Introduction to Electromagnetic Information Security

doi: 10.1587/transcom.2018EBI0001

IEICE TRANSACTIONS

on Communications

DOI:10.1587/transcom.2018EBI0001

Publicized:2018/08/17

A PUBLICATION OF THE COMMUNICATIONS SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3chome, Minato-ku, TOKYO, 105-0011 JAPAN

INPUT THE TYPE OF MANUSCRIPT

Introduction to Electromagnetic Information Security

Yu-ichi Hayashi[†], ***Regular and*** **Naofumi Homma**[††], ***Regular***

SUMMARY With the rising importance of information security, the necessity of implementing better security measures in the physical layer as well as the upper layers is becoming increasing apparent. Given the development of more accurate and less expensive measurement devices, high-performance computers, and larger storage devices, the threat of advanced attacks at the physical level has expanded from the military and governmental spheres to commercial products. In this paper, we review the issue of information security degradation through electromagnetic (EM)-based compromising of security measures in the physical layer (i.e., EM information security). Owing to the invisibility of EM radiation, such attacks can be serious threats. We first introduce the mechanism of information leakage through EM radiation and interference and then present possible countermeasures. Finally, we explain the latest research and standardization trends related to EM information security.

Key words: *EM information security, TEMPEST, Side-channel attacks, Fault analysis, Hardware Trojan horse, Electromagnetic compatibility*

1. Introduction

Today's "information society" owes its existence to rapid advancements in the information and communications technology (ICT) field and the proliferation of personal ICT devices. An important requirement for such a society is to ensure information security, including the protection of individual privacy and the establishment of secure e-commerce channels. Information security can be roughly divided into three elements: confidentiality, integrity, and availability. These elements should be implemented longitudinally from the application layer to the physical layer; if they are not ensured across these layers, reliability and security will be degraded significantly, as each layer in an ICT device works under the assumption that information coming from the lower layers can be trusted. Because any vulnerability of hardware at the physical layer can critically decrease its security, ensuring the security of the physical layer is a vital issue for ICT devices.

In this paper, we focus on electromagnetic (EM) information security, a major component of information security at the physical layer. In particular, we focus on the issue of information leakage through electromagnetic (EM) waves, motivated by the serious threat such leakage represents in terms of its potential to degrade mobile ICT device in a non-traceable and undetectable manner.

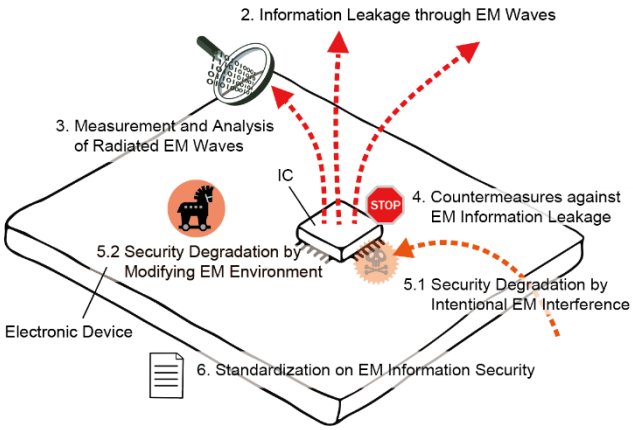


Fig. 1 Overview of EM information security issues addressed in this paper.

The problem of information leakage through EM emanation has been studied in a military context since the 1950s. This research approach is often referred to as TEMPEST, which is a codename for techniques and standards to suppress emissions that can compromise security. In the context of TEMPEST research, EM emissions from ICT devices are defined as "unintentional intelligence-bearing signals," which, if intercepted and analyzed can disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment [1].

TEMPEST research includes, among other factors, technologies for suppressing unnecessary signals from ICT devices and the underlying causes of EM emanation. In its early stages, technology for performing TEMPEST-related attacks required expensive and difficult-to-obtain equipment for monitoring EM emanation. In addition, the security community held the belief that such highly sophisticated monitoring was possible only in the case of government-level attacks.

In 1985, van Eck reported that the execution of TEMPEST attacks was no longer limited to governments and the military by showing that such attacks can be conducted by virtually anyone [2]. He demonstrated that unintentional EM emanations from a cathode-ray tube (CRT) display could be captured by specially designed devices and used to quickly reconstruct the state of the display. Following this seminal work, TEMPEST-related research such as studies on the acquisition of EM emanations and information extraction began to appear in academic papers and

† The author is with Nara Institute of Science and Technology 8916-5 Takayama, Ikoma, NARA 630-0192, Japan
†† The author is with Research Institute of Electrical Communication Tohoku University, 2-1-1 Katahira, Aoba-ku, Sendai 980-8577, JAPAN

inspired active discussion.

In the 1990s, the risk of information leakage via EM emanation increased as computers became faster and less expensive [3]. Emerging analysis techniques exploited advanced signal processing and statistical techniques using substantial amounts of CPU time and memory. At present, ICT devices prone to TEMPEST attacks include many commercial products that handle private and valuable data, including CRT and LCD monitors [4-13], touch screen monitors [14], printers [15], keyboards [16-19], central processing units (CPUs) [20], and cryptographic modules [21–28].

In this survey paper on the field of EM information security, we discuss the threats and mechanisms of information leakage through EM waves that can be used to compromise commercial devices and equipment and then describe the latest research and standardization trends for countering or deterring these threats. The remainder of this paper is organized as follows (Fig. 1). Section 2 briefly describes the mechanism of information leakage through EM waves unintentionally emitted from ICT devices. Section 3 describes the measurement environment of EM waves and the process of recovering information from their measurement. Section 4 describes countermeasures against both unintentional emanation and monitoring. In Section 5, we describe threats that degrade the confidentiality and integrity of devices as a result of EM interference, a phenomenon that represents the inverse of EM leakage and is known as the reciprocity theorem for electromagnetic fields. We also outline threats that increase EM emissions from devices by intentionally changing the circuit design, thereby causing security degradation. Section 6 presents works relating to the standardization of EM information security. Finally, in Section 7 we provide concluding remarks.

2. Information Leakage through EM Waves

EM information leakage is primarily caused by EM radiation arising from the time variation in generated/transmitted electrical signals produced by data processing within ICT devices (Fig. 2). In general, the level of EM radiation generated by an ICT device is regulated from the standpoint of EM compatibility (EMC). However, as the information leakage through EM radiation corresponds to the wave frequency pattern, such leakage can occur even if the intensity of the EM radiation is less than the standard regulation value.

Fig. 3 shows how information leaks occur through EM radiation. An integrated circuit (IC) processing data can act as a leakage source [29] if it produces a signal that includes information with frequency components corresponding to the time variation rate. Higher-frequency components are often propagated through EM coupling to device components that behave as an antenna [30], resulting in spatial radiation of the leakage following the frequency characteristics of the antenna [31,32].

Such antennas can be in the form of a wiring pattern on a printed circuit board (PCB), a conductor constituting a device chassis, or a line connected to the device. EM radiation is usually generated through such unintentional antennas.

Information included in a radiated EM wave can be extracted using a leakage model. An example of a leakage model for a display would involve EM radiation from an IC that serially processes data on the basis of screen drawing or from a path that transmits displayed image data. Based on the physical characteristics of the device, the frequency and periodicity of observed meaningful EM waves can therefore be determined.

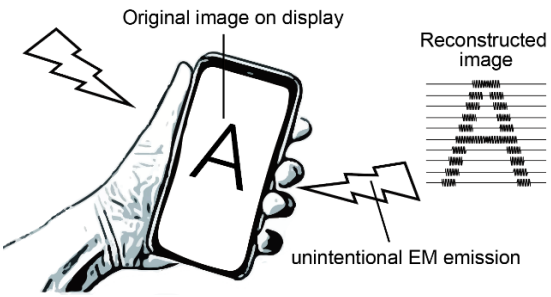


Fig. 2 EM information leakage from ICT device

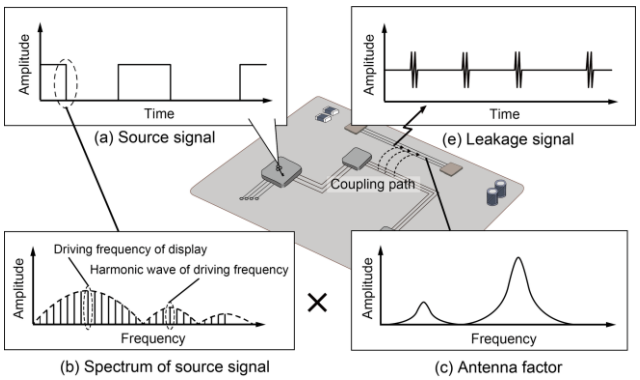


Fig. 3 Model of leakage of ICT device via EM field

3. Measurement and Analysis of Radiated EM Waves

Information acquisition from radiated EM waves comprises two components: (i) measurement of radiated EM waves and the information contained therein, and (ii) analysis of measured EM waves. In this section, we first describe the environment (i.e., setup) for measuring radiated EM waves and then classify analysis methods based on their respective observation times. Finally, we describe analysis methods performed following EM wave measurement.

3.1 Measurement of Radiated EM Waves

Radiated EM waves are measured either in the time or frequency domains. For these measurements, it is necessary to appropriately set various parameters related to measurement such as bandwidth, sampling speed, trigger, frequency band, observation period, etc. In addition, because procedures and interfaces for parameter setting differ considerably by measurement device, and the operation of each device requires expert knowledge, it is difficult to develop common or shared operations.

However, in recent years, application programming interfaces (APIs) and software development toolkits have been developed to enable common operability among many measurement devices. Using such APIs and libraries based on high-level languages, it is possible to overcome the issue of differences among measurement devices in developing a unified software that can control a variety of devices.

For example, it is possible to set up measurement parameters for using a software-defined radio (SDR) as a measuring device via software development toolkits such as GNU Radio [33] or MATLAB [34] without consideration of the details of physical measurement. Such software can also control signal processing and transmission procedures such as the signal modulation used in measurement. In this manner, the hardware configuration used for attacks can be easily reconfigured to allow an attacker to measure radiated EM waves by downloading and running a program that analyzes the differences among signals produced by different devices.

In addition to device control, the assumption of a common measurement environment allows for the use of various measurement parameters without the need for direct parameter estimation; in such cases, attackers (hobbyists) can collaborate with other attackers by using network computational resources to extract appropriate parameter values in an exhaustive (i.e., brute force) manner. In other words, attackers do not require professional knowledge and skills because appropriate parameter values are available online (Fig. 4).

As an example, we look at the case of smart devices (e.g., smart phones) as targets of attack via radiated EM waves. Because such products have common models that are widely marketed worldwide, the necessary parameters for an attack can be estimated, published, and shared. The availability of shared parameter-estimation programs on the network means that attacks on the physical layer of devices using their EM radiation patterns can be executed in a manner similar to attacks executed in cyberspace.

3.2 Information Acquisition from Measured EM Waves

This subsection presents an overview of information acquisition processes based on the interception of EM radiation. During operation, an electronic device will generate and emit radio signals that often contain encoded information as a result of the electrical switching processes occurring in its digital circuitry. This can occur even when the

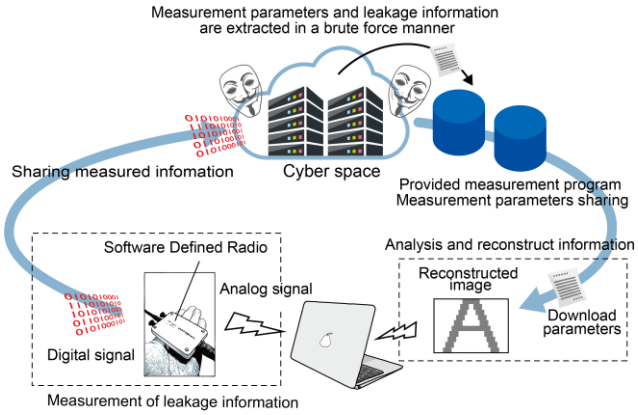


Fig. 4 Parameter extraction by exhaustive search

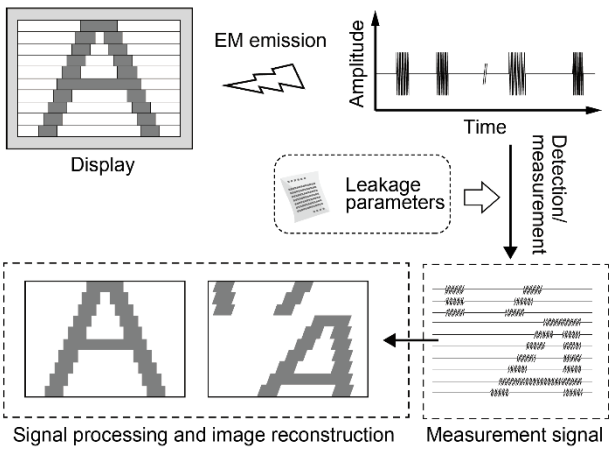


Fig. 5 Information acquisition based on single observation

emitted signal is suppressed in accordance with EMC standards. The intermediate or final results of device operation can be acquired from such EM emission signals; two typical methods for doing so are discussed as follows.

3.2.1 Information Acquisition Based on Single Observation

This method involves the acquisition of one or more EM signals emitted during a target operation. Following acquisition, the attacker attempts to extract the desired information directly from the EM trace. Although this method requires detailed knowledge regarding the implementation of the target device, it is feasible even if only one or a few traces are available.

For example, this method can be used to acquire information directly from a monitor or keyboard. The color and

contrast of pixels in a monitor are represented as combinations of red-green-blue (RGB) voltage signals that change continuously as the image changes on the screen. Fig. 5 shows an image of a display connected to a display controller. When black characters are displayed on a white background, the voltage signals are turned ON and OFF in accordance with the shapes of the characters, and a specific set of ON/OFF signals is transmitted to the display controller depending on the displayed images and characters. The patterns of these ON/OFF signals are altered by input from the keyboard. During signal switching, transient currents appear in the monitor for a short period of time.

Such transient currents can be regarded as information signals with high-frequency components that are emitted through the device's antenna or by a component acting as an antenna. Information can also be conducted through communication and power cables attached to the device.

Fig. 6 shows a display image reconstruction based on the measured time changes in the EM waves carrying the signals for drawing the display on a tablet PC. For touch screen devices such as tablets and smart phones, the acquisition of the time changes in a software keyboard image displayed on the screen leads to information leakage of both the input destination and content.

The signal observation method is also applicable to cryptographic devices; in this case, it is referred to as simple EM analysis (SEMA) [26]. When a cryptographic device performs two operations (A and B) based on a secret key, an attacker can identify the difference between the respective EM traces of A and B within a single execution step and subsequently estimate the secret key from the sequence pattern.

In general, SEMA attacks are suitable for public-key ciphers, which require a considerable number of computations to calculate each bit of the secret key. For example, the RSA cryptosystem [35], one of the most popular public-key ciphers, performs encryption and decryption through simple modular exponentiation. The typical exponentiation algorithm performs multiplication and squaring sequentially in accordance with the bit pattern of the exponent corresponding to the secret key. Thus, the key bit pattern can be derived by analyzing where multiplication and squaring operations appear in an EM trace. Several advanced analysis methods using chosen-message techniques have also been reported [36-38].

The attacks described above have been shown to be applicable to radiated and conducted emissions [28, 39] from laptop PCs and servers equipped with public-key ciphers.

3.2.2 Information Acquisition Based on Multiple Observations

The other primary acquisition method involves obtaining a large number of EM traces during a target operation and then performing statistical analysis on the obtained data to reduce noise and retrieve secret information. This method is powerful in applications involving ICT devices in which the EM emissions are of extremely low power but noisy. In addition,

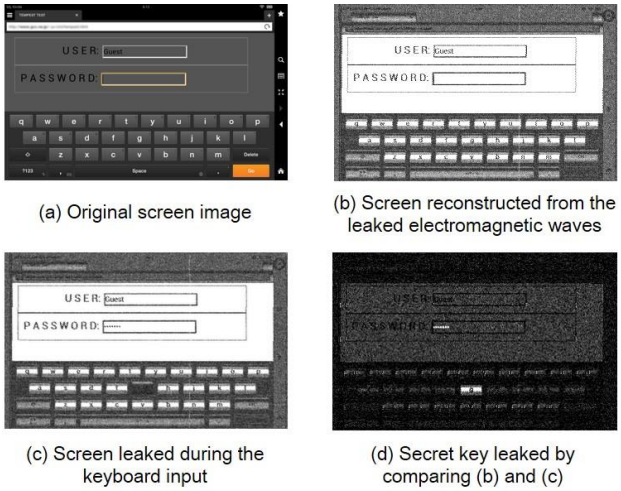


Fig. 6 Image reconstructed from EM leakage from a Tablet PC [14]

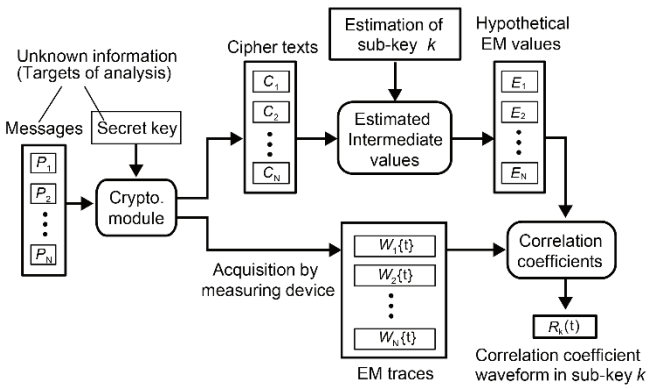


Fig. 7 Basic flow of CEMA.

attackers do not require detailed knowledge about the implementation of the target cryptographic device. This method is known as differential EM analysis (DEMA) [26] and represents an important type of side-channel attack on cryptographic devices.

Fig. 7 shows the basic flow of DEMA (more precisely, correlation EM analysis (CEMA) [40]). In a typical scenario, the ciphertexts are known while the plaintext characters (i.e., messages) and secret key are unknown to the attacker; thus, the goal of the analysis is to recover the secret key. The attacker eavesdrops on the ciphertexts corresponding to several encrypted messages to acquire the corresponding EM traces, then guesses the value of a specific subkey and uses it to generate hypothetical EM values corresponding to the ciphertexts. It is important to note that, in modern ciphers the encryption process is determined in part by such subkeys (which might be, for instance, a one-byte key). In the case of the 128-bit Advanced Encryption Standard (AES) [41] implementation, there are 16 S-boxes, each with a one-byte input and output, with each output independently combined with the one-byte subkey in the AddRoundKey operation. Therefore, the number of hypothetical EM values is at most

256 (=2^8). Finally, the attacker calculates the correlation between the measured EM traces and the hypothetical EM values at an arbitrary time index to generate a correlation coefficient trace for each estimated subkey. If the estimation is correct, the attacker would find a high peak value somewhere within the generated trace.

Unlike SEMA, DEMA is primarily applied to symmetric block ciphers such as AES or data encryption standard ciphers [42], in which the EM emission is considerably less powerful than in the case of public-key ciphers, as symmetric block ciphers are frequently used for encrypting larger amounts of data than asymmetric ciphers. By applying DEMA to several EM waves, it is possible to suppress the noise component contained in a radiated EM wave and extract its secret key information. Chosen-message power analysis has been proposed as another means of expanding the range of target algorithms [43, 44].

DEMA attacks are also known to be applicable to actual systems. For example, attacks have been reported on AES implemented in commercial CPUs and on RFID devices equipped with DES and AES [45-48].

4 Countermeasures against EM Information Leakage

Countermeasures against EM emanation from ICT devices are primarily classified into two types. The first type includes countermeasures applied to EM emanation sources (e.g., large-scale integration (LSI) chips and devices) in which the information requiring protected from leakage is processed. The second type includes countermeasures applied to paths (i.e., source-antenna and antenna-receiver) from the source to the receiver.

Depending on the application and usage environment, more than one countermeasure can be applied, as there is no universal solution satisfying the criteria of both high effectiveness and low implementation cost for any device. The following subsections describe and provide examples of the two types of countermeasures.

4.1 Countermeasures Applied to EM Emanation Sources

The EM radiation from an ICT device is caused by the time variation in currents (produced, for example, by differences between electrical switching operations) generated by the data processing in the device. In this context, the electric module or device processing data are known as the "emanation source."

For example, a display module in a PC or a cryptographic module in a mobile phone can be an emanation source. To better understand potential countermeasures to such EM emanation, we first look at how it is generated. A display module such as a PC monitor uses video signals to produce a series of pixel patterns, and a combination of voltages within the signals is used to control the color on the display. The magnitude of the emitted EM signals depends on the variations in video signal voltage between neighboring pixels. Using this information, any image can be reconstructed by acquiring the appropriate EM signals, although the reconstructed display image will be in grayscale mode with values corresponding to the magnitude of the EM signal alone. In this manner, voltage variation in a video signal can lead to information leakage via the emitted EM signal.

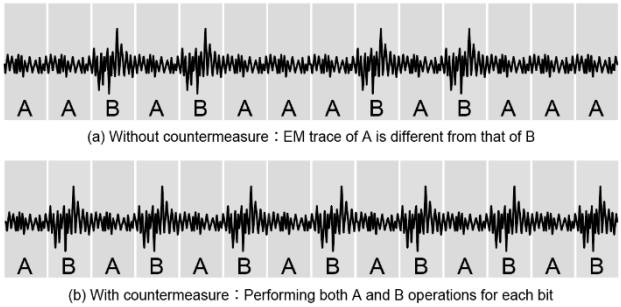


Fig. 8 Example of hiding-type countermeasure

One method for preventing such reconstruction is to reduce the contrast between the colors of the foreground text and the background image. This is useful because different colors emit different levels of EM radiation in rough proportion to the luminance of the pixel. Based on the results in [3], removing the upper 30% of the spectrum produced by text to reduce the peak voltage level appears to provide a satisfactory compromise between protection and rendering quality. The same author also suggested that randomizing the least significant bit (LSB) of the screen image as another source of noise is a better countermeasure [49].

A method in which a significant amount of noise is superimposed onto displayed images is presented in [50]. In this method, which takes advantage of the characteristic of human vision known as additive color mixing, mutually complementary images are generated from a sequence of input images and a random image; these are then shown on a screen by flipping them in quick succession, which causes the human brain to perform color mixing. As a result, the images can be seen as intended on the screen but an attacker monitoring the EM emanation would not be able to recreate the images.

Countermeasures against side-channel attacks on cryptographic modules have also been reported [51]; such countermeasures can be classified as either hiding and masking techniques.

Hiding is implemented by removing the correspondence between side-channel information (i.e., power consumption and EM radiation) and processed data/operations. A typical hiding-type countermeasure against EM analysis attacks is to change the algorithm and/or circuit of the cryptographic module to produce a constant EM radiation pattern that does not change with the processed data.

Fig. 8 illustrates the concept of a hiding-type countermeasure. In Fig. 8(a), operations "A" and "B" are performed in accordance with the bit pattern of a secret key. The key can be revealed using the pattern in this figure because, in the absence of a countermeasure, the EM trace of A is different from that of B. By contrast, using a countermeasure

(for example, inserting a dummy operation B after each operation A) results in the EM trace shown in Fig. 8(b), which indicates falsely that both A and B are performed for each bit. This prevents an attacker from deducing the specific pattern of operations based on the secret key. In cases in which the dummy operation B can be distinguished from an actual operation B, an advanced hiding countermeasure such as the Montgomery powering ladder [52] can be applied to the cryptographic modules to prevent an attacker from identifying any particular operations.

Masking, on the other hand, is performed by randomizing the intermediate data processed by the module. In particular, the use of chosen-message techniques by attackers can be rendered ineffective using message masking. The capability of this countermeasure depends on the random mask size and the frequency of its update. To achieve a higher level of security, the mask value should be sufficiently large and frequently changed according to the application of modules.

Hiding and masking countermeasures have been developed and applied primarily at the algorithmic, architectural, and circuit levels. In [53] and [54], algorithmic countermeasures in which operations are performed over a constant time interval independent of the secret key bit pattern were demonstrated using double-and-add and Montgomery powering ladder approaches, respectively. Although the countermeasures developed in these studies can be easily implemented, according to [37,55] they can be broken by attacks with chosen-message scenarios. In [37], a doubling attack using an input pair X and X^2 that could break a simple double-and-add algorithm was presented. In [55], a comparative power analysis attack using an input pair Y and Z (Y^α=Z^β) that could break standard constant-time algorithms including the Montgomery powering ladder was presented.

Countermeasures at the circuit level provide another general-purpose solution, although one that can be expensive and difficult to design. In this context, random switching logic (RSL) [56] and wave dynamic differential logic (WDDL) [57] are well known typical countermeasures for masking and hiding, respectively. RSL uses random data to mask the transition probabilities of inputs and outputs, while WDDL is an extended version of sense amplifier-based logic [58] that successfully balances circuit activity using complementary logic gates and a pre-charge phase. It is important to note that both of these countermeasures must be carefully designed to achieve completely-masked/hidden values.

Threshold implementation (TI) [59] was recently introduced as a circuit-level masking countermeasure and has been mathematically and experimentally shown to be robust against differential EM/power analysis attack (a type of side-channel attack [22]). However, the overhead of this countermeasure is non-trivial and prevention of advanced (i.e., higher-order) attacks would not be practical.

An attacker who could closely approach the surface of a cryptographic LSI could defeat hiding or masking countermeasures by precisely observing local information from a specific part of the LSI beyond the conventional security assumptions (power/EM models, attackers' capabilities, etc.).

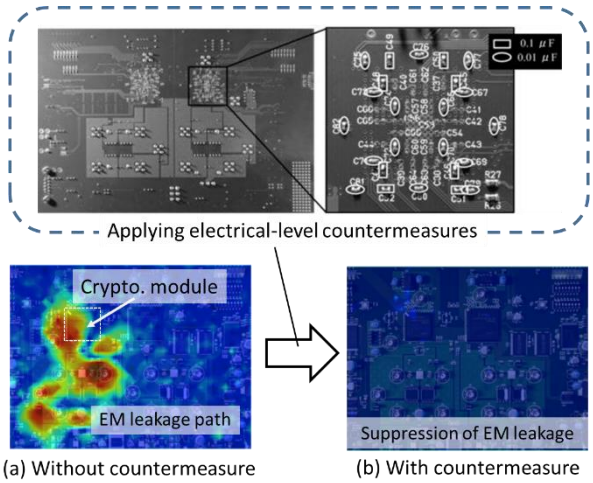


Fig. 9 Cost-effective electrical countermeasures using electric elements [63]

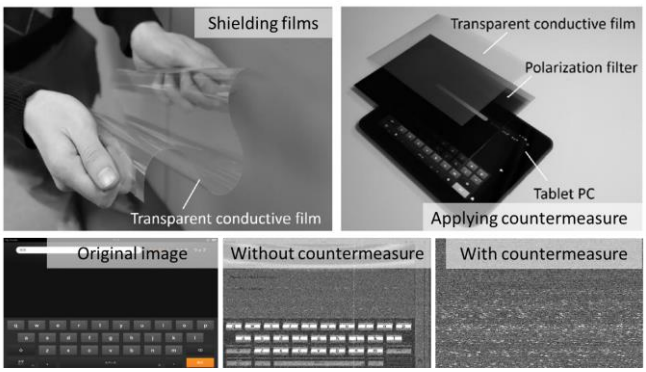


Fig. 10 Countermeasure based on EM shielding film [14]

In [60], the possibility of exploiting leaks inside semi-custom application-specific ICs (ASICs) using microprobe-based EM analysis was demonstrated. The work demonstrated the measurement of current-path and internal-gate leaks in a standard cell and geometric leaks in a memory macro by placing a magnetic field microprobe on the chip surface. This suggests that most conventional countermeasures would become ineffective if such leaks can be measured by an attacker.

To address the limitations of conventional countermeasures against such attacks, a reactive countermeasure against EM leakage was proposed in [61,62] based on the general phenomenon of electrical coupling between two conductive items in close proximity (in this case, a probe in the form of a looped conductor and a measured object). The proposed countermeasure uses an LC oscillator-based sensor to protectively react to any invasion of this nature. Such reactive countermeasures can be considered to be effective solutions to advanced EM attacks using high-space/time precision equipment.

4.2 Countermeasures Applied to emission Paths

Countermeasures applied to EM emission paths are also effective in reducing information leakage. Such paths include coupling paths (i.e., EM signals induced in an antenna by a source), any antenna generated by the physical structure of a device (e.g., printed circuit boards (PCBs) and connecting lines), and free space between an antenna and a receiver.

Most conventional EMC techniques can be considered to represent this type of countermeasure. Typical countermeasures applied to coupling paths and antennas include: i) constructing decoupling circuits between the power source and ground near the source (i.e., power decoupling); ii) devising a specific structure and wiring pattern for any PCBs in the device (i.e., PCB design); and iii) ensuring conductivity at the junctions of a package by installing conductive components such as conductive gaskets and shielding connected cables by filtering components such as ferrite cores (i.e., package shielding).

Any combinations of the above countermeasures can be employed, and effective reduction in EM emission can be obtained by combining and/or strengthening such countermeasures because the intensity of EM emission also depends on the power of the source and the radiative efficiency of the antenna.

Figs. 9 and 10 show examples of emission path countermeasures. Fig. 9(a) shows a generated EM wave propagating from a cryptographic module to a power line connected to equipment through the wiring pattern of a board. The suppression of this propagation is shown in Fig. 9(b) through the mounting of a decoupling capacitor onto the assembly. As another example (Fig. 10), the edge of a display screen can act as an antenna and leak radiation. It is possible to prevent reconstruction of the screen image by attaching a shielding structure close to the antenna that effectively blocks the frequency causing information leakage.

These types of countermeasures are not always available because office devices and systems are often leased. In such cases, the suppression of EM signals at the level of a specific site, building, or facility would be required for effective reduction of EM information leakage. In other words, the implementation of countermeasures at these levels can be effective and sufficient even if some of the devices and systems performing data processing are left unprotected at an individual level. The requirements for such shielding are defined in [64] and [65]. For facility-level countermeasures, measurement and confirmation of the shielding performance are also required upon completion of construction. It is important to confirm whether EM signals can be measured from the best available position (e.g., the border between the facility and the outside environment) and how effectively EM signals can be suppressed by shielding.

5. Other Types of Security Degradation by EM Waves

In this section, we focus on the problem of security degradation arising from disturbances induced inside of equipment through intentional EM interference. We then outline the problem of security degradation arising from the deliberate modification of circuitry within a device.

5.1 Security Degradation by Intentional EM Interference

Threats that degrade the availability of ICT devices via intentional EM interference (IEMI) have been previously studied. In such cases, ICT devices can be overwhelmed by IEMI to the point of cessation of operation or even damage to circuit elements. IEMI creates a high-power EM environment (HPEM) that far exceeds the EM tolerance of an attacked ICT device. Conventionally, the threat of IEMI to electronic devices using HPEMs was limited to certain influence areas, namely, governments and militaries; however, in recent years small-sized high-power transmitters and related devices have become commercially available, making the threat of IEMI to common ICT devices a more likely prospect.

To address these threats, discussion and research on their mechanisms and corresponding countermeasure technologies is being actively conducted, in particular by the IEEE EMC Society [66,67]. In addition, the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU) are including such threats in their standardization works and have defined the "radiative HPEM environment" and "conductive HPEM environment" as "the peak electric field strength more than or equal to 100 V/m", and “the high-power EM current and voltage coupled or injected into cables or electric wires exceeding the voltage level of 1 kV," respectively.

Furthermore, threats from the non-invasive degradation of the confidentiality and integrity of ICT devices using IEMI waves with amplitudes considerably smaller than HPEM levels have been reported. Devices vulnerable to such attacks include cryptographic devices [68, 69], microphones [70], pacemakers [70], and smart phones [71]. During such an attack, a temporal fault is caused in the device by IEMI; the attacker then uses the failure to acquire confidential information from the device in the form of, e.g., faulty outputs that include secret information. In another attack scenario, the attacker rewrites the data transmitted within the device to an arbitrary value and then issues an arbitrary command to lower the confidentiality and integrity of the device.

As countermeasures against such attacks, specific circuit techniques have been developed to detect unintended EM wave propagation within devices [72, 73], and EMC countermeasures [74,75] can be implemented either inside or outside of devices to suppress EM wave propagation that can cause security degradation.

5.2 Security Degradation through Modification of EM Environment

In this subsection, we discuss the problem of security degradation arising from changes in the EM environment caused by the intentional modification of chips and devices.

For reasons including cost reduction, hardware companies have recently made use of third-party foundries to inexpensively manufacture the IC chips that the companies design. This raises the possibility of adding functions not intended by the chip designer to the IC at the time of manufacture that can be exploited by attackers to trigger IC destruction or security degradation under specific conditions. Such circuitry added contrary to the intention of a designer is called a hardware trojan (HT). HTs have been found at the government level and are now regarded as one of the more urgent security issues in the context of electronic attacks.

The effects of HTs can include changes in functionality, reduced reliability, information leakage, or denials-of-services [76, 77]. In general, however, HTs induce information leakage from devices via operations not included in the original design (e.g., [78-82]). Possible methods for detecting HTs, include physical inspection, built-in tests [83], functional testing [84-88], and side channel analyses [89-92]; these primarily target HTs located within an IC.

In recent years, it has been shown that HTs can also be placed in peripheral circuits [93]. Unlike IC HTs, these do not need to be introduced at the time of manufacture and can be mounted on the surfaces of existing electric circuit components; correspondingly, many devices on the market can be targeted, expanding the HT target object range. An HT that could be mounted on a device with low emission intensity was reported in [93]. Instead of exploiting information leakage itself, the HT amplified the device's emission intensity through the application of IEMI [93]; thus, a prospective attacker could successfully obtain information from EM radiation from even a few meters away. In the future, in addition to conventional passive attacks using naturally radiated EM waves, it will be necessary to deal with the problem of security degradation caused by such active attacks.

6. Standardization on EM Information Security

In this section, we introduce existing work on standardization associated with risk evaluation and countermeasures used in EM information security.

An information security management system (ISMS) is a set of policies that should be implemented and maintained by companies or organizations in relation to their information security management or IT-related risks. The concept of ISMS arose primarily from the ISO 27001 standard specification [94]. The requirements of physical security in ISMS are provided on the basis of Recommendation ITU-T X.1051 [95], as well as ISO/IEC Standards 27001 and 27002 [96]. These specifications and standards can be used to evaluate threats and mitigate their impacts from the equipment to the site level. The threats addressed in the these specifications and standards are essentially related to confidentiality within an ISMS.

Recommendation ITU-T K.84 [97] describes threats in the form of information leakage arising from unintentional EM emanations and outlines two mitigation approaches: i) reduction of emissions from equipment, and ii) increasing the level of site shielding. In the first approach, emission requirements and methods for examining equipment are applied when the equipment cannot be installed at a shielded site and emission from the equipment can be reduced. In the second approach, shielding requirements for sites such as buildings are applied when equipment can be installed at secure sites. Methods for testing conducted and radiated emission related to information leakage are also presented in [97]; the purpose of this recommendation is to prevent information leakage in the form of unintentional EM radiation from telecommunication equipment when the equipment or sites are managed by an ISMS.

It is important to note, however, that this recommendation only covers information leakage from equipment in which raster scan video signals are present. Although it acknowledges that information is transmitted through EM waves unintentionally emitted by various types of equipment including personal computers, data servers, laser printers, keyboards, and cryptographic modules, further updates to the recommendation will be required to fully cover such leaked signals.

Another set of standardizations covers the requirements that should be satisfied by cryptographic modules with respect to side-channel attacks. International Standard ISO/IEC 15408 (known as the common criteria) [98] is a standard for evaluating whether IT-related products or systems are properly designed and correctly implemented. It is noteworthy that all IT-related products are covered by the common criteria, although the security targets are left to be defined by the respective developers.

There is another specific standard for evaluating cryptographic modules; currently, ISO/IEC 19790 [99] serves as a security evaluation standard for cryptographic modules and covers eleven points related to their design and implementation. ISO/IEC 24759 [100] provides the derived test requirements for ISO/IEC 19790 [99], and detailed technical descriptions related to non-invasive attacks including side-channel attacks are provided in ISO/IEC 17825 [101].

7. Concluding Remarks

The threat of information leakage through EM emanation is expected to increase as a result of technological advances in measurement devices and low-cost, high-performance computers and the development of advanced analytical techniques. To effectively reduce information leakage through EM emissions, it will be necessary to use appropriate EM radiation suppression technologies based on EMC research in addition to conventional countermeasures implemented in

hardware and software.

Designers of ICs and ICT devices should analyze their systems in their entirety as well as the manner in which the devices will be used to determine the extent of the risk of EM information leakage and then, if necessary, apply appropriate countermeasures. Even countermeasures that cannot prevent information leakage under all conceivable attacks can be realistically adequate in many cases. Additionally, it will become increasingly important for users to be conscious of whether such countermeasures are effective.

References

[1] (1982, Feb.). NACSIM 5000: Tempest Fundamentals. National Security Agency, Fort George G. Meade, MD, USA. [Online]. Available partially declassified transcript: http://cryptome.org/nacsim-5000.htm

[2] W. van Eck, “Electromagnetic radiation from video display units: An eavesdropping risk?” Comput. Security, vol. 4, pp. 269–286, 1985.

[3] M. G. Kuhn and R. J. Anderson, “Soft tempest: Hidden data transmission using electromagnetic emanations,” in Proc. 2nd Workshop Inf. Hiding, LNCS 1525, Portland, OR, USA, Apr. 1998, pp. 124–142.

[4] M. G. Kuhn, “Optical time-domain eavesdropping risks of CRT displays,” in Proc. IEEE Symp. Security Privacy, Berkeley, CA, USA, May 2002, pp. 3–18.

[5] M. G. Kuhn, “Electromagnetic eavesdropping risks of flat-panel displays,” in Proc. 4th Workshop Privacy Enhanc. Technol., LNCS 3424, 2004, pp. 88–105.

[6] M. G. Kuhn, “Security limits for compromising emanations,” in Proc. Workshop Cryptograph. Hardware Embedded Syst., LNCS 3659, 2005, pp. 265–279.

[7] M. G. Kuhn, "Compromising Emanations of LCD TV Sets," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 564-570, June 2013.

[8] H. Sekiguchi and S. Seto, “An evaluation method of the display image re-constructed by electromagnetic emanation,” in Proc. EMC Eur. Workshop [CD-ROM]. no. abs-133, 2007.

[9] H. Sekiguchi and S. Seto, “Proposal of information signal measurement method in display image contained in electromagnetic noise emanated from a personal computer,” in Proc. IEEE Int. Instrum. Meas. Technol. Conf., Victoria, BC, Canada, May 2008, pp. 1859–1863.

[10] H. Sekiguchi, “Information leakage of input operation on touch screen monitors caused by electromagnetic noise,” in Proc. IEEE Int. Symp. Electromagn. Compat., Jul. 2010, pp. 127–131.

[11] H. Sekiguchi and S. Seto, "Study on Maximum Receivable Distance for Radiated Emission of Information Technology Equipment Causing Information Leakage," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 3, pp. 547-554, June 2013.

[12] T. Tosaka, Y. Yamanaka, and K. Fukunaga, “Method for determining whether or not information is contained in electromagnetic disturbance radiated from PC display,” IEEE Trans. Electromagn. Compat., vol. 53, no. 2, pp. 318–324, May 2011.

[13] 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," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 2, pp. 164-172, April 2015.

[14] Y. Hayashi, N. Homma, M. Miura, T. Aoki, H. Sone, “A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation, " 21st ACM Conference on Computer and Communications Security (CCS'14), pp. 954-965, 2014.

[15] 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," 2006 17th International Zurich Symposium on Electromagnetic Compatibility, Singapore, 2006, pp. 630-633.

[16] M. Vuagnoux and S. Pasini, “Compromising electromagnetic emanations of wired and wireless keyboards,” in Proc. 18th Conf. USENIX Security Symp., 2009, pp. 1–18.

[17] M. Vuagnoux and S. Pasini, “An improved technique to discover compro-mising electromagnetic emanations,” in Proc. IEEE Int. Symp. Electro-magn. Compat., Jul. 2010, pp. 121–126.

[18] M. Kinugawa, Y. i. Hayashi, T. Mizuki and H. Sone, "The effects of PS/2 keyboard setup on a conductive table on electromagnetic information leakages," 2012 Proceedings of SICE Annual Conference (SICE), Akita, pp. 60-63, 2012.

[19] M. Kinugawa, Y. Hayashi, T. Mizuki and H. Sone, “Study on Information Leakage of Input Key due to Frequency Fluctuation of RC Oscillator in Keyboard,” IEICE Trans. Commun., vol. E96-B, no.10, pp. 2633-2638, 2013.

[20] A. Zajic and M. Prvulovic, “Experimental demonstration of electromagnetic information leakage from modern processor-memory systems,” IEEE Transaction on Electromagnetic Compatibility, vol.56, no.4, pp.885–892, March, 2014.

[21] P. Kocher, “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems,” in Proc. 16th Annu. Int. Cryptology Conf. Adv. Cryptology, LNCS 1109, 1996, pp. 104–113.

[22] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” in Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology, LNCS 1666, 1999, pp. 388–397.

[23] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side channel cryptanalysis of product ciphers,” J. Comput. Security, vol. 8, no. 2–3, pp. 141–158, 2000.

[24] C. K. Koc, Cryptographic Engineering. New York, NY, USA: Springer-Verlag, 2009.

[25] K. Gandolfi, C. Mourtel, and F. Olivier, “Electromagnetic analysis: Con-crete results,” in Proc. 3rd Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 2162, 2001, pp. 251–261.

[26] J. Quisquater and D. Samyde, “Electromagnetic analysis (EMA): Mea-sures and counter-measures for smart cards,” in Proc. E-Smart,LNCS 2140, Sep. 2001, pp. 200–210.

[27] E. Peeters, X. Standaert, and J. Quisquater, “Power and electromagnetic analysis: Improved model, consequences and comparisons,” Integr. VLSI J., vol. 40, no. 1, pp. 52–60, 2007.

[28] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, “The EM side-channel(s),” in Proc. 4th Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 2523, Aug. 2002, pp. 29–45.

[29] D. M. Hockanson, J. L. Drewniak, T. H. Hubing, T. P. VanDoren, F. Sha,andM. J.Wilhelm, ``Investigation of fundamental EMI source mechanisms driving common mode radiation from printed circuit boards with attached cables," IEEE Transactions on Electromagnetic Compatibility, vol. 38, no. 4, pp. 557–576, Nov. 1996.

[30] T. Watanabe, O. Wada, T. Miyashita, and R. Koga, ``Common-mode current generation caused by difference of unbalance of transmission lines on a printed circuit board with narrow ground pattern," Inst. Electron. Inform. Commun. Eng. Trans. Commun., vol. E83-B, no. 3, pp. 593–599, 2000.

[31] H. W. Shim and T. H. Hubing, ``Model for estimating radiated emissions from a printed circuit board with attached cables due to voltage-driven sources," IEEE Transaction on Electromagnetic Compatibility, vol. 47, no. 4, pp. 899–907, Nov. 2005.

[32] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, L. Sauvage and J.-L. Danger,“Analysis of Electromagnetic Information Leakage from Cryptographic Devices with Different Physical Structures,” IEEE Trans. on Electromagnetic Compatibility, vol. 55, No. 3, pp. 571-580, June 2013.

[33] (2001). GNU Radio. [Online]. Avail-able: https://www.gnuradio.org/

[34] (1994) MATLAB (matrix laboratory), MathWorks, https://www.mathworks.com/products/matlab.html

[35] R. L. Rivest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures and public-key cryptosystems,” Commun. ACM, vol. 21, no. 2 pp. 120–126, Feb. 1978.

[36] R. Novak, “SPA-based adaptive chosen-ciphertext attack on RSA imple-mentation,” in Proc. Public Key Cryptography, LNCS 2274, Feb. 2002, pp. 252–262.

[37] A. P. Fouque and F. Valette, “The doubling attack -why upwards is bet-ter than downwards,” in Proc. Int. Workshop Cryptographic

Hardware Embedded Syst., LNCS 2779, Sep. 2003, pp. 269–280.

[38] Miyamoto, N. Homma, T. Aoki, and A. Satoh, “Chosen-message SPA attacks against FPGA-based RSA hardware implementations,” in Proc. Int. Conf. Field Programmable Logic Appl., Sep. 2008, pp. 35–40.

[39] D. Genkin , I. Pipman , E. Tromer, “Get Your Hands Off My Laptop: Physical Side-Channel Key-Extraction Attacks on PCs,” Proceedings of the 16th International Workshop on Cryptographic Hardware and Embedded Systems --- CHES 2014, September 23-26, 2014.

[40] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in Proc. 6th Int. Workshop Cryptographic Hardware Embedded Syst., LNCS 3156, Aug. 2004, pp. 16–29.

[41] National Institute of Standards and Technology (NIST). (2001, Nov.). Advanced Encryption Standard (AES), FIPS PUB. 197. [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[42] National Institute of Standards and Technology (NIST), Data Encryption Standard (DES) FIPS PUB. 46-3. (1999). [Online]. Available: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

[43] K. Schramm, G. Leander, P. Felke, and C. Paar, “A collision-attack on AES combining side-channel and differential-attack,” in Proc. Int. Work-shop Cryptographic Hardware Embedded Syst., LNCS 3156, Aug. 2004, pp. 163–175.

[44] J. Jaffe, “More differential power analysis: Selected DPA attacks,” presented at the Summer School on Cryptographic Hardware, Side-Channel and Fault Attacks, Jun. 2006, Louvain-la-Neuve, Belgium.

[45] P. Rohatgi, "Defend encryption systems against side-channel attacks," EDN network, March 2015.

[46] T. Kasper, D. Oswald, C. Paar, “Side-channel analysis of cryptographic RFIDs with analog demodulation,” in International Workshop on Radio Frequency Identification: Security and Privacy Issues pp. 61-77, 2011.

[47] M. Hutter, S. Mangard, M. Feldhofer, “Power and EM Attacks on Passive 13.56 MHz RFID Devices, “in International Workshop on Cryptographic Hardware and Embedded Systems, pp. 320-333, 2007.

[48] T. Kasper, D. Oswald, C. Paar, “EM side-channel attacks on commercial contactless smartcards using low-cost equipment” in Information Security Applications, pp. 79-93, 2009.

[49] M. G. Kuhn, “Compromising emanations: eavesdropping risks of com-puter displays,” Univ. Cambridge, Computer Lab., Cambridge, U.K., Tech. Rep. UCAM-CL-TR-577, 2003.

[50] T. Watanabe, H. Nagayoshi, T. Urano, T. Uemura, and H. Sako, “Counter-measure for electromagnetic screen image leakage based on color mixing in human brain,” in Proc. IEEE Int. Symp. Electromagn. Compat.,Jul. 2010, pp. 138–142.

[51] S. Mangard, E. Oswald, and T. Popp, Power Analysis Attacks - Reveal-ing the Secrets of Smart Cards. New York, NY, USA: Springer-Verlag, 2007.

[52] Joye, Marc, and Sung-Ming Yen. "The Montgomery powering ladder." CHES. Vol. 2. 2002.

[53] J. S. Coron, “Resistance against differential power analysis for elliptic curve cryptosystems,” in Proc. 1st Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 1717, Aug. 1999, pp. 192–302.

[54] M. Joye and S. M. Yen, “The montgomery powering ladder,” in Proc. 4th Int. Workshop Cryptographic Hardware and Embedded Syst.,LNCS 2523, Aug. 2002, pp. 291–302.

[55] N. Homma, A. Miyamoto, T. Aoki, A. Satoh, and A. Shamir, “Collision-based power analysis of modular exponentiation using chosen-messagepairs,” in Proc. 10th Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 5154, Aug. 2008, pp. 15–29.

[56] D. Suzuki, M. Saeki, and T. Ichikawa, “Random switching logic: A new countermeasure against DPA and second-order DPA at the logic level,” IEICE Trans. Fundamentals, vol. E90-A, no. 1, pp. 160–168, Jan. 2007.

[57] K. Tiri, D. Hwang, A. Hodjat, B. C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, “Prototype IC with WDDL and differential routing—DPA resistance assessment,” in Proc. Int. Workshop Cryptographic Hardware and Embedded Syst., LNCS 3659, May 2005, pp. 354–365.

[58] K. Tiri, M. Akmal, and I. Verbauwhede, “A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards,” in Proc. 28th Eur. Solid-State Circuits Conf., Sep. 2002, pp. 403–406.

[59] S. Nikova, C. Rechberger, and V. Rijmen. Threshold implementations against side-channel attacks and glitches. In ICICS, volume 4307 of LNCS, pages 529–545. Springer, 2006.

[60] T. Sugawara, D. Suzuki, M. Saeki, M. Shiozaki, and T. Fujino, “Measurable Side-Channel Leaks Inside ASIC Design Primitives,” CHES 2013, Lecture Notes in Computer Science, vol. 8086, pp.159–178, Aug. 2013.

[61] N. Homma, Y. Hayashi, N. Miura, D. Fujimoto, M. Nagata, and T. Aoki, “Design Methodology and Validity Verification for a Reactive Countermeasure against EM Attacks,” Journal of Cryptology 30.2 pp. 373-391, 2017.

[62] D. Ishihata, N. Homma, Y. Hayashi, N. Miura, D. Fujimoto, M. Nagata,and T. Aoki, "Enhancing Reactive Countermeasure against EM Attacks with Low Overhead," IEEE International Symposium on Electromagnetic Compatibility, pp.399-404, 2017.

[63] Y. Hayashi, N. Homma, T. Mizuki, H. Shimada, T. Aoki, H. Sone, L. Sauvage and J.-L. Danger, “Efficient Evaluation of EM Radiation Associated with Information Leakage from Cryptographic Devices,” IEEE Trans. on Electromagnetic Compatibility, vol. 55, No. 3, pp. 555-563, June 2013.

[64] (1995, Dec. 12). National Security Telecommunications and In-formation Systems Security Advisory Memorandum NSTISSAM TEMPEST/2-95: RED/BLACK Installation Guidance. National Secu-rity Agency, Fort George G. Meade, MD, USA. [Online]. Available: http://cryptome.org/tempest-2-95.htm

[65] US Department of Defense, “Radio frequency shielded enclosures,” MIL-HDBK-1195, Sep. 1988.

[66] W. A. Radasky, C. E. Baum and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)," in IEEE Transactions on Electromagnetic Compatibility, vol. 46, no. 3, pp. 314-321, Aug. 2004.

[67] W. A. Radasky, "Fear of frying electromagnetic weapons threaten our data networks. Here's how to stop them," in IEEE Spectrum, vol. 51, no. 9, pp. 46-51, Sept. 2014.

[68] P. Maurine, "Techniques for EM Fault Injection: Equipments and Experimental Results," 2012 Workshop on Fault Diagnosis and Tolerance in Cryptography, Leuven, 2012, pp. 3-4.

[69] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki and H. Sone, "Transient IEMI Threats for Cryptographic Devices," in IEEE Transactions on Electromagnetic Compatibility, vol. 55, no. 1, pp. 140-148, Feb. 2013.

[70] D. F. Kune et al., "Ghost Talk: Mitigating EMI Signal Injection Attacks against Analog Sensors," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 145-159.

[71] C. Kasmi and J. Lopes Esteves, "IEMI Threats for Information Security: Remote Command Injection on Modern Smartphones," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 6, pp. 1752-1755, Dec. 2015.

[72] El-Baze, D., Rigaud, J. B., & Maurine, P. (2016, August). An Embedded Digital Sensor against EM and BB Fault Injection. In Fault Diagnosis and Tolerance in Cryptography (FDTC), 2016 Workshop on (pp. 78-86). IEEE.

[73] Sho Endo, Yang Li, Naofumi Homma, Kazuo Sakiyama, Kazuo Ohta, Daisuke Fujimoto, Makoto Nagata, Toshihiro Katashita, Jean-Luc Danger, and Takafumi Aoki, “A Silicon-level Countermeasure against Fault Sensitivity Analysis and Its Evaluation,” IEEE Transactions on Very Large Scale Integration Systems, Vol.23, No.8, pp.1429--1438 2015

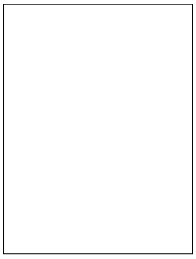
[74] Paul, Clayton R. Introduction to Electromagnetic Compatibility. Vol. 184. John Wiley & Sons, 2006.

[75] N. Miura, D. Fujimoto, Y. Hayashi, N. Homma, T. Aoki, M. Nagata, "Integrated-circuit countermeasures against information leakage through EM radiation." (EMC), in Proc. IEEE International Symposium on Electromagnetic Compatibility, pp. 748-751, 2014.

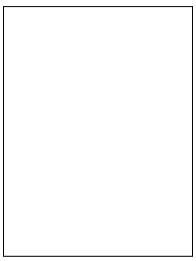
[76] Tehranipoor, Mohammad, and Cliff Wang. Introduction to hardware security and trust. Springer Science & Business Media, 2011.

[77] Tehranipoor, Mohammad, and Farinaz Koushanfar. "A survey of hardware trojan taxonomy and detection." IEEE design & test of

computers 27.1 (2010).
[78] K. Yang, M. Hicks, Q. Dong, T. Austin, D. Sylvester, “Analog malicious hardware,” In Security and Privacy, IEEE Symposium on In Security and Privacy, pp. 18-37, 2016.
[79] Z. Gong and M. X. Makkes "Hardware Trojan side-channels based on physical unclonable functions", WISTP 2011, LNCS 6633 pp. 293-303, 2011.
[80] R. M. Rad, X. Wang, M. Tehranipoor, and J. Plusquellic, "Power supply signal calibration techniques for improving detection resolution to hardware trojans," IEEE/ACM International Conference on Computer-Aided Design (ICCAD '08), pp. 632-639, 2008.
[81] J. Yier, N. Kupp, Y. Makris, "Experiences in Hardware Trojan design and implementation," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp. 50-57, July 2009.
[82] [28] J. Clark, S. Leblanc, S. Knight, "Risks associated with USB Hardware Trojan devices used by insiders," 2011 IEEE International on Systems Conference (SysCon), pp. 201-208, April 2011.
[83] L. W. Kim and J. D. Villasenor, "A System-On-Chip Bus Architecture for Thwarting Integrated Circuit Trojan Horses," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 19, no. 10, pp. 1921-1926, Oct. 2011.
[84] R. Rad, J. Plusquellic, M. Tehranipoor, "Sensitivity analysis to hardware Trojans using power supply transient signals," IEEE International Workshop on Hardware-Oriented Security and Trust (HOST 2008), pp. 3-7, June 2008.
[85] M. Banga and M. Hsiao, "A Region Based Approach for the Identification of Hardware Trojans," Proc. IEEE International Workshop Hardware-Oriented Security and Trust, 2008, pp. 40-47.
[86] R. S. Chakraborty, F. Wolff, S. Paul, C. Papachristou, and S. Bhunia, "MERO: a statistical approach for hardware Trojan detection," Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems, 2009, pp. 396-410.
[87] S. Jha and S. K. Jha, "Randomization Based Probabilistic Approach to Detect Trojan Circuits," Proc. 11th IEEE High Assurance Systems Engineering Symp. , IEEE CS Press, 2008, pp. 117-124.
[88] F. Wolff, C. Papachristou, S. Bhunia, and R. S. Chakraborty, "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme," Design, Automation and Test in Europe, pp. 1362-1365, March 2008.
[89] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar, “Trojan detection using IC fingerprinting,” IEEE Symposium on In Security and Privacy, pp. 296-310, 2007.
[90] L. Lin, W. Burleson, and C. Paar, "MOLES: malicious off-chip leakage enabled by side-channels," IEEE/ACM International Conference on Computer-Aided Design (ICCAD '09), pp. 117-122, 2009.
[91] S. Bhasin, J.-L. Danger, S. Guilley, X. T. Ngo, L. Sauvage, "Hardware Trojan Horses in Cryptographic IP Cores," Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC), pp. 15-29, Aug. 2013.
[92] J. Balasch, B. Gierlichs and I. Verbauwhede, "Electromagnetic circuit fingerprints for Hardware Trojan detection," 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, 2015, pp. 246-251.
[93] M. Kinugawa, Y. Hayashi,“Evaluation of Information Leakage caused by Hardware Trojans Implementable in IC Peripheral Circuits, 2016 Asia-Pacific Symposium on Electromagnetic Compatibility, 2016.
[94] Information Technology – Security Techniques – Information Security Management Systems—Requirements, Int. Org. Standardization (ISO) and Int. Electrotechnical Commission (IEC), ISO/IEC 27001, 2005.
[95] Information Security Management System-Requirements for Telecommu-nications (ISMS-T), Int. Telecommun. Union-Telecommun. Standardiza-tion Sector (ITU-T), ITU-T X.1051, 2004.
[96] Information Technology - Security Techniques - Code of Practice for Infor-mation Security Management, International Organization for Standardiza-tion (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27002, 2005.
[97] Test Methods and Guide Against Information Leaks Through Unintentional Electromagnetic Emissions, Int. Telecommun. Union-Telecommun. Standardization Sector (ITU-T), ITU-T K.84, 2011.
[98] Common Criteria for Information Technology Security Evaluation, Int. Organization for Standardization (ISO) and Int. Electrotechnical Com-mission (IEC), ISO/IEC 15408-1, 2005.
[99] Information Technology - Security Techniques - Security Requirements for Cryptographic Modules, Int. Org. Standardization (ISO) and Int. Electrotechnical Commission (IEC), ISO/IEC 19790, 2006.
[100] Information Technology - Security Techniques - Test Requirements for Cryptographic Modules, Int. Org. Standardization (ISO) Int. Electro technical Commission (IEC), ISO/IEC 24759, 2008.
[101] Information technology -- Security techniques -- Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, Int. Org. Standardization (ISO) Int. Electro technical Commission (IEC), ISO/IEC 17825, 2016.



Yu-ichi Hayashi received his M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2005 and 2009, respectively. He is currently a Professor in the Graduate School of Information Science, Nara Institute of Science and Technology. His research interests include electromagnetic compatibility and information security. Dr. Hayashi is the Chair of EM Information Leakage Subcommittee in IEEE EMC Technical Committee 5.



Naofumi Homma received his M.S. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 1999 and 2001, respectively. He is currently a Professor in the Research Institute of Electrical Communication, Tohoku University. His research interests include hardware security, computer arithmetic, EDA methodology, and cryptographic implementation. Dr. Homma is a member of Advisory Board for Cryptographic Technology, Japan.