Artificial Metrics of Electric Devices and Their Applications

Artificial Metrics of Electric Devices and Their Applications

Hidenori KUWAKADO[*1], Yasushi HORII[*1],
Takashi KOBAYASHI[*1], Tomoya KAMBARA[*2,1)]

Abstract

An Identification of artificial objects is lately receiving much attention for two reasons: the problem of counterfeiting of artificial objects, such as goods that use brand names, in international trade and the necessity of achieving a secure communication in the Internet of Things (IoT), which is a network of artificial objects that are embedded with network connectivity. To identify artificial objects, “fingerprints” of artificial objects, introduced during manufacturing and non-separable characteristics from artificial objects themselves, have to be discovered. This article reports fingerprints for acceleration sensors, flash memory, non-Foster matching circuits and elemental techniques for identifying fingerprints or measuring fingerprints with stability. This article demonstrates an encoding method for recording fingerprints securely in a distributed storage system.

Keyword: device fingerprint, artificial metrics, physical unclonable function

1. Introduction

The report by the organisation for economic cooperation and development (OECD) warns that the impact of counterfeiting on international trade amounted to $250 billion in losses in 2007 [1]. The amount can be predicted to increase much more currently. Other reports as well as OECD’s that caution about the economic impact of counterfeiting have been published. From the other perspective, artificial objects are also receiving much attention lately. The Internet of Things (IoT) is a network of artificial objects that are embedded with electronics, software, sensors, actuators, and network connectivity. The identification of artificial objects is essential to establish secure communication between artificial objects in IoT.

Recent developments on sensing technology allow us to identify artificial objects one by one instead

*1 Faculty of Informatics, Kansai University
*2 Faculty of Culture and information Science, Doshisha University
1) This research was done at Faculty of Informatics, Kansai University.

of merely telling the real from the false. Identification methods are classified into two categories. The first category is to equip objects with tags that contain identification information. An RFID tag is the example of such a tag. The second category is to use the uniqueness of their physical properties. Such physical properties depend on random physical factors introduced during manufacturing and are expected to be unpredictable and uncontrollable which makes it impossible to clone properties precisely. The physical property used in this identification method is called a physical unclonable function (PUF) or an artificial metrics (e.g., [2] [3]). This is an analogous concept of biometrics that refers to metrics related to human characteristics. Namely, this is an object's fingerprint. To achieve authentication protocols, the physical property is often combined with cryptographic technique. This paper focuses on methods in the second category, that is, the PUF or the artificial metrics.

PUFs (or PUF-like methods) have been reported for a wide variety of technologies and materials such as glass, paper, and electronic devices. An example of non-electronic PUFs is the random fiber structure of a paper. Electronic PUFs use electronic characteristics such as resistance and capacitance. An example of electronic PUFs is a silicon PUF that are based on the randomness of the semiconductor chip manufacturing process PUFs are also classified based on the randomness of objects: intrinsic randomness and non-intrinsic randomness (or explicitly-introduced). The advantage of use of intrinsic randomness is not to require any modifications to the manufacturing process. Many articles on electronic PUFs using intrinsic randomness have been published recently. Although the non-intrinsic randomness usually gives a high ability to distinguish objects from one another, the manufacturing process has to be changed one by one to introduce non-intrinsic randomness.

This article reports electronic PUFs using intrinsic randomness. Unlike previous works, our PUFs do not directly use the randomness of the semiconductor chip manufacturing process, but use the difference in object's outputs that are caused by the randomness of the semiconductor chip manufacturing process. That is, we focus on PUFs of mass-produced products that are designed in such a way that they are not purposefully equipped with PUFs.

This article is organized as follows: Section 2 describes an acceleration-sensor metrics and discuss its application for individual identification. This section was handled by Kobayashi.

Section 3 reports metrics on memory chips including controllers that are used for USB3.0 thumb drives. It is known that writing speed and reading speed depend on USB3.0 thumb drives. We focus on the fact that they are different even for the same products. This section was handled by Kambara.

Section 4 studies metrics based on non-Foster matching circuits and proposes stabilization of their metrics. Non-Foster matching circuits have originally studied in the field of wireless communication. Since non-Foster matching circuits we consider that this property can be used the artificial metrics. This section was handled by Horii.

Section 5 describes encoding methods for storing metrics information in distributed storage systems.

Since the amount of metrics information of mass-produced objects is expected to be large, distributed storage systems are inevitably required. The management of metrics information requires not only the availability of distributed storage systems but also the confidentiality. This section proposes a secure regenerating code that achieves both of availability and confidentiality. Whereas previous secure regenerating codes are based on the informationally-secure model, the proposed code is based on the computationally-secure model. The advantage of the proposed code is that the size of distributed information to each storage nodes is smaller than that of previous secure regenerating codes. That is, the storage capacity of each storage nodes can be saved. This section was handled by Kuwakado.

Section 6 concludes this paper and describes future work.

2. Acceleration-Sensor Metrics and Individual Identification

2.1 Introduction

We are studying personal authentication application using an acceleration and gyro sensor. People can produce a variety of motion; each motion can be used to identify each person. In previous our studies, as well as simple motions, even with complex motions, it has been found that personally identifiable. Also, some research in another study area (sports science [4], zoology [5], behavioral analysis [6]) has used the information of the acceleration sensor, and there is an increasing demand for sensor information.

The data that can be obtained from the acceleration sensor has a variation because of the status of the peripheral circuits. It is possible to distinguish from other individuals by capturing the characteristics of each sensor an individual.

For example, acquired as time-series information from the acceleration sensor in a stationary state. As shown in Figure 1, the analysis of the frequency shows the components of various frequencies

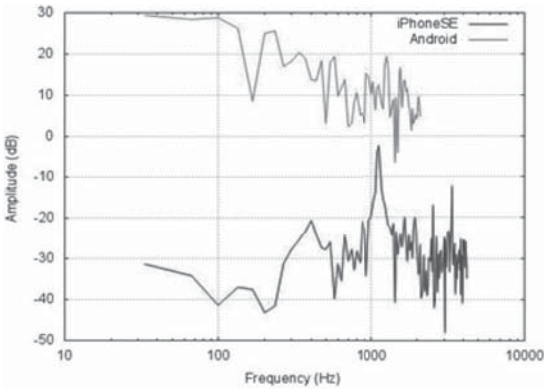


Figure 1 Frequency analysis of acceleration sensors (2 types of mobile phone)

among two models of mobile phone.

By applying this, it is possible to use a different random number seed for each individual in the event of random numbers, it becomes possible to use to identify individuals that owns it. In this study, to identify the accelerometer individuals is tried by using those samples data from a plurality of acceleration sensors. As a result, it was found that we can identify each of these sensors.

2.2 Acceleration Sensor Mechanism and Accuracy

An accelerometer mounted on the portable device or the like, by MEMS (Micro Electro Mechanical System) technology, are manufactured as having both a mechanical structure and an integrated circuit structure on a semiconductor wafer. Therefore, it becomes possible to combine two of an accuracy of the mechanical precision and the integrated circuit; it is the present study focused on this precision. To come out a difference in degree of accuracy in the manufacturing process are aware, it (voltage distribution and temperature characteristics obtained from 1000 individuals or more sensors) which is also described in Specification Sheet of the acceleration sensor. To further retrieve the data from the acceleration sensor, it is necessary to configure the electrical and electronic circuits not least, since the components thereof there is a slight difference in accuracy, it comes out the difference in each manufacturing individual it is inevitably. Focusing on the accuracy of the difference in each individual of these sensors (and peripheral circuit), based on the value output from the sensor, we found differences in individuals, attempts to apply to identifying individuals.

2.3 Data Acquisition of the Acceleration Sensor

The acquisition of the acceleration data is a method obtaining the program from a device with an acceleration sensor and a method receiving from the acceleration sensor itself directly. Acquisition of the data from the devices which have an accelerometer needs to prepare a large number of devices, in the present study, we adopted a method of obtaining from the acceleration sensor itself. In an accelerometer, ADXL327BCPZ of Analog Devices Inc. [7] was used and prepared that attaching a capacitor 0.1 MicroF to the output of the X and Y and Z axes. Input voltage is in the range of from 1.8 to 3.6V (Figure 2).

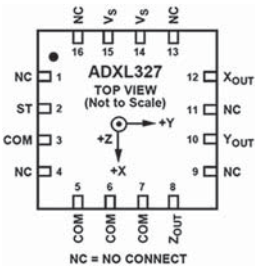


Figure 2 Acceleration sensor: ADXL327CPZ

To obtain the sensor information of each axis from the evaluation circuit, we have used Raspberry Pi 3, which is a kind of microcomputer. The Raspberry Pi produces the power input to the acceleration sensor, but the Raspberry Pi doesn't have any AD converter, so, as shown in Figure 3, the measurement was carried out through the AD converter using MCP3208 (12bit converter). This converter provides the value of the range from 0 to 4095; where, 0 volt equals to 0, and V_{ss} voltage equal to 4095. Table 1 shows a few samples of the output value which are converted and generated by Raspberry Pi. These samples show the values of X, Y and Z axes sensors in a line. For example, the first column of the first line is 2054, which means the X-axis data of the sensor and the value is calculated with the Eq. (1):

$$\mathrm{Axis}_x = \frac{4095 * \mathrm{Volt}_x}{V_{ss}} \tag{1}$$

where Vold_x is the voltage of X axis of sensor and V_{ss} is the voltage provided to the sensor. The second and third column of the Figure is Y- and Z-axis data of the sensor, respectively.

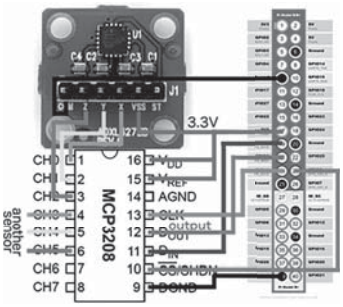


Figure 3 Measurement circuits with Raspberry Pi3

Table 1 A few samples of output from the AD converter

X-axis	Y-axis	Z-axis
2054	2077	1393
2055	2076	1394
2054	2077	1395
2053	2079	1391
2054	2075	1397
…	…	…

We have employed 8 acceleration sensors in the experiments. We put these sensors in on the same installation conditions and environmental conditions. Installation at the measurement evaluation circuit including a sensor fixed to the acrylic plate, which was kept stationary without rotation in on a stable base. Measurement environment is carried out on the stable desk, the experiments were performed in

an atmosphere without vibration, etc. (Figure 4)

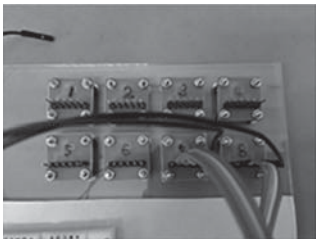


Figure 4 Array of acceleration sensor evaluation boards

2.4 Feature Extraction of the Acceleration Sensor

We have fulfilled frequency analysis of the data obtained from the acceleration sensor with a low-pass filter, and the data returned to time domain are used in the identification of each sensor.

To achieve the identification, we applied the multi-layered perceptron with the back-propagation algorithm. The reason why using the perceptron is that these sensor's data are vast scale (many samples and patterns). The multi-layered perceptron, aka Neural Network, has the feature which adopts the several input parameters to the outputs vector, in other words, which fits the output function with the contribution parameters. This fitting is achieved from the training the network parameters.

In this proposal method, we apply the sensor's output (low-passed) to the input parameters and the sensor individuals to the output. These combinations are from sensor's measurements. Figure 5 shows the characteristics of each sensor. Each sensor has 3-dimensional data, but it is hard to use these complex data as input parameters. Therefore, we use the equation (2.1) to simplify these complex data. Equation (2) calculates the absolute value of 3-dimensional vector data.

$$\text{value} = \sqrt{x^2 + y^2 + z^2}\,. \tag{2}$$

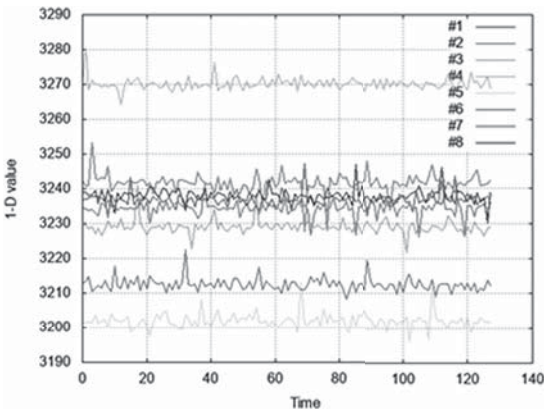


Figure 5 1-D time series of each sensor

2.5 Experiments of Acceleration Sensor Identification

The multi-layered perceptron used in experiments has seven layers; input, output and 5 middle layers. The number of input units is 128, the output unit is 8, and the intermediate layers has 100, 80, 60, 40 and 20 units respectively. The training times is 40,000. The total training and test pattern is 800; test patterns are selected from the total patterns randomly. The ratio of test patterns is 30%. We try to identify the acceleration sensor itself. As the results of identification for eight sensors, we achieve 100% for training datasets and almost 100% for test datasets as the rate of identification. The time of training the perceptron is several seconds. These results are the average score of 20 times experiments. Table 2 illustrates the part of results, trials of which has the ratio of identification except for 100% and the class of which has the ratio except for 100%. The class and trial-sets, those are not shown in Table 2, have the 100% identification ratio.

Table 2 The part of the results of identification ratio

trial	class 1	class 8
1	100.00%	96.00%
3	100.00%	96.77%
6	100.00%	97.56%
7	100.00%	96.88%
9	100.00%	96.55%
14	96.77%	100.00%
17	96.67%	100.00%
18	100.00%	93.94%
average	99.67%	98.89%

2.6 Conclusion

We tried to identify the acceleration sensor itself. As the results of identification for 8 sensors, we achieved almost 100% as the rate of identification with multi-layered perceptron. However, because almost all results show 100% identification ratio, the structure of a neural network is overfitting with training datasets. In the future studies, we plan to grab each sensor's characteristics and apply them to the individual identification.

3. Extraction of Memory-Chip Metrics

3.1 On Extraction of Memory-Chip Metrics

In recent years, authentication using a Physical Unclonable Function (PUF) that generates chip specific values using variations occurring by chance at the time of manufacture attracts attention [8]. In this authentication, inputting data on the chip gives unique output data from each chip. By registering

this unique output data in the server and referring at the time of authentication, authentication of the chip becomes possible.

In this research, we aim to make it possible to identify each USB 3.0 flash memory (USB memory) by extracting device specific characteristic quantities in USB memory like PUF. In previous research [9] [10], we verified whether it is visually distinguishable by acquiring data on whether arbitrary USB memory can be identified in some USB memories and graphing it based on it. In this chapter, using the write speed obtained from the USB memory, etc., it is actually executed using machine learning and decision tree whether each USB memory can be actually identified, and data necessary for the decision tree is specified it is aimed at.

3.2 Measurement Method

USB memory used for measurement is 16 GB products of 6 manufacturers sold in the market (Table 3). In addition, in the ELECOM, it was prepared a plurality of the same model number. File system of USB memory of the experimental subject is a NTFS.

[Measurement Method]: In order to check the transfer speed for these USB memories, the performance monitor attached to Microsoft Windows 8.1 was used. As a file to be transferred, it was prepared those of 0.5GB that was filled with byte data of 0x00. Measurement was performed 10 times with writing to USB memory and reading from USB memory set. Between writing and reading, processing for unmounting volumes was performed once in order to invalidate the cache. Then, in order to check whether there is a difference in transfer speed depending on the data already written, we added a file of 0.5 GB and measured 28 times.

Table 3 Measured USB memories

Manufacturer's name	Model number
ELECOM	MF-RDSU3 16G
TOSHIBA	TransMemory-MX V3KMM-016G-BK
BUFFALO	RUF3-WB16G-BK
I-O DATA	BUM-3C16G/K
TDK	Prime Line UFD16GE-PL3
SanDisk	SDDD2-016G-G46

3.3 Experiment

Weka [11] was used for construction and evaluation of decision trees.

[About Small Data]: Measurement data was obtained by writing data of 0.5 GB and writing data of 0.5 GB consecutively to the 7 USB memories of ELECOM. The data used to construct the decision tree was 280 times of 10 × 28 for each USB memory. For all USB memories, it is 1980 times of data of 7 × 280. Also, the size of the tree and the number of correctly classified instances did not change

even if static elements were deleted.

Table 4 shows the elements used to construct the decision tree to determine what the important factor in constructing the decision tree is. At the time of measurement, what we do not change in value depending on turns is called static element, and what changes value by turn is called dynamic element here.

Table 4 Static elements and dynamic elements

Static Element	Target memory name · Capacity already written · Capacity of written file
Dynamic Element	A write speed average over the whole / B Write time on the whole / C First write average speed / D first maximum write speed (per second) / E second write average speed / F second maximum write speed (per second)

The number of correctly classified instances by the decision tree when using all this element was 91.47%. The size of the decision tree was 61 and the number of leaves was 31.

Table 5 shows the number of correctly classified instances, the size of trees, and the number of leaves in case of removing some elements.

Table 5 Relationship between excluded elements and correctly classified instances

Excluded Dynamic Elements	Correctly Classified Instances	Size of Tree	Number of Leaves
No exclusion	91.47%	61	31
A	91.42%	61	31
B	91.83%	47	24
C	91.78%	51	26
D	86.07%	61	31
E	91.78%	51	26
F	90.30%	39	20
AB	91.63%	53	27
CD	86.32%	55	28
EF	90.51%	35	18
CE	92.04%	47	24
DF	72.96%	63	32
ABCE	91.78%	35	18

Deleting a dynamic element and having extremely fewer instances correctly classified correctly than when including all included cases when deleting one or two maximum speeds. Also, those that deleted and the number of correctly classified instances increased was B · C · E. When ABCE is deleted since the number of correctly classified instances has become less than when deleting only CE,

we think that the total time and so on are slightly affected. When I checked the branch of the constructed decision tree, since D or F frequently occurred, I think that the most important factor is the maximum speed per second.

[For Large Scale Data]: When trying to construct a decision tree for the data acquired in the previous study [9] [10], only the ABCD of the dynamic element and the static element are available in Table 4. The number of data is 1400 in total, 10 times the size of write data (0.5 / 1/2/4/8 GB) × the data size already written (28 times per 0.5 GB) for one USB memory. Because it is acquired for a total of 14 pieces of USB memory is approximately 20,000 of data.

Construct a decision tree for this 20 thousand data. At this time, the number of correctly classified in-stances was 71.47%. The tree size was 2037 and the number of leaves was 1019. Construct the decision tree for ELECOM and other USB memories respectively. When constructing a decision tree other than ELECOM, the number of correctly classified instances was 72.89%. The tree size was 463 and the number of leaves was 232. In contrast, if ELECOM is the only target, the number of correctly classified instances was 79.31%. At this time the tree size was 271 and the number of leaves was 136. From these facts, it was confirmed that by identifying the same type of USB memory at the same time, the number of correctly classified instances increases. Also it was confirmed that the number of incorrectly classified instance for slow USB memory has become many.

3.4 Conclusions

In this chapter, the extraction of the matrix of the USB memory was discussed. For the identification of the USB memory, the maximum speed when several files are written differs for each USB memory, and it is possible to distinguish which USB memory is about 80% when building a decision tree with only that element alone all right. From this, it is thought that the identification accuracy increases when there are multiple data of USB memory of the same maker, but the size of the tree also increases in the same way. Since writing the 0.5 GB file and measuring the maximum speed, since it takes 14 to 25 seconds to write once, if it can measure at high speed by changing the file size or the like, the identification speed because think that it is also possible to improve, I want to advance the investigation.

4. Stabilization of Circuit Metrics based on Matching Circuits

4.1 Introduction

With the great expectations for upcoming 5G mobile communications and Internet of Things (IoT), built-in antennas of wireless communication systems are strongly required to design more compact and broadband. However, since the well-known theoretical limitation called “Chu Limit” defines conflicting

relationship between operational frequency bandwidth and antenna dimensions [12], super compact broadband antennas cannot be realized by the conventional impedance matching technologies.

Recently, non-Foster impedance matching, utilizing non-Foster elements such as negative capacitors and negative inductors, drawn great attentions among antenna researchers as a new technology to provide broader impedance matching [13] [14] [15]. When an E-field-resonance-based electrically small antenna (ESA) is designed, real part of the antenna impedance (radiation resistance) becomes smaller, while imaginary part of the impedance (capacitance at this time) becomes significant. In such a case, by connecting an appropriate negative capacitor in series to the antenna, undesired antenna capacitance can be canceled by the negative capacitor, leading to broadband antenna matching beyond the conventional theoretical limitation.

The non-Foster reactance is an unusual component [16]. When an applied voltage is increasing, conventional capacitors will be charged. However, in case of the negative capacitor, the capacitor will be discharged against the applied voltage [17]. A negative impedance converter (NIC), configured by active elements and positive feedback loops, generates sign-reversed impedance of an impedance element connected to the NIC. Therefore, if a capacitor is connected to the NIC as the impedance element, the NIC will generate negative capacitance. However, the NIC easily becomes unstable because of the positive feedback loop. In Section 4, three types of NICs, that is, a bipolar-transistor-based floating NIC, a bipolar-transistor-based grounded NIC, and an operational-amplifier-based NIC, are introduced and their theoretical and experimental performances are summarized. Finally, feasibility of the non-Foster elements as metrics of circuits and devices is discussed.

4.2 Bipolar-Transistor-Based Floating NICs[2)]

Figure 6a shows circuit configuration of a bipolar-transistor-based floating NIC [18]. Bias circuits and filters to control feedback loop gains are not presented in this figure for better understanding of the operational principle of the NIC. Apart from DC bias voltages, let's consider only alternative currents (AC) here. The notations in the figure v1, v2, va, and vb denote AC voltages on corresponding nodes, and i1 and is are AC currents of corresponding circuit branches. Assume that base current of transistors is small enough comparing with the collector and emitter currents, and it can be ignored. In addition, the base and emitter voltages of each transistor are assume to be the same in terms of AC voltages. Under such assumptions, Eqs. (3), (4), and (5) are obtained as shown in Figure 6b. By substituting these results into Eq. (6), an impedance ZL, connected to the NIC, is sign-reversed into -ZL as shown by Eq. (6). This means that the circuit in Figure 6a works as a 2-port floating NIC.

Figure 6c shows a prototype NIC designed at VHF and UHF bands. The circuit patterns on printed

2) Refer to articles [17] [25] [32] [34] [35] [23] for more information about this subsection.

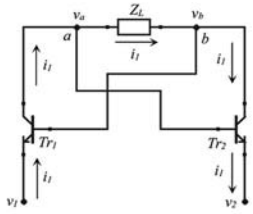
circuit board (PCB) were made by using a milling machine LPKF Protomat S100, and all circuit elements including transistors Renesas NE68133 and other surface mounted devices (SMDs) were soldered on the PCB by cream solder. As an ESA, a monopole antenna operating at 1 GHz was connected to Port 2 of the NIC. For simulations, the monopole antenna was modeled by the series connection of a 3 ohm resistor, a 10 nH inductor, and a 3.0 pF capacitor.

Input impedance and return loss characteristics of the NIC are shown in Figure 6d when the monopole antenna is connected to the NIC. The graphs on left-hand side and right-hand side of this figure present simulated and measured results, respectively. It can be confirmed that the NIC provides better impedance matching at 600 MHz in simulation and 300 MHz in experiment. In this demonstration, we found following features on this NIC.

1) The NIC circuit requires three types of filters on the feedback loop to control the loop gain precisely; one for gain suppression at lower frequencies and two at higher frequencies. If the feedback loop gain is controlled appropriately, the NIC works quite stable.

2) The NIC circuit strongly requires that the AC signals should be blocked perfectly not to flow into the DC biasing circuits. To do this, high performance inductors are indispensable.

3) If high performance inductors are not available, use of current mirrors, resistors and high DC biasing will be useful as an alternative way [14].



(a) Simplified NIC circuit

$$v_1 = v_b \quad (3)$$

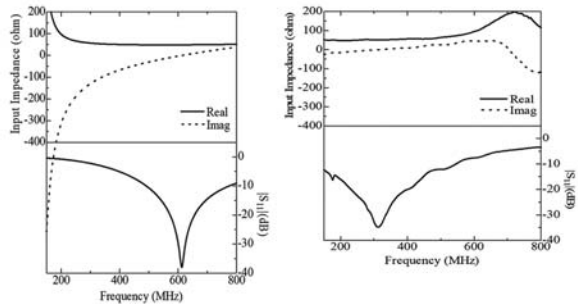
$$v_2 = v_a \quad (4)$$

$$v_a - v_b = v_2 - v_1 = Z_L i_1 \quad (5)$$

$$Z_{in} = \frac{v_1 - v_2}{i_1} = -Z_L \quad (6)$$

(b) Equations

(c) Fabricated NIC



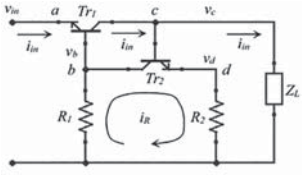
(d) Performance

Figure 6 Bipolar-transistor-based floating negative impedance converters

4.3 Bipolar-Transistor-Based Grounded NICs[3)]

Figure 7a shows circuit configuration of a bipolar-transistor-based grounded NIC [18]. Bias circuits and filters to control feedback loop gains are not presented in this figure. Similarly, let's consider only the AC effects. An input voltage vin is almost equal to the base voltage of vb of Tr1, as shown in Eq. (4.5). The node voltage vc is also equal to the emitter voltage vd of Tr2 as presented in Eq. (8). Since the emitter current is approximately the same with the collector current, an input current iin flows through Tr1, node c and impedance ZL. As a result, Eq. (9) is obtained for ZL. When a loop current iR is defined as shown by Figure 7a, Eqs. (10) and (11) are obtained for R1 and R2, respectively. Finally, by solving these equations, Eq. (12) is derived. This equation means that the NIC response, Zin = -ZL, is obtained when R1 = R2. Figure 7c shows a prototype model of the NIC working at VHF and UHF bands. This circuit was also fabricated on the PCB board by using the same procedure as mentioned in Sec.4.2. For transistors, Renesas NE68133 was used.

In simulations, not only circuit simulator ADS, but also EM-field solver Momentum was utilized to evaluate the NIC performance precisely. In experiment, a vector network analyzer 8714B was connected to Port 1 of the NIC, and input impedance was measured. From imaginary part of the input impedance, generated capacitance was calculated and given in Figure 7d. We have still some errors between simulation and experiment, frequency dependence of these responses are quite similar. The error would be caused due to unexpected inductance induced on the actual NIC and PCB circuits.



(a) Simplified NIC circuit

$$v_{in} = v_b \quad (7)$$

$$v_c = v_d \quad (8)$$

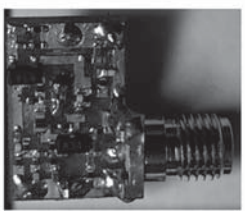
$$v_c = Z_L i_{in} \quad (9)$$

$$v_b = -R_1 i_R \quad (10)$$

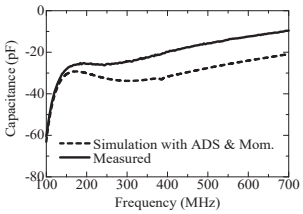
$$v_d = R_2 i_R \quad (11)$$

$$Z_{in} = \frac{v_{in}}{i_{in}} = -\frac{R_1}{R_2} Z_L \quad (12)$$

(b) Equations



(c) Fabricated NIC



(d) Performance

Figure 7 Bipolar-transistor-based grounded negative impedance converters

3) Refer to article [30] for more information about this subsection.

4.4 Operational-Amplifier-Based Grounded NICs[4)]

Figure 8a shows circuit configuration of an operational-amplifier-based grounded NIC. This circuit can be analyzed by applying the following approximations widely applied for ideal operational amplifiers (OPamps). That is,

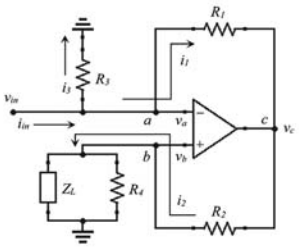
1) input impedance is infinity (currents flowing into input ports can be ignored),

2) output impedance is zero,

3) amplitude ratio is infinity (voltages at both input ports can be treated as identical).

Based on this approximation, Eqs. (13) - (18) shown in Figure 8b are obtained. By solving these equations, an input impedance of the NIC Zin can be derived as Eq. (19). If the relation Eq. (20) is assumed, Zin in Eq. (19) becomes Eq. (21). This means that the circuit works as a grounded NIC.

Figure 8c shows a photograph of a prototype fabricated on PCB. AS for OPamps, Texas Instruments OPA690 was selected. As a sign-reversed impedance Zin, a capacitor C0 with capacitance of 100pF was connected. Two models with R0 = 20 ohm and R0 = 39 ohm were demonstrated and the results are shown in Figure 8d. When R0 = 39 ohm, the NIC generates negative capacitance successfully in theory, but it shows unstable response in experiment. On the other hand, when R0 = 20 ohm, negative capacitance around -500pF is obtained experimentally. We have studied OPamp-based NICs afterwards, and finally, we concluded that OPamp-based NICs were not suitable to generate non-Foster reactance because the inner parameters of the OPamp package cannot be controlled from the outside.



(a) Simplified NIC circuit

$$v_{in} - v_c = R_1 i_1 \quad (13)$$

$$v_c - v_b = R_2 i_2 \quad (14)$$

$$v_{in} = R_3 i_3 \quad (15)$$

$$i_2 = v_b \left(\frac{1}{Z_L} + \frac{1}{R_4}\right) \quad (16)$$

$$v_{in} = v_a = v_b \quad (17)$$

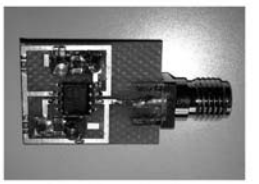
$$i_{in} = i_1 + i_3 \quad (18)$$

$$Z_{in} = \frac{v_{in}}{i_{in}} = \frac{1}{\frac{R_2}{R_1}\left(\frac{1}{Z_L} + \frac{1}{R_4}\right) + \frac{1}{R_3}} \quad (19)$$

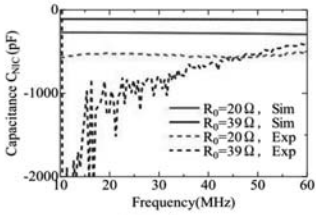
$$R_1 = R_2 = R_3 = R_4 = R_0 \quad (20)$$

$$Z_{in} = -Z_L \quad (21)$$

(b) Equations



(c) Fabricated NIC



(d) Performance

Figure 8 Operational-amplifier-based grounded negative impedance converters

4) Refer to articles [31] [22] [27] [28] [33] [36] [24] [29] for more information about this subsection.

4.5 Feasibility of Non-Foster Reactance as Metrics of Wireless Communication Systems[5)]

Non-Foster impedance matching for ESAs is the most promising and indispensable technique for antenna design to realize high-speed wireless data communication systems. However, it is also true that the non-Foster reactance suffers from the influence of environmental conditions. For instance, tolerance of resistance, capacitance, inductance and amplitude ratio of transistors (those are configuring the NIC circuit) affects total performance of the NIC. As a result, every NIC shows its own peculiar feature in their frequency domain and time domain responses. Generally, such nonidentical behavior should be avoided from industrial products. However, from the view point of device metrics, this feature will be useful to identify wireless communication systems and instruments. We believe that the non-Foster reactance will be a key technology for future highly-secured wireless communication systems.

5. Secure Encoding Method for Saving Metrics

5.1 Regenerating Codes

Large-scale storage systems that save their artificial metrics play an essential role in operating a system for distinguishing artificial objects. Since component failures in storage systems often happen, data have to been stored in redundant ways to ensure their availability. Regenerating codes [19] allow us to encode a message (original data) to n shares in such a way that the following properties are satisfied: (i) reconstruction: the message can be reconstructed from any k shares, (ii) regeneration: any share can be regenerated from any d pieces that are computed from shares. The efficient regeneration is a remarkable property of regenerating codes. This property allows us to shorten the downtime of a storage system.

Since the seminal paper [19] was published, many regenerating codes have been proposed. In addition to above-mentioned n, k, d, regenerating codes have the following parameters: α is the size of a share, β is the size of a piece, and B is the size of a message. These are usually counted by the number of appropriate symbols (e.g., symbols in a finite field). The parameters are written as $[n, k, d, \alpha, \beta, B]$.

Although the objective of regenerating codes originally is to improve the availability of distributed storage systems, the confidentiality of data is often a property required for distributed storage systems. Regenerating codes for achieving the confidentiality, called secure regenerating codes, have been proposed in article [20]. However, previous works on secure regenerating codes are based on information-theoretical security. It causes inefficient storage usage. Specifically, the amount of data after encoding is several times as much as that before encoding. To solve the problem on ineffigcient

5) Refer to article [26] for more information about this subsection.

storage usage, this section describes a secure regenerating code based on computational security. The amount of data after encoding in our secure regenerating code is almost equal to that before encoding.

5.2 Security Definition

The proposed encoding scheme consists of two phases. First, a message is transformed into a pseudo-message by using an all-or-nothing transform. After that, the pseudo-message is encoded with a regenerating code. The all-or-nothing transform is a transform such that any symbol of the pseudo-message is lost, no information on the message is obtained from remaining symbols of the pseudo-message. Owing to the above-mentioned property of the all-or-nothing transform, this composite scheme seems to work well. Unfortunately, it is not true. A counter example was given in article [21]. The previous definition of the all-or-nothing transform, which was given in article [21], is not suitable for discussing the composite scheme; since it assumes that a symbol of the pseudo-message is lost, it does not provide the security when the linear combination of symbols is lost. We here describe a new definition of the all-or-nothing transform that is suitable for discussing the composite scheme.

Definition 1 Let O be an oracle that performs $\Pi = (E, D)$. For a probabilistic algorithm (an adversary) A and $b \in \{0, 1\}$, define an experiment $\mathrm{Exp}_{\Pi}^{\mathrm{aon}}(A, b)$ as follows.

1. The adversary A prepares two distinct messages $(m_1, \ldots, m_B)$, $(\hat{m}_1, \ldots, \hat{m}_B)$, and auxiliary information s that may be some hints when the two messages are produced. The adversary gives the two messages to the oracle O.

2. The oracle chooses a bit $b \in \{0, 1\}$ at random. If $b = 0$, then $(z_1, \ldots, z_{B'}) \leftarrow E((m_1, \ldots, m_B))$. Otherwise $(z_1, \ldots, z_{B'}) \leftarrow E((\hat{m}_1, \ldots, \hat{m}_B))$. Suppose that z_i in the pseudo-message $(z_1, \ldots, z_{B'})$ can be regarded as an element of a finite field F_p. that contains p elements.

3. The adversary gives a $(B' - 1) \times B'$ matrix U that causes the loss of a symbols. Note that U is not square, $B' - 1$ rows in U may be linearly dependent, and all the elements are in F_p.

$$U = \begin{pmatrix} u_{1,1} & \cdots & u_{1,B'} \\ \vdots & \ddots & \vdots \\ u_{B'-1,1} & \cdots & u_{B'-1,B'} \end{pmatrix}$$

4. The oracle returns $v_1, \ldots, v_{B'-1}$ given by

$$\begin{pmatrix} v_1 \\ \vdots \\ v_{B'-1} \end{pmatrix} = U \begin{pmatrix} z_1 \\ \cdots \\ z_{B'} \end{pmatrix} \text{ over } \mathrm{F}_p. \tag{22}$$

5. The adversary guesses the value of b from $v_1, \ldots, v_{B'-1}$, and auxiliary information s, which results in the value of $\mathrm{Exp}_{\Pi}^{\mathrm{aon}}(A, b)$.

The advantage of A is defined as

$$\mathrm{Adv}_{\Pi}^{\mathrm{aon}}(A) = \left| \Pr\left(\mathrm{Exp}_{\Pi}^{\mathrm{aon}}(A, 1) = 1\right) - \Pr\left(\mathrm{Exp}_{\Pi}^{\mathrm{aon}}(A, 0) = 1\right) \right|,$$

and the advantage of Π is defined as

$$\mathrm{Adv}_{\Pi}^{\mathrm{aon}}(q) = \max_{A} \mathrm{Adv}_{\Pi}^{\mathrm{aon}}(A)$$

where q is the number of queries to underlying oracles that are used by E and D if they exist. If $\mathrm{Adv}_{\Pi}^{\mathrm{aon}}(q)$ is not larger than some criterion, then Π is called to be an all-or-nothing transform in the sense of this definition.

The difference from the previous definition is Eq. (22). The previous definition assumes that one pseudo-message symbol is lost. This assumption means that U is a matrix that is obtained by deleting the i-th row from the identity matrix. When a transform confirms to the definition above, even if any linear transform is performed after the transform, the property of an all-or-nothing transform is not compromised.

The previous definition of secure regenerating codes is in the information-theoretically secure model. We relax the definition of secure regenerating codes to the computationally secure model that is based on the indistinguishability of two messages. The following definition means that no information about the message is obtained from shares and pieces.

Definition 2 Let O be an oracle that performs an $[n, k, d, \alpha, \beta, B]$ regenerating code $\Omega = (P, Q, R)$ where P, Q, and R denote an encoding, a reconstructing, and a regenerating algorithm, respectively. An experiment for an adversary A, denoted by $\mathrm{Exp}_{\Omega}^{\mathrm{sr}}(A, b)$, is defined as follows.

1. The adversary A produces two distinct messages, that is, $\left((m_1, \ldots, m_B), (\widehat{m}_1, \ldots, \widehat{m}_B), s\right) \leftarrow A$ where message symbols m_i, $\widehat{m}_i$ are elements in F_p and s denotes auxiliary information. The adversary gives the two messages to the oracle O. Note that if the oracle uses other oracles, the adversary can make queries to the oracles.
2. The oracle chooses a bit $b \in \{0, 1\}$ at random. If $b = 0$, then $C \leftarrow P\left((m_1, \ldots, m_B)\right)$, otherwise $C \leftarrow P\left((\widehat{m}_1, \ldots, \widehat{m}_B)\right)$
3. The adversary asks the oracle to give τ ($\leq l$) shares and μ ($\leq u$) piece vectors, which are denoted by

$$(\mathrm{c}^{(i_1)}, \ldots, \mathrm{c}^{(i_\tau)}), \left(v_{f_1}^{(i_{f1,1}, \ldots, i_{f1,d})}, \ldots, v_{f_\mu}^{(i_{f\mu,1}, \ldots, i_{f\mu,d})}\right),$$

   respectively. The oracle uses algorithms Q, R to compute them. Note that if the oracle uses other oracles to compute them, the adversary can make queries to the other oracles.
4. The adversary guesses the value of b, which results in the value of $\mathrm{Exp}_{\Omega}^{\mathrm{sr}}(A, b)$.

The advantage of A is defined as

$$\mathrm{Adv}_{\Omega}^{\mathrm{sr}}(A) = \left|\Pr\left[\mathrm{Exp}_{\Omega}^{\mathrm{sr}}(A, 1) = 1\right] - \Pr\left[\mathrm{Exp}_{\Pi}^{\mathrm{sr}}(A, 0) = 1\right]\right|,$$

and the advantage of Ω is defined as

$$\mathrm{Adv}^{\mathrm{st}}_{\Omega}(q) = \max_{A} \mathrm{Adv}^{\mathrm{st}}_{\Omega}(A),$$

where q is the number of queries to oracles. If $\mathrm{Adv}^{\mathrm{st}}_{\Omega}(q)$ is not larger than some criterion, then Ω is an $[n, k, d, \alpha, \beta, B, l, \mu]$ secure regenerating code.

5.3 Proposed Encoding Method

Our encoding method is the combination of any existing regenerating code and an all-or-nothing transform that is newly designed to be used for this method. The all-or-nothing transform is implemented with a practical blockcipher such as AES and its security is proved in the ideal cipher model. We here describe a new all-or-nothing transform $\Pi = (E, D)$ where E and D are the forward transform and the backward one, respectively. Suppose that Enc is the encryption of an ideal cipher $\{0, 1\}^{\zeta} \times \{0, 1\}^{l} \rightarrow \{0, 1\}^{l}$, that is, Enc is a keyed permutation from a ζ-bit key and an l-bit message to an l-bit ciphertext.

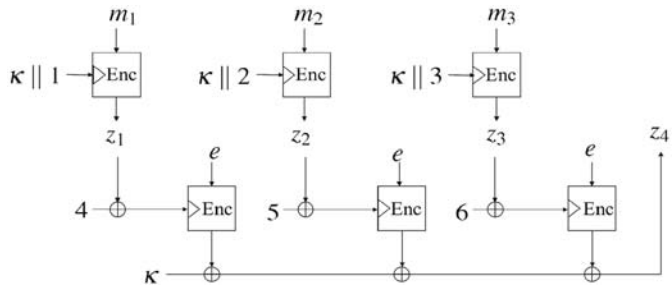


Figure 9 New all-or-nothing transform

The algorithm of E is as follows (Figure 9). Let $(m_1, \ldots, m_B)$ be a message where $m_i \in \{0, 1\}^{l}$ and $\zeta \geq l + \log_2(2B)$. Choose a pseudo-key κ from $\{0, 1\}^{l}$ uniformly at random. For $i = 1, \ldots, B$, compute a pseudo-message symbol z_i as

$$z_i = \mathrm{Enc}(\kappa \| i, m_i),$$

where $\|$ denotes the concatenation operator of strings. Next, for $i = 1, \ldots, B$, compute w_i as

$$w_i = \mathrm{End}(z_i \| (B + i), e), \tag{23}$$

where e is a public constant value (say, all zero bits). Compute the last pseudo-message symbol z_{B+1} as

$$z_{B+1} = \kappa \oplus w_1 \oplus \ldots \oplus w_B.$$

Finally, output $z = (z_1, \ldots, z_{B+1})$ as a pseudo-message.

The transform above E is invertible. Its backward transform D is given as follows. Given the pseudo-message $z = (z_1, \ldots, z_{B+1})$, compute w_i with Eq. (23) for $i = 1, \ldots, B$. The pseudo-key κ can be obtained by

$$\kappa = z_{B+1} \oplus (w_1 \oplus \ldots \oplus w_B).$$

By using κ, the message $(m_1, \ldots, m_B)$ can be obtained by

$$m_i = \mathrm{Dec}\ (\kappa \| i,\ z_i)$$

where Dec is the decryption function of Enc.

Lemma implies that $\Pi = (E, D)$ is the all-or-nothing transform in the sense of Definition 1 if the number of queries to the ideal cipher is much less than 2^l. The proof has been given in article [21].

Lemma 1 The advantage of Π in the sense of Definition 1 is given by

$$\mathrm{Adv}_{\Pi}^{\mathrm{aon}}(q) \le \frac{2(2B+3)q}{2^l - q},$$

where q is the number of queries to the ideal cipher.

The combination of the all-or-nothing transform Π and any regenerating code, denoted by Ω, provides a secure regenerating code. The algorithm of Ω is as follows. Given a message $(m_1, \ldots, m_B) \in \{0, 1\}^{lB}$ where $m_i \in \{0, 1\}^l$, compute a pseudo-message $(z_1, \ldots, z_{B+1}) \in \{0, 1\}^{l(B+1)}$ using E of Π. Consider the pseudo-message as a vector over F_{2^l}, that is, $(z_1, \ldots, z_{B+1}) \in \mathrm{F}_{2^l}^{B+1}$. For the pseudo-message, produce a share $c^{(i)} = \left(c_1^{(i)}, \ldots, c_\alpha^{(i)}\right) \in \mathrm{F}_{2^l}^{\alpha}$ of node i using any $[n, k, d, \alpha, \beta, B+1]$ linear regenerating code G over F_{2^l}. The reconstruction and the regeneration are omitted.

The advantage of Ω is that the overhead caused by achieving the security is only one symbol regardless of B. Hence, the overhead is negligible as B is sufficiently large. Since previous secure regenerating codes requires random symbols as many as message symbols, the overhead cannot be negligible even if B is sufficiently large. This composite scheme Ω is trivially an $[n, k, d, \alpha, \beta, B]$ regenerating code. The following theorem that was proved in article [21] shows that Ω is a secure regenerating code. The premise of the advantage in the following theorem is mainly Lemma 1.

Theorem 1 Suppose that an $[n, k, d, \alpha, \beta, B+1]$ linear regenerating code is used. The composite scheme Ω is an $[n, k, d, \alpha, \beta, B, l, \mu]$ secure regenerating code where $0 \le \mu \le l$ if

$$(l - \mu)\ \alpha + \mu d\beta \le B.$$

The advantage of Ω is given by

$$\mathrm{Adv}_{\Omega}^{\mathrm{sr}}(q) \le \frac{2(2B+3)q}{2^l - q}.$$

6. Concluding Remarks

Hardware security including physical unclonable functions, device fingerprints, and artificial metrics etc. have attracted attention over a few years. For example, the research group on hardware security

has been established in the Institute of Electronics, Information and Communication Engineers, which is the largest academic society on these field in Japan. Research conferences on hardware security have been held in not only Japan but also Europe and the United States.

In consideration of such research trend, we launch research on device fingerprints. This project covered device fingerprints of several different devices and storage systems for device fingerprints. Unlike previous works, we focused on the difference in object's outputs that are caused by the randomness of the semiconductor chip manufacturing process. Although industrial products are generally expected to deliver the same quality, we empirically know that there is an individual difference in the same industrial products. The objective of this project is to quantify the magnitude of such individual differences.

This article summarized results obtained by the project "Further development of identification technology based on device fingerprints." Although each of results were described as in this article, we have two future works: Our device fingerprints are not solidly stable because they are not purposefully equipped with devices. Hence, more precise methods of measuring the characteristic of device fingerprints are required. Another is to evaluate degrading with age of device fingerprints.

Acknowledgments

This is a product of research which was financially supported in part by the Kansai University Outlay Support for Establish Research Centers, 2015 "Further development of identification technology based on device fingerprints." Kenichi MATSUMOTO and Shoji YAMANAKA partially contributed to this research through their master theses at Kansai University.

References

[1] Organisation for Economic Co-operation and Development, "Magnitude of counterfeiting and piracy of tangible products – November 2009 update," 2008. [Online]. Available: http://www.oecd.org/sti/ind/magnitudeofcounterfeitingandpiracyoftangibleproductsnovember2009update.htm.

[2] C. Boehm, M. Hofer, Physical Unclonable Functions in Theory and Practice, Springer, 2013.

[3] R. Maes, Physically Unclonable Functions: Constructions, Properties and Applications, Springer, 2016.

[4] S. K. Keadle, J. N. Sampson, K. L. Haocheng Li, C. E. Matthews and R. J. Carroll, "An Evaluation of Acelerometer-derived Metics to Assess the Daily Behavioral Patterns," *Medicine and Science in Sports and Exercise,* vol.49, no.1, pp.54−63, 2017.

[5] G. Fehlmann, M. Justin O'Riain, P. W. Hopkins, J. O'Sullivan, M. D. Holton, E. L. C. Shepard and A. J. King, "Identification of behaviours from accelerometer data in a wild social primate," *Animal Biotelemetry,* vol.5, no.1, p.6, 2017.

[6] S.-M. Lee, S. M. Yoon and H. Cho, "Human activity recognition from accelerometer data using Convolutional Neural Network," *2017 IEEE International Conference on Big Data and Smart Computing (BigComp),* pp.131−134, 2017.

[7] Analog Device Inc., "ADXL327CPZ Datasheet," [Online]. Available: http://www.analog.com/media/en/

technical-documentation/data-sheets/ADXL327.pdf. [Accessed 30 4 2017].

[8] S. Okumura, S. Yoshimoto, H. Kawaguchi and M. Yoshimoto, "A 128-bit Chip Identification Generating Scheme Exploiting SRAM Bitcells with Failure Rate of 4.45 × 10−19," *IEICE Technical Report,* vol.112, no.15, pp.97−102, 2012.

[9] T. Kambara, "A Method for Identifying USB3.0 Flash Drives," *The 2016 IEICE General Conference,* p.189, 2016.

[10] T. Kambara, "USB3.0 フラッシュメモリに対する個体識別のための特徴量抽出 (only Japanese title)," *The 78th National Convention of IPSJ,* pp.501−502, 2016.

[11] "Weka 3: Data Mining Software in Java," [Online]. Available: http://www.cs.waikato.ac.nz/~ml/weka/. [Accessed 28 2 2017].

[12] L. J. Chu, "Physical limitations of omni-directional antennas," *J. Appl Phys.,* vol.19, pp.1163−1175, 1948.

[13] K. S. Song, "Non-Foster impedance matching and loading networks for electrically small antennas," Dissertation of Electrical and Computer Engineering, The Ohio State University, 2011.

[14] C. R. White, J. S. Colburn and R. G. Nagele, "A non-Foster VHF monopole antenna," *IEEE Ant. Wireless Prop., Lett.,* vol.11, pp.584−587, 2012.

[15] S. E. Sussman-Fort and R. M. Rudish, "Non-Foster impedance matching of electrically-small antennas," *Trans. Ant. & Prop.,* vol.57, no.8, pp.2230−2241, 2009.

[16] R. M. Foster, "A reactance theorem," *Bell Syst. Tech., J.,* vol.3, pp.259−267, 1924.

[17] Y. Horii, "Non-Foster metamaterials composed of non-Foster impedances," *Microwave Workshop and Exhibition (MWE2015), Proceedings,* Vols. FR2A-1, pp.1−10, 2015.

[18] J. G. Linvill, "Transistor negative impedance converters," *Proc. IRE,* vol.41, pp.725−729, 1953.

[19] A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Transactions on Information Theory,* vol.56, no.9, pp.4539−4551, 2010.

[20] S. Pawar, S. E. Rouayheb and K.~Ramchandran, "On secure distributed data storage under repair dynamics," 2010. [Online]. Available: http://arxiv.org/abs/1003.0488.

[21] H. Kuwakado and M. Kurihara, "Secure regenerating codes using linear regenerating codes and the all-or-nothing transform," *IEICE Transactions on Information and Systems,* Vols. E100-D, no.3, pp.483−495, 2017.

[22] S. Yamanaka, Y. Utoku, Y. Horii, "A non-Foster negative capacitance generated by parasitic components of operational amplifiers," *The 5th Korea-Japan Metamaterials Forum, Proceedings,* pp.75−76, 2015.

[23] Y. Horii, "Design of non-Foster elements and their applications," *The Radiation Science Society of Japan, Proceedings,* Vols. RS16−10, 2017.

[24] Y. Horii, K. Matsumoto, S. Yamanaka and R. Tabuchi, "Experimental demonstrations of operational-amplifier-based negative impedance converters (NICs) for generation of negative capacitance," *IEEE APS and URSI, Proceeding,* 2016.

[25] Y. Horii, "New high-frequency technorolies inspired by non-Foster elements," *JSPS, Metamaterials 187, The 6th EM Metamaterial Conf., Proceedings,* pp.14−25, 2016.

[26] Y. Horii, "Prospective of negative impedance converters for device fingerprint technology," *The 5th Korea-Japan Metamaterials Forum, Proceedings,* pp.31−32, 2015.

[27] Y. Horii and S. Takagi, "Theoretical study on stable broadband non-Foster negative capacitors yielded by parasitic reactance of an operational amplifier," *Metamateials 2015, Proceedings,* pp.809−808, 2015.

[28] K. Matsumoto, S. Yamanaka and Y. Horii, "Bandwidth enhancement of negative capacitance generated by operational amplifier based negative impedance converter," *IEICE, Technical Report,* vol.115, no.314, pp.41−46, 2015.

[29] K. Matsumoto, S. Yamanaka and Y. Horii, "Bandwidth enhancement of negative capacitance utilizing circuit pattern of operational amplifier-based negative impedance converters," *IEICE, Electronics Society Conf., Proceedings,* vol. Electronics 1, no. C−2−54, p.64, 2016.

[30] K. Matsumoto, S. Yamanaka and Y. Horii, “Design of Linvill’s negative impedance converters - The present conditions and issues -,” *IEICE, Technical Report,* vol.116, no.363, pp.67−72, 2016.

[31] K. Matsumoto and Y. Horii, “Operational-amplifier-based negative impedance converters for generation of negative capacitance,” *The 5th Korea-Japan Metamaterials Forum, Proceedings,* pp.67−68, 2015.

[32] Y. Horii, “Experimental study on Linvill’s negative impedance converters for generation of pure non-Foster reactance,” *2016 Thailand-Japan MicroWave (TJMW2016), Proceedings,* Vols. FR3−01, 2016.

[33] S. Yamanaka, K. Matsumoto and Y. Horii, “Generation of negative capacitance on a basis of operational amplifier based negative impedance converters,” *IEICE, Technical Report,* vol.115, no.314, pp.35−40, 2015.

[34] S. Yamanaka and Y. Horii, “Influence of parasitic capacitance of transistors in negative impedance converter circuits,” *IEICE, Electronics Society Conf., Proceedings,* vol. Electronics 1, no. C−2−53, p.63, 2016.

[35] S. Yamanaka and Y. Horii, “Stability analysis of negative impedance convereters for deveopment of design procedures,” *IEICE General Conf. Proceedings,* vol. Electronics, 2017.

[36] S. Yamanaka, K. Matsumoto and Y. Horii, “Theoretical study on operational-amplifier-based negative impedance converters with symmetrically allocated impedance elements,” *2015 Asia Pacific Microwave Conference (APMC), Proceeding,* pp.1−3, 2015.