)/receiver (RX) system to execute Echo TEMPEST. (a) TX system. A signal generator generates the EM waves while sweeping the frequency and amplitude, and the EM waves are irradiated through the TX antenna. (b) RX system receives the *Echo* radiated from the target device. The *Echo*, with the same frequency as the irradiated EM waves from the TX system, is received using the RX antenna and AM demodulated.

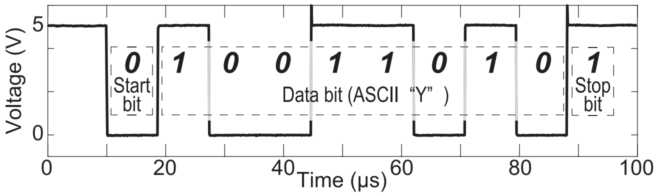


Fig. 10. Single-ended signal was measured by tapping the transmission line of the target UART modules. The voltage fluctuations corresponding to the 1-bit start bit, the 8-bit data bits with the least significant bit as the first bit, and the 1-bit stop bit were confirmed.

types of devices were used to demonstrate the feasibility of Echo TEMPEST and demonstrate that the distance, which can be obtained information from the device, can be controlled depending on the intensity of the irradiated EM waves used for active sensing.

A. Construction of a System to Obtain Information by Active Sensing

The system for obtaining information via active sensing requires transmitter (TX) and receiver (RX) systems. The system consists of a system that irradiates EM waves onto a device containing the target circuit and a system that receives and AM demodulates the *Echo* reflected from the target circuit. Fig. 9 shows the TX/RX system for executing Echo TEMPEST.

The frequency of the propagating EM waves with low loss to the target circuit inside the device is unknown. Therefore, in the TX system [see Fig. 9(a)], a signal generator is used to sweep the frequency and amplitude of the irradiating EM waves.

In the RX system [see Fig. 9(b)], the *Echo* generated by the target circuit and radiated outside the device is received and processed by software-defined radio (SDR). The signal input to the SDR was converted to an intermediate-frequency (IF) signal using a superheterodyne method. The converted signal is sampled by an analog-to-digital converter to the digital signal, and the digital signal is AM demodulated by envelope detection. We obtained the transmitted information of the target IC from the AM demodulated waveforms.

In this experiment, the TX/RX systems were controlled by a PC, which synchronizes the frequency to be obtained according to the sweep of the irradiating EM wave frequency. At this time, the SDR AM demodulates the *Echo* and obtains the amplitude of the AM demodulated waveform. Finally, we selected the frequency with the highest amplitude for the AM demodulated waveforms.

B. Target Signals of the Evaluated Devices

In this experiment, serial communication systems, which are generally targeted for EM information leakage, were used as evaluation targets. Devices that output single-ended signals and devices that output differential signals were used as devices with different signals transmitted from the IC among the serial communication methods. Specifically, universal asynchronous receiver/transmitter (UART) modules were used to transmit single-ended signals, and universal serial bus (USB) keyboards were used as devices transmitting differential signals.

1) UART Module: UARTs connect TX and RX devices with a transmission line; there is no clock (CLK) signal in the transmission line, and CLK is not shared between the TX and RX devices. Therefore, the baud rate is shared in advance to synchronize the bit timing between the TX and RX devices. The start and stop bits are added before and after the data bits indicate the start and end bits, respectively. The data bits were transmitted from the least significant bits of the data. Additionally, a parity bit can be inserted at the end of the data bits to detect data errors [25].

In this experiment, the transmission line between the UART modules was simplex to simplify the experimental target and connected by a signal line and a GND line with a length of 1 m cables. The bit parameters were 1 bit for the start bit, 8 bits for the data bits, and 1 bit for the stop bit, for a total of 10 bits as one frame. The baud rate was set to the generally used 115.2 kb/s. The voltage value on the transmission line was positive logic; high and idle states were set to 5 V, and low was set to 0 V.

Fig. 10 shows the waveform when "Y" was transmitted by the UART module used for the evaluation, as measured by an oscilloscope. The voltage fluctuations of "0100110101," including the start bit, data bits with the least significant bit as the first bit, and stop bit, were observed.

2) USB Keyboard: USB keyboards generally use a transmission rate of 1.5 Mb/s for USB 2.0 low-speed [26]. The transmission line of the USB keyboard consists of V_{BUS}, GND, and differential signals $\boldsymbol{D}+$ and $\boldsymbol{D}-$, where $\boldsymbol{D}-$ is connected to the power supply by a pull-up resistor.

When input information is transmitted from a USB keyboard to a PC, token packets are transmitted from the PC to the USB keyboard. Then, the input information is transmitted from a USB keyboard to a PC as data packets. Token packets contain an address depending on the device; therefore, a different address is added for each connection. These signals are transmitted in 1 ms cycles in units called frames, and the transmission signals are encoded in the NRZI format. After each packet, both $\boldsymbol{D}+$ and $\boldsymbol{D}-$ will have a low-transmission signal to indicate the end-of-packet (EOP).

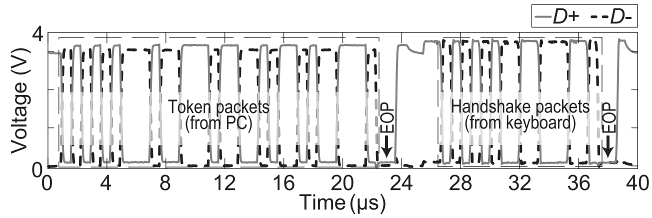


Fig. 11. Example of differential signals was measured by tapping the transmission line connecting a USB keyboard and a PC. The token packets transmitted from a PC and the handshake packets transmitted from the USB keyboard are surrounded by dashed rectangles.

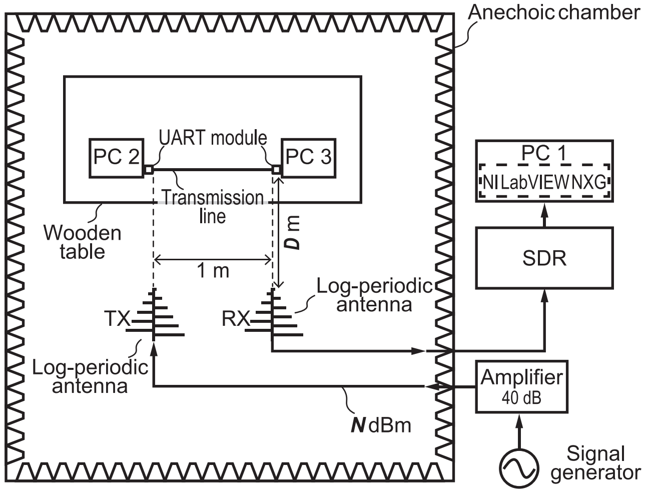


Fig. 12. Diagram of the setup used to evaluate Echo TEMPEST for the UART module.

In this experiment, there was no input to the USB keyboards to prevent invasion of the evaluation environment and to ensure reproducibility. The steady-state transmitted signals between a PC and a USB keyboard were used as evaluation targets. Fig. 11 shows an example of waveforms measured when a PC and a USB keyboard are connected without input. The dashed rectangles surround the token packets transmitted from a PC and handshake packets transmitted from a USB keyboard, as shown in Fig. 11. Handshake packets, such as data packets containing input information, are processed by the IC inside the keyboard and outputted through the I/O circuit. Therefore, if Echo TEMPEST can obtain the transmission signals representing the handshake packets, data packets, which are the USB keyboard input information, can be obtained.

C. Echo TEMPEST for UART Module

Fig. 12 shows a diagram of the experimental setup for the evaluation, and Table III lists the experimental setup and parameters used in the evaluation.

The UART modules to be evaluated were connected to the USB ports of two PCs placed on a 75 cm high wooden table in an anechoic chamber. Two log-periodic antennas were used for the TX/RX antennas. The TX/RX antennas were set at the same height as the transmission line of the UART modules. The distance between the antenna and the transmission line in Fig. 12 is defined as ***D*** m, representing 1, 2, and 3 m.

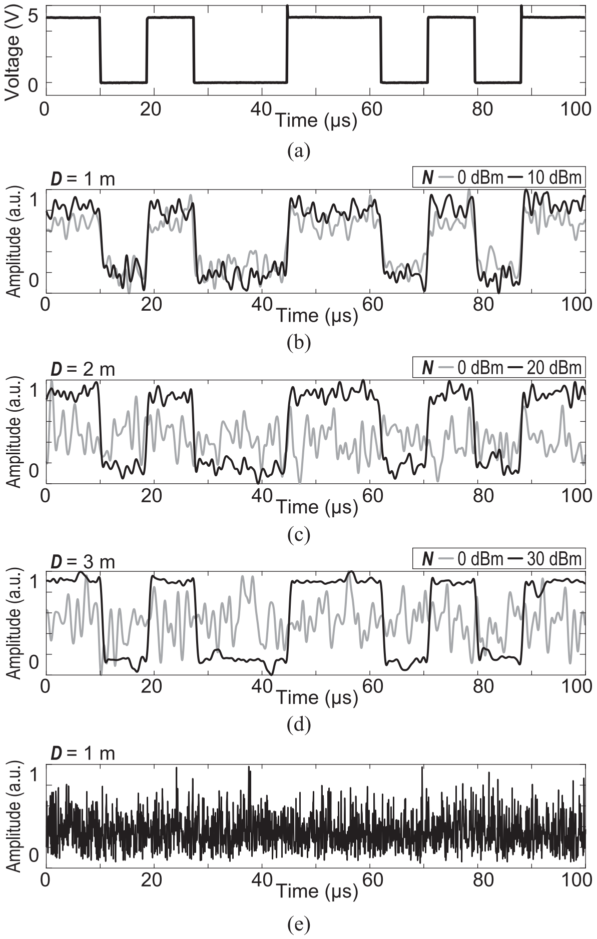
TABLE III
EVALUATION SETUP AND PARAMETERS FOR UART MODULE

Experiment equipment	
SDR	Ettus Research, USRP X310
SDR daughterboard	Ettus Research, TwinRX 10-6000 MHz
SDR control software	NI, LabVIEW NXG 5.0
Signal generator	Rohde & Schwarz, SMA100B
Amplifier	R&K, A000110-4040-R
TX / RX antenna	Ettus Research, LP0410
Experimental parameters	
SDR sampling rate	20 MS/s
Frequency	463 MHz
TX gain (***N***)	0–30 dBm
Distance (***D***)	1, 2, 3 m
SDR RX gain	60 dB

The EM waves generated by the signal generator are amplified by the amplifier and irradiated from the TX antenna to the UART module. The intensity of the EM waves was defined as ***N*** dBm and was changed from 0 to 30 dBm. The frequency of the EM waves varied from 300 to 1000 MHz. This frequency band indicates the frequency at which the wavelength is nearly equal to the length of the transmission line between the UART modules and the upper-frequency limit of the antennas. We selected 463 MHz as the frequency of the irradiating EM waves, where the amplitude of the AM demodulated waveform of the *Echo* was measured to be the largest in the advanced evaluation.

The *Echo*, generated by the UART module and radiated outside, was received and processed by the SDR with a fixed RX gain of 60 dB through the RX antenna. The sampling rate of the SDR was set to 20 MS/s, which is sufficiently higher than the UART baud rate according to the sampling theorem.

Fig. 13 shows the evaluation results of Echo TEMPEST for the UART module. Fig. 13(a) shows the waveform measured when the transmission line of the UART module was tapped with an oscilloscope when the "Y" ASCII code was transmitted. Fig. 13(b)–(d) shows the AM demodulated waveforms of the *Echo* measured at a distance of ***D*** m, and the EM waves with 463 MHz were irradiated at ***N*** dBm. Each waveform was normalized after applying a 400 kHz low-pass filter (LPF). Fig. 13(b) shows the results measured when the distance ***D*** was set to 1 m and the irradiation intensities ***N*** were set to 0 and 10 dBm. The voltage fluctuations shown in Fig. 13(a) were obtained at both irradiation intensities. Fig. 13(c) and (d) shows the results measured when distance ***D*** was set to 2 and 3 m, respectively. In both cases, when the irradiation intensity ***N*** of the EM waves was set to 0 dBm, the voltage fluctuations shown in Fig. 13(a) were not observed. However, voltage fluctuations were observed when the irradiation intensity ***N*** was increased to 20 or 30 dBm. Fig. 13(e) shows the leakage waveform measured using the conventional EM information leakage method without EM irradiation, and the distance ***D*** was set to 1 m. It was impossible to obtain the voltage fluctuation because of the weak intensity of the EM emission and the influence of the surrounding noise.



(a)

(b)

(c)

(d)

(e)

Fig. 13. Results of Echo TEMPEST evaluation for the UART module. (a) Waveform of the transmission signal indicating “Y” in the ASCII code transmitted from the UART module is shown as measured by an oscilloscope. (b)–(d) AM demodulation waveforms when the distances ***D*** were set to 1, 2, and 3 m, and the irradiation intensities ***N*** were changed from 0 to 30 dBm of the EM waves with 463 MHz. The waveform amplitudes were normalized after applying a 400 kHz low-pass filter (LPF). (b) Waveforms were obtained by AM demodulation of the *Echo* measured when the irradiation intensities ***N*** of the EM waves were set at 0 and 10 dBm. (c) and (d) Transmission signal could not be obtained when the irradiation intensity ***N*** of the EM waves was set at 0 dBm. However, by increasing the irradiation intensity ***N*** of the EM waves, the transmission signals were obtained when the distances ***D*** were changed. (e) Waveform was measured using the conventional EM information leakage method, with the distance ***D*** set to 1 m. The transmission signal could not be obtained.

From these results, we confirmed that Echo TEMPEST was feasible for the UART module, which is difficult to obtain using the conventional EM information leakage method, with a weak EM emission intensity. We also confirmed that the distance, which can be obtained information from the transmitted information from the device, can be controlled depending on the intensity of the EM irradiation. In this section, we only show the results when an ASCII code of “Y” was transmitted from the UART module; however, we also confirmed that Echo TEMPEST was feasible when different ASCII codes were transmitted in the same evaluation environment.

TABLE IV
USB Keyboards for Evaluation

No.	Manufacturer, Model name	Length of transmission line (***L***) [cm]
1	N/A, NBO109U01BK1	182
2	Lenovo, SK-8827	190
3	Lenovo, KU-1601	183
4	Penixx, PERIBOARD-106	175

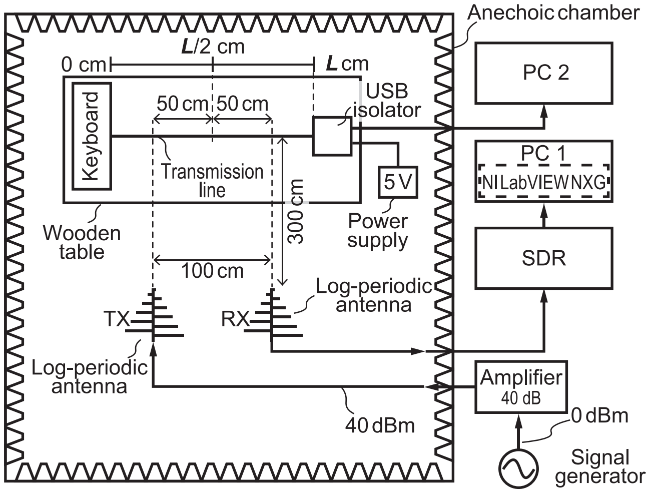


Fig. 14. Diagram of the setup used to evaluate Echo TEMPEST for USB keyboards.

TABLE V
Evaluation Setup and Parameters for USB Keyboards

Experiment equipment			
SDR			Ettus Research, USRP X310
SDR daughterboard			Ettus Research, TwinRX 10-6000 MHz
SDR control software			NI, LabVIEW NXG 5.0
Signal generator			Rohde & Schwarz, SMA100B
Amplifier			R&K, A000110-4040-R
TX / RX antenna			Ettus Research, LP0410
USB isolator			Analog Devices, EVAL-ADuM4160EBZ
Power supply			Texio, PA18-2B
Experimental parameters			
SDR sampling rate			20 MS/s
TX gain			40 dBm
Specific parameters for USB keyboard No. #	1	Frequency	922 MHz
		SDR RX gain	73 dB
	2	Frequency	546 MHz
		SDR RX gain	70 dB
	3	Frequency	867 MHz
		SDR RX gain	68 dB
	4	Frequency	699 MHz
		SDR RX gain	76 dB

D. Echo TEMPEST for USB Keyboards

This experiment demonstrates the feasibility of executing Echo TEMPEST for four models of USB keyboards that transmit differential signals. Table IV presents the USB keyboards. Fig. 14 and Table V show the setup and parameters used for the evaluation.

We used the same evaluation setup described in the previous section, with the TX/RX antennas placed 300 cm from the transmission line of the USB keyboard. The USB keyboard was connected to a PC outside the anechoic chamber using a USB isolator. The USB isolator reduces the influence of noise from the PC by separating the power and GND of the PC and keyboard, and the power of the keyboard is supplied from the stabilized power supply. The USB keyboard is connected to the USB isolator with a taut transmission line of length $\boldsymbol{L}$ (see Table IV). We selected the frequency of the irradiating EM waves, where the amplitude of the AM demodulated waveform of the measured *Echo* was the largest, by sweeping the frequency band of the antenna for each USB keyboard. In addition, the RX gain of the SDR was determined to automatically adjust the intensity such that the received signal was not saturated by the measurement program (see Table V).

Fig. 15 shows the evaluation results of Echo TEMPEST for the four different USB keyboards. Fig. 15 shows the following four types of waveforms for each USB keyboard.

(i) The waveforms were measured without input from a USB keyboard. The waveform was measured by tapping the measurement port on the USB isolator using an oscilloscope. As four USB keyboards were used, the token packets had different addresses.

(ii) The waveform was AM demodulated by the *Echo*. The waveform was AM demodulated by the *Echo* generated by the irradiated EM waves. The graph's vertical axis shows the normalized value after applying a 4 MHz LPF to the waveform.

(iii) The waveforms were reconstructed from the AM demodulated waveform according to the NRZI coding scheme. The waveforms were binarized by signal processing of the AM demodulated waveform obtained in (ii). Specifically, the waveforms were estimated from the extreme values of the differentiated AM demodulated waveform, focusing on *Echo* amplitude changes when the transmission signals change.

(iv) The waveform was measured using the conventional EM information leakage method, and the results of measuring EM waves radiated from a USB keyboard without EM wave irradiation.

Fig. 15(a)–(d) shows the evaluation results for USB keyboards No. 1–4 using the parameters in Table V. Fig. 15(a)(ii) and (b)(ii) indicates that the *Echo* containing token packets and handshake packets were measured. The AM demodulated waveforms were signal-processed, and the binarized results are shown in Fig. 15(a)(iii) and (b)(iii). We can see that the reconstructed waveforms have equivalent voltage fluctuations to the waveforms in Fig. 15(a)(i) and (b)(i). We confirmed that the *Echo* radiated with different amplitudes depending on the target circuit, which was the source of the transmitted signal, from Fig. 15(a)(ii) and (b)(ii).

The *Echo* is expected to contain token packets and handshake packets in Fig. 15(c)(ii) and (d)(ii), which are indicated by dashed lines. In both waveforms, the *Echo* corresponding to handshake packets was measured. Fig. 15(c)(iii) shows the reconstructed waveforms of the voltage fluctuations equivalent to handshake packets. However, in Fig. 15(d)(iii), we confirmed that the timing of the transmitted signals could not be reconstructed, and it was difficult to obtain this information. In Fig. 15(c)(ii) and (d)(ii), the amplitude fluctuations of the *Echo* corresponding to the token packets are small, making it difficult to reconstruct the transmitted signals.

Fig. 15(a)–(d)(iv) indicates that it is difficult to reconstruct the transmitted signals for all the USB keyboards from the measured waveforms using the conventional EM information leakage method.

The abovementioned results show that Echo TEMPEST could execute on USB keyboards, which did not confirm information leakage using the conventional EM information leakage method, by active sensing through EM wave irradiation. Echo TEMPEST showed that it is possible to obtain handshake packets generated by the same process as the keyboard input information.

We confirmed the differences in the amplitude of the information contained in the *Echo* depending on the target circuit outputting the transmission signals [see Fig. 15(a)–(c)]. However, the device was found to have difficulty reconstructing the transmission signals, even when using the proposed method [see Fig. 15(d)]. This may be due to the small difference in the input impedance value depending on the value of the output signal of the target circuit, resulting in smaller amplitude fluctuations of the generated *Echo*. Furthermore, the transfer function between the TX/RX antennas and the target device's target circuit affects the EM waves. Therefore, the irradiated EM waves and the radiated *Echo* were attenuated during propagation between the TX/RX antenna and the target circuit, and were influenced by background noise. Therefore, it is difficult to reconstruct the information in transmitted signals.

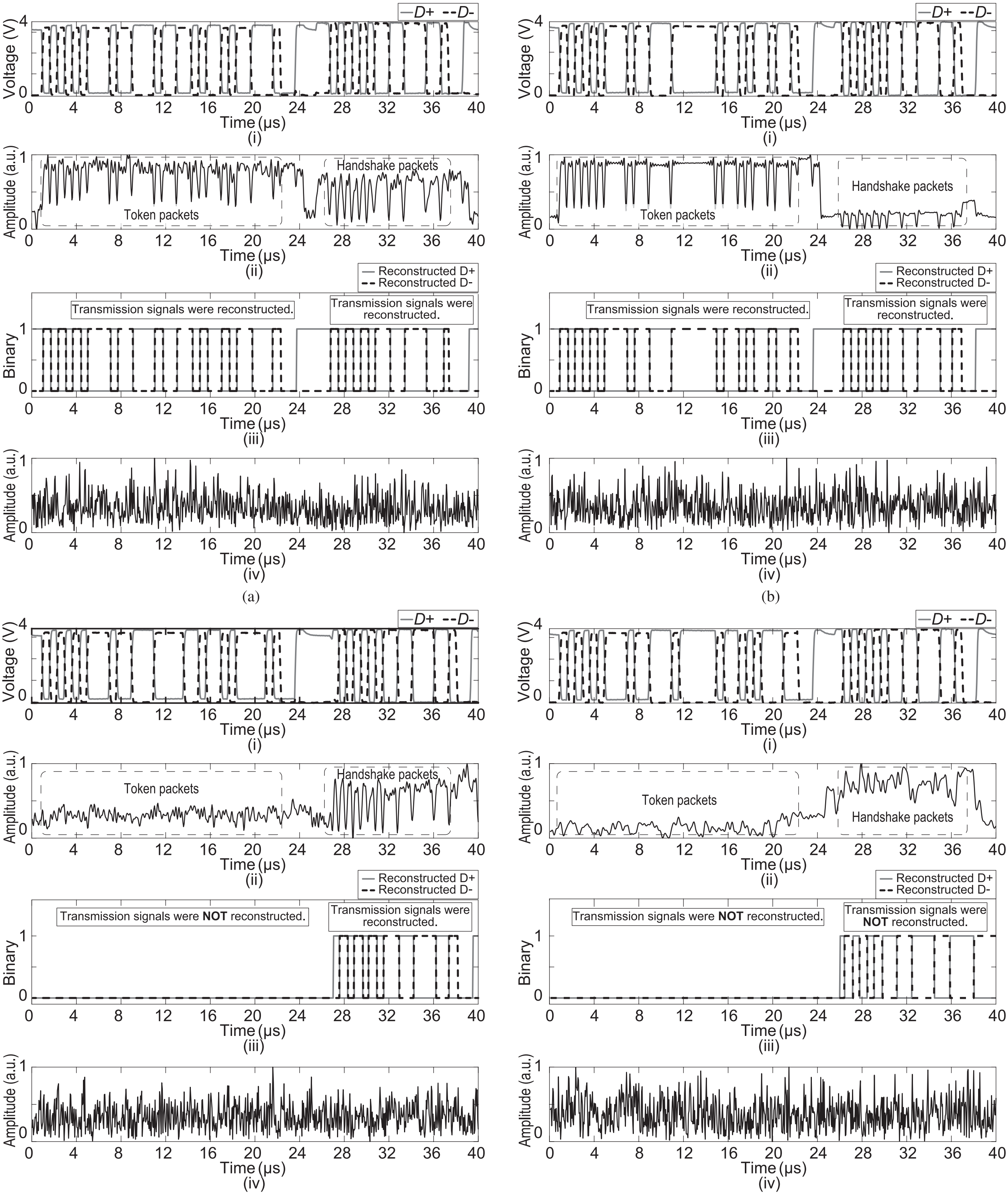
V. Countermeasure Methods Against Echo TEMPEST

The countermeasures against Echo TEMPEST proposed in this article include two types: methods that make it difficult to obtain the *Echo* and methods that make it difficult to reconstruct information from the *Echo*.

A. *Methods that Make it Difficult to Obtain the Echo*

It is necessary to propagate EM waves to the target circuit to execute Echo TEMPEST. Thus, an attacker irradiates EM waves with an intensity stronger than the background noise around the target device, and measures the *Echo* generated by the target device. Therefore, the following methods are considered practical: detecting irradiated EM waves, attenuating EM waves propagating to the target circuit, and attenuating the intensity of the radiated *Echo* generated by the target device.

Methods for detecting irradiated EM waves have also been reported. A method of detection by measuring the power supply voltage on the FPGA that fluctuates owing to the irradiated EM waves [27], a method of detection by measurement of the frequency and phase synchronization gap between the reference CLK and the FPGA's CLK [28], a method of detection by analysis of the abnormal operation log of the system caused by interference with transmission signals [29], and a method of detection by measurement using hardware consisting of SDRs and/or discrete components [30], [31]. These methods can detect



(a)

(b)

(c)

(d)

Fig. 15. Evaluation results of Echo TEMPEST for USB keyboards. (a) USB keyboard No. 1. (b) USB keyboard No. 2. (c) USB keyboard No. 3. (d) USB keyboard No. 4. (a)–(d) Following four waveforms are shown for each USB keyboard. (i) Waveforms were measured by an oscilloscope without input. (ii) AM demodulated waveform of the measured *Echo* by active sensing. The amplitudes of the AM demodulation waveforms were normalized after applying a 4 MHz LPF. (iii) Waveforms were reconstructed from the extreme values of the differentiated AM demodulated waveform, focusing on the amplitude of the radiating *Echo* corresponding to the change in the transmission signals. (iv) Measured waveform of the EM waves radiated from a USB keyboard without the irradiated EM waves.

the irradiated EM wave, which is the first stage of Echo TEMPEST, and interrupt the transmission process of the information, making it more difficult for an attacker to obtain the *Echo*.

In addition, improving the immunity of the device and attenuating the radiated EM waves can be countermeasures, focusing on the propagation of the EM waves to the target circuit and the measurement of the *Echo* radiated from the device. As shown in Fig. 15(d)(ii), if the amplitude of the *Echo* radiated from the device is small, it is difficult for the attacker to reconstruct the information because of background noise. Therefore, methods to make it more difficult to obtain the *Echo* using conventional EM information leakage countermeasure methods, such as shielding enclosures, buildings, and connecting lines [32], [33], zoning [32], [34], [35], and jamming using noise [36], may be applied to Echo TEMPEST.

B. Methods that Make it Difficult to Reconstruct Information From the Echo

The transmitted signals of the devices used for evaluation in this article or potential Echo TEMPEST targets were not encrypted. Altogether, information leaks when *Echo* occurs, corresponding to transmission signals. In contrast, encrypting the transmission signals may protect the information, even if it is leaked through the *Echo*. However, transmission signal encryption must be implemented at the device design stage, and specifications and standards must be standardized among the ICs and devices that transmit and receive information. Therefore, it is difficult to apply this countermeasure method to a system that has already been manufactured or is in operation.

VI. Conclusion

This article demonstrates the feasibility of Echo TEMPEST, which measures electrical changes in the information transmission process by irradiating EM waves that cause information leakage. Specifically, we focused on the input impedance of the target circuit when the information processing inside the IC was transmitted through the I/O circuit. We then investigated a method to estimate the transmitted information from the amplitude fluctuation of the *Echo* generated by the reflection and absorption of the irradiated EM wave.

In this article, we confirmed that the change in the input impedance generated an *Echo* according to the value of the transmitted signals using the DUT implemented with an inverter element that has the same structure as the output buffer of the I/O circuit of the IC. Then, we demonstrated the feasibility of Echo TEMPEST using the UART modules that output single-ended signals and USB keyboards that output differential signals. Moreover, we demonstrated that the distances obtained information from the transmitted signals could be controlled depending on the intensity of the irradiated EM waves using the UART modules. We also confirmed that transmitted information could be obtained by executing Echo TEMPEST on devices that are not confirmed to leak using the conventional EM information leakage method. Finally, we discussed the countermeasure methods that focused on the difficulty of obtaining and reconstructing information from the *Echo*.

This article targeted a device in which information is transmitted on a single line. Whether the threat can be executed for a device in which information is divided into multiple lines is a future topic. Furthermore, if the coupling between the TX/RX antennas is high or if the RX antenna is affected by the multipath of the irradiated EM waves, it may be difficult to obtain the amplitude fluctuations from the *Echo* depending on the dynamic range of the receiver. Another future topic is to verify the feasibility of Echo TEMPEST in such environments.

References

[1] Joint Task Force, “Security and privacy controls for information systems and organizations,” National Institute of Standards and Technology, NIST Special Publication 800-53 Revision 5, Sep. 2020. Accessed: Oct. 1, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[2] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Hoboken, NJ, USA: Wiley, 2008.

[3] M. G. Kuhn and R. J. Anderson, “Soft tempest: Hidden data transmission using electromagnetic emanations,” in *Information Hiding*, D. Aucsmith, Ed., vol. 1525. Berlin, Germany: Springer, 1998, pp. 124–142.

[4] Internet Security Glossary, “IETF RFC 2828,” May 2000. Accessed: Oct. 1, 2022. [Online]. Available: https://www.ietf.org/rfc/rfc2828.txt

[5] M. G. Kuhn, “Compromising emanations of LCD TV sets,” *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 3, pp. 564–570, Jun. 2013.

[6] H. S. Lee, D. H. Choi, K. Sim, and J.-G. Yook, “Information recovery using electromagnetic emanations from display devices under realistic environment,” *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 4, pp. 1098–1106, Aug. 2019.

[7] P. de Meulemeester, B. Scheers, and G. A. E. Vandenbosch, “Eavesdropping a (ultra-) high-definition video display from an 80 meter distance under realistic circumstances,” in *Proc. IEEE Int. Symp. Electromagn. Compat. Signal/Power Integrity*, 2020, pp. 517–522.

[8] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone, “A threat for tablet PCs in public space: Remote visualization of screen images using EM emanation,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2014, pp. 954–965.

[9] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, and M. Hattori, “Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer,” in *Proc. 17th Int. Zurich Symp. Electromagn. Compat.*, 2006, pp. 630–633.

[10] N. Zhang, Y. Lu, Q. Cui, and Y. Wang, “Investigation of unintentional video emanations from a VGA connector in the desktop computers,” *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 6, pp. 1826–1834, Dec. 2017.

[11] M. Vuagnoux and S. Pasini, “Compromising electromagnetic emanations of wired and wireless keyboards,” in *Proc. USENIX Secur. Symp.*, vol. 1, 2009, pp. 1–16.

[12] D.-J. Sim, H. S. Lee, J.-G. Yook, and K. Sim, “Measurement and analysis of the compromising electromagnetic emanations from USB keyboard,” in *Proc. Asia-Pacific Int. Symp. Electromagn. Compat.*, 2016, vol. 1, pp. 518–520.

[13] J. Choi, H.-Y. Yang, and D.-H. Cho, “TEMPEST comeback: A realistic audio eavesdropping threat on mixed-signal SoCs,” in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2020, pp. 1085–1101.

[14] W. van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?,” *Comput. Secur.*, vol. 4, no. 4, pp. 269–286, Dec. 1985.

[15] C. R. Paul, *Introduction to Electromagnetic Compatibility*. Hoboken, NJ, USA: Wiley, 2006.

[16] H. W. Ott, *Electromagnetic Compatibility Engineering*. Hoboken, NJ, USA: Wiley, 2011.

[17] F. Elibol, U. Sarac, and I. Erer, “Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system,” in *Proc. 20th Eur. Signal Process. Conf.*, 2012, pp. 1767–1771.

[18] Y. Hayashi, N. Homma, Y. Toriumi, K. Takaya, and T. Aoki, “Remote visualization of screen images using a pseudo-antenna that blends into the mobile environment,” *IEEE Trans. Electromagn. Compat.*, vol. 59, no. 1, pp. 24–33, Feb. 2017.

[19] P. Juyal, S. Adibelli, N. Sehatbakhsh, and A. Zajic, "A directive antenna based on conducting disks for detecting unintentional EM emissions at large distances," *IEEE Trans. Antennas Propag.*, vol. 66, no. 12, pp. 6751–6761, Dec. 2018.

[20] H. Sekiguchi and S. Seto, "Study on maximum receivable distance for radiated emission of information technology equipment causing information leakage," *IEEE Trans. Electromagn. Compat.*, vol. 55, no. 3, pp. 547–554, Jun. 2013.

[21] V. Yli-Mäyry, D. Miyata, N. Homma, Y. Hayashi, and T. Aoki, "Statistical test methodology for evaluating electromagnetic information leakage from mobile touchscreen devices," *IEEE Trans. Electromagn. Compat.*, vol. 61, no. 4, pp. 1107–1114, Aug. 2019.

[22] T.-L. Song, Y.-R. Jeong, and J.-G. Yook, "Modeling of leaked digital video signal and information recovery rate as a function of SNR," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 2, pp. 164–172, Apr. 2015.

[23] S.-M. Kang and Y. Leblebici, *CMOS Digital Integrated Circuits Analysis & Design*, 4th ed. New York, NY, USA: McGraw-Hill, 2002.

[24] J. M. Rabaey, *Digital Integrated Circuits: A Design Perspective*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1996, pp. 135–167.

[25] U. Nanda and S. K. Pattnaik, "Universal asynchronous receiver and transmitter (UART)," in *Proc. 3rd Int. Conf. Adv. Comput. Commun. Syst.*, vol. 1, 2016, pp. 1–5.

[26] USB Implementers Forum, "Universal serial bus specification revision 2.0," Apr. 2000. Accessed: Oct. 1, 2022. [Online]. Available: https://www.usb.org/document-library/usb-20-specification

[27] D. Fujimoto, Y.-I. Hayashi, A. Beckers, J. Balasch, B. Gierlichs, and I. Verbauwhede, "Detection of IEMI fault injection using voltage monitor constructed with fully digital circuit," in *Proc. IEEE Int. Symp. Electromagn. Compat. IEEE Asia-Pacific Symp. Electromagn. Compat.*, 2018, pp. 753–755.

[28] N. Miura et al., "PLL to the rescue: A novel EM fault countermeasure," in *Proc. 53rd ACM/EDAC/IEEE Des. Automat. Conf.*, 2016, pp. 1–6.

[29] C. Kasmi et al., "Event logs generated by an operating system running on a COTS computer during IEMI exposure," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 6, pp. 1723–1726, Dec. 2014.

[30] J. F. Dawson et al., "A cost-efficient system for detecting an intentional electromagnetic interference (IEMI) attack," in *Proc. Int. Symp. Electromagn. Compat.*, 2014, pp. 1252–1256.

[31] A. K. Bellamkonda, P. H. Rao, and S. Saxena, "Intentional electromagnetic interference reception in 0.5–2.0 GHz," *IEEE Trans. Electromagn. Compat.*, vol. 64, no. 6, pp. 2163–2169, Dec. 2022.

[32] ITU, "K.115: Mitigation methods against electromagnetic security threats," Nov. 2015. Accessed: Oct. 1, 2022. [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12664&lang=en

[33] V. Bîndar, M. Popescu, and A. Vulpe, "Considerations regarding shielding effectiveness and testing of electromagnetic protected enclosures used in communications security," in *Proc. 10th Int. Conf. Commun.*, 2014, pp. 1–6.

[34] H. Sekiguchi and S. Seto, "Estimation of receivable distance for radiated disturbance containing information signal from information technology equipment," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, 2011, pp. 942–945.

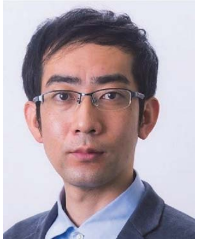
[35] V. Bîndar, M. Popescu, and R. Craciunescu, "Aspects of electromagnetic compatibility as a support for communication security based on TEMPEST evaluation," in *Proc. 10th Int. Conf. Commun.*, 2014, pp. 1–4.

[36] T.-L. Song, Y.-R. Jeong, H.-S. Jo, and J.-G. Yook, "Noise-jamming effect as a countermeasure against TEMPEST during high-speed signaling," *IEEE Trans. Electromagn. Compat.*, vol. 57, no. 6, pp. 1491–1500, Dec. 2015.

Shugo Kaji (Student Member, IEEE) received the B.E. degree in engineering from Toyohashi University of Technology, Toyohashi, Japan, in 2017 and the M.E. degree in engineering in 2019 from Nara Institute of Science and Technology, Ikoma, Japan, where he is currently working toward the Ph.D. degree in engineering.

His research interests include electromagnetic information security, electromagnetic compatibility, and hardware security.

Mr. Kaji is a student member of the Institute of Electronics, Information and Communication Engineers.



Daisuke Fujimoto (Senior Member, IEEE) received the B.E., M.E., and Ph.D. degrees in engineering from Kobe University, Kobe, Japan, in 2009, 2011, and 2014, respectively.

He is currently an Assistant Professor with the Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma, Japan. He is also a visiting Assistant Professor with the Institute of Advanced Sciences, Yokohama National University. His research interests include hardware security and implementation of security cores.

Dr. Fujimoto is a member of Institute of Electronics, Information, and Communication Engineers.

Masahiro Kinugawa (Member, IEEE) received the B.E. and M.S. degrees in computer science and engineering from Aizu University, Aizu Wakamatsu, Japan, in 2004 and 2006, respectively, and the M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2010 and 2013, respectively.

He is currently an Associate Professor with the University of Fukuchiyama, Fukuchiyama, Japan. His research interests include electromagnetic compatibility, information system security, and electromagnetic information security.

Dr. Kinugawa is a member of the Institute of Electronics, Information and Communication Engineers.

Yuichi Hayashi (Senior Member, IEEE) received the M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2005 and 2009, respectively.

He is currently a Professor with the Nara Institute of Science and Technology, Ikoma, Japan. His research interests include electromagnetic compatibility and information security.

Dr. Hayashi was a recipient of many awards and honors, including the IEEE Electromagnetic Compatibility Society Technical Achievement Award, IEEE International Symposium on EMC Best Symposium Paper Award, and Workshop on Cryptographic Hardware and Embedded Systems Best Paper Award. He is the Chair of Electromagnetic Information Leakage Subcommittee in IEEE EMC Technical Committee 5.