

**A Study on Improvement of EMI Characteristics and
Enhancement of Hardware Security by Suppressing
Mode Conversion Based on Imbalance Matching**

September, 2021

Md. Ashraful Islam

**Graduate School of
Natural Science and Technology
(Doctoral Course)
OKAYAMA UNIVERSITY**

A Study on Improvement of EMI Characteristics and Enhancement of Hardware Security by Suppressing Mode Conversion Based on Imbalance Matching

Copyright © 2021 by Md. Ashraful Islam

All rights reserved.

Printed in Japan

Abstract

In recent years, the use of a wide range of Ethernet communication applications has increased and become popular. Ethernet communication applications are mostly used in automobiles, telecommunication sectors, data security, high-speed data communication systems, etc. Due to the structural difference at the discontinuity point where the cable connects with the printed circuit board (PCB) through the connector, mode conversion occurs and generates common-mode noise. This common-mode noise-induced due to mode conversion in a PCB with attached-cables is one of the significant factors of electromagnetic interference (EMI) issues. It degrades the system performance and causes disturbances to other systems. Besides, the risk of security attacks such as side-channel attacks (SCA) due to EMI, has also increased. SCAs are a major concern for hardware security as different electronic equipment is used indoors and outdoors and is open and easy to access physically.

In order to reduce the common-mode noise, it is essential to suppress mode conversion effectively through mode-conversion analysis, which is one of the factors of EMI. This thesis aims to improve EMI issues in signal transmission system and enhance hardware security of the cryptographic module when secret information leaks outside the module via common-mode current through the power cable. The author achieved both goals by suppressing mode conversion at the interface where the cable (communication/power) connects with the PCB. In this thesis, the author focuses on the following two points to solve the EMI and security issues:

- (A) Mode conversion at the connector section due to imbalance difference between cable and connector section.
- (B) Secret information leakage outside the cryptographic module via the common-mode current in a power cable.

The main objective of this thesis is to achieve (A) and (B). Therefore, a concrete method was proposed for each point to realize (A) and (B). Chapter 3 proposed an imbalance matching method to solve (A), and Chapter 4 applies the mode conversion suppression technique at the discontinuity point on the power delivery network (PDN) for enhancing hardware security to solve (B).

In Chapter 2, modal-equivalent circuit model is used to analyze mode conversion at the connector section that connects the cable with the PCB. The parameter, h , is known as

the imbalance factor, represents the degree of imbalance of a transmission line. When two transmission lines with different imbalance factors are connected, mode conversion occurs at the interface that causes EMI issues in transmission line, and information leakage from the cryptographic module. The modal-equivalent circuit model assumes that the mode conversion electromotive force is proportional to the product of imbalance difference, Δh and the normal-mode voltage, V_n . However, mode conversion can be suppressed by reducing Δh based on imbalance matching between two transmission line or reducing V_n at the discontinuity point on PDN. Based on modal-equivalent circuit model, (A) is achieved in chapter 3, by reducing Δh , and (B) is achieved in chapter 4 by reducing V_n .

Chapter 3 solved point (A). When an STP cable is connected with a PCB via an Ethernet (RJ45) connector, mode conversion occurs at the connector section due to their structural difference that causes the difference in the imbalance factor of the transmission line. This chapter treats two common modes, and the secondary-common mode of the two is recognized as a significant factor of EMI issues in signal transmission line. Suppressing the mode conversion with the secondary-common mode at the Ethernet connector improved EMI issues in signal transmission line. To verify the above idea, mode conversion is suppressed at the connector section based on imbalance matching with the cable section. The inadequate shielding around the connector section causes imbalance difference with the cable section and result in mode conversion at the connector section. The author improved the footprint of female connector by placing a copper layer on the PCB surface, and the inadequate shielding at the edge of the connector section by soldering and wrapping it with copper tape. The imbalance matching is achieved with the improvement around the connector section, and results in the suppression of the mode conversion. The approach is evaluated by comparing the circuit simulation result with the measurement result by using mixed-mode S -parameters as an evaluation index. The simulation result showed that mode conversion is reduced by improving the footprint of the female connector on the PCB surface. It is also observed that the measurement result obtained with the VNA (vector network analyzer) measurement agrees well with the simulation results. Therefore, the effect of the shield-improved connector with an improved footprint of female connector on mode conversion suppression at the connector section is validated experimentally and numerically to improve EMI issues in signal transmission line.

Chapter 4 solved point (B). Secret information can leak via common-mode current in a power cable that delivers power to a cryptographic module, enabling attackers to eavesdrop from a remote location. The secret information initially leaks as normal-mode noise from the cryptographic module, and then mode conversion conveys this secret information as side-channel information from the normal-mode noise to the common-mode current at the connector section where the imbalance factor between the power cable and the trace on a power delivery network (PDN) is discontinuous. This common-mode current is generated due to mode conversion and flows through a power cable as side-channel information. We apply the mode-conversion suppression technique at the discontinuity

point on a PDN to reduce the common-mode current as a side-channel attack (SCA) countermeasure. We place a capacitor at the discontinuity point of an imbalance factor between the trace and the ground layer of the module to suppress mode conversion by reducing normal-mode voltage, V_n . Therefore, the common-mode current in a power cable is also reduced and should enhance SCA resistance of the cryptographic module. To enhance hardware security, this work evaluates the effectiveness of the mode-conversion suppression technique by analyzing the reduced common-mode current with correlation power analysis (CPA). The CPA result shows that correlation values were decreased with the capacitor at this discontinuity point. The experimental result also shows that the number of key bytes disclosed decreases with the mode conversion suppression technique. Therefore, the impact of the mode conversion suppression technique by reducing the value of V_n at the discontinuity point is experimentally validated to enhance SCA resistance when information leakage occurs far from the cryptographic module via the common-mode current in a power cable.

Acknowledgments

This thesis is a summary of my doctoral study at Department of Electronic and Information Systems Engineering, Okayama University. I am grateful to a large number of people who have directly and indirectly helped me finish this work.

First of all, I would like to express my deep gratitude to Professor Yoshitaka Toyota, my supervisor, who has granted me the chance to start this research, and has given me innumerable advice and unrelenting encouragement. Thank is extended to Professor Kazuhiro Uehara who have given me much precious advices on the course of this research. I am also deeply grateful to Assistant Professor Kengo Iokibe for his constructive comments, advices, and enthusiastic arguments which inspired many of the ideas in this thesis. I am also indebted to Professor Yasuyuki Nogami for his helpful comments and great insight during the discussion of my research work.

I am also grateful to all present and past members of Optical and Electromagnetic Waves Laboratory, Okayama University. My sincere appreciation is due to all of my lab members for their kind-hearted supports that inspired to complete my thesis work. I particularly thank to the following present members in our lab, who did much of the technical work and helped me overcome the difficulties encountered in my studies: Mr. Shuqi Zhang, Mr. Sao Kanao, Mr. Shohei Kan, Mr. Daiki Kameyama, Mr. Tomoaki Kan, Mr. Tomoya Takeuchi, Mr. Ryuta Nakasishi, Mr. Hiroaki Iwasaki, Mr. Zhenhong Xu, Mr. Masaki Himuro, Ms. Mio Ohara, Mr. Shuhei Kodama, Mr. Kohei Shimoda, Mr. Hiroki Takahashi, Mr. Kairi Terado, Mr. Noaki Nishikawa, Ms. Kanon Hamura and Mr. Ryohei Harada. I would like to thank specially Mr. Irishika, Mr. Mori, Mr. Kanao and Mr. Himuro for their premilitary support to develop my knowledge on my research field. I also thankful to Mr. Wang and Mr. Satano who gave me mental support and inspired me during my research work. I feel proud to have such a wonderful and supportive people around me.

Finally, I would like to dedicate this thesis to my parents, Ms. Dill Afroza Parvin and Mr. Md. Aminul Islam, My wife, Ms. Shammi Akhter and My son, Md. Abu Bakar Siddik Tahsin in appreciation of their unconditional support and continuous encouragement throughout the thesis. I would also like to thank Almighty Allah for all the blessings, without which none of this would have been possible.

Contents

Abstract	i
Acknowledgments	v
List of Variable	xvii
1 General Introduction	1
1.1 Background	1
1.2 Motivation	2
1.3 Structure of the Thesis	8
2 Mode Conversion Analysis by using Modal-equivalent Circuit Model	11
2.1 Introduction	11
2.2 Imbalance Factor of Transmission line	12
2.2.1 Definition of Imbalance Factor	12
2.2.2 Imbalance Factor for Different Transmission Line Structure	12
2.3 Mode conversion due to Imbalance Difference	14
2.4 Modal-equivalent Circuit Model for Analysis Mode Conversion	17
2.4.1 Mode Conversion Mechanism	18
2.4.2 Construction of Modal-equivalent Circuit Model for 4-conductor Transmission Line	21
2.5 Application of Modal-equivalent Circuit Model	26
2.5.1 Mode Conversion Suppressing at Ethernet Connector to Solve EMI Issues	26
2.5.2 Mode Conversion Suppression Technique to Enhance Hardware Se- curity	26
2.6 Conclusion	29
3 Mode Conversion Suppression at Connector Section based on Imbalance Matching	31
3.1 Introduction	31
3.2 LAN Cable and Ethernet Connector	35
3.2.1 LAN Cable for analysis Mode Conversion	35

3.2.2	Etherent Connector for analysis Mode Conversion	36
3.2.3	Connection Scenario between LAN Cable and Ethernet Connector .	37
3.3	Improvement around Connector Section for Imbalance Matching	38
3.3.1	Improvement of Female Connector Footprint on PCB Surface	39
3.3.2	Improvement of Shielding around Connector	40
3.3.3	Imbalance Matching Due to Improvement around Connector Section	42
3.4	Measurement of Mode Conversion Suppression	44
3.4.1	Evaluation System	45
3.4.2	Measurement Result	48
3.5	Estimation of Mode Conversion by using Modal-Equivalent Circuit Model .	54
3.5.1	Modal-equivalent Circuit Model for Estimating Mode Conversion .	54
3.5.2	Simulation Result obtained from Modal-equivalent circuit	56
3.6	Verification of Mode Conversion Suppression Method by Comparing Mea- surement Result with Simulation Result	61
3.7	Conclusion	63
4	Enhancement of Hardware Security through Mode Conversion Analysis	65
4.1	Introduction	65
4.2	Information Leakage via Common-mode Current	67
4.3	Mode Conversion Suppression Technique at Connector Section of PDN to Enhance Hardware Security	69
4.3.1	Mode Conversion Suppression Technique to Enhance Hardware Se- curity	70
4.3.2	Reduction of Normal-mode Voltage V_n by Placing Capacitor at the Discontinuity Point on the PDN	73
4.4	Measurement Setup	75
4.4.1	Test Board for Analysis	75
4.4.2	Target Encryption Algorithm and Correlation Power Analysis (CPA)	77
4.4.3	Experimental Setup and Measurement Condition	79
4.5	Measurement Result	83
4.5.1	Measurement of Normal-mode Voltage and Common-mode Current for different conditions	83
4.5.2	CPA Result	85
4.6	Conclusion	87
5	General Conclusion	89
A	Mixed-mode S-parameter for 4-port Netwrok	93
B	Mixed-mode S-parameter for Imperfect Transmission Line	97
	Bibliography	103

Contents

ix

Research Activities

111

Biography

113

List of Figures

1.1	Communication system for exchange information.	3
1.2	Noise issues in signal transmission system (a) 4-conductor transmission line (b) cross-sectional view of the connector section (c) cross-sectional view of the cable section	4
1.3	Information leakage due to mode conversion at the discontinuity point on the PDN.	6
1.4	Structure of thesis.	10
2.1	Current is divided between two orthogonal modes.	13
2.2	Mode conversion occur due to imbalance difference.	14
2.3	Factors that causes mode conversion (a) Mode conversion at pigtail termi- nation (b) Mode conversion at connector section (c) Mode conversion at the discontinuity point on PDN.	15
2.4	Orthogonal modes (a) 3-conductor transmission system (a) 4-conductor transmission system.	17
2.5	Modal voltage and modal current for transmission line with different im- balance factor.	20
2.6	Mode-equivalent circuit of a 4-conductor transmission system.	22
2.7	Mode equivalent circuit under condition $h_{1a}=h_{1b} = 0.5$	23
2.8	Mode conversion when imbalance factor $h_{1a}=h_{1b}=0.5$	25
2.9	Modal-equivalent circuit for 3-conductor transmission system.	27
3.1	Analysis of mode conversion at the connector section of a 4-conductor trans- mission line (a) side view (b) top view.	32
3.2	LAN cable for analysis mode conversion in Ethernet commuication. (a) LAN cable with 4-pair of STP cable (b) Cross-sectional view of LAN cable (c) Single pair STP-cable (d) Single STP-cable is considered as 4-conductor transmission line	35
3.3	Ethernet connector of male type (a)unshielded (b)shielded (c) pin configu- ration.	36
3.4	Ethernet connector of female type (a)unshielded (b)shielded (c) pin con- figuration.	36

3.5	Footprint of female connector (a) original footprint of female connector on PCB surface (b) improved footprint of female connector on PCB surface (c) cross-sectional view of PCB layer.	38
3.6	PCB used in this experiment (a) before improvement (b) after improvement	39
3.7	Original connector with improved PCB structure.	40
3.8	Improved shielding around connector.	41
3.9	Improved shielding around male connector (a) original connector (b) shield improved connector.	42
3.10	Printed Circuit Board (PCB) used for measurement (a) top view (b) cross-sectional view.	44
3.11	Stand used to hold PCB above system ground.	45
3.12	STP-cable system for validation.	46
3.13	Port definitions: (a) Ports I to IV in VNA measurement of standard S -parameters; (b) Logical ports 1 to 3 for evaluation by single-ended mixed-mode S -parameters.	47
3.14	Measured spectra of (a) S_{nn11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.	49
3.15	Measured spectra of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.	50
3.16	Measured spectra of (a) S_{ns12} (S_{sn21}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ns13} (S_{sn31}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.	51
3.17	Measured spectra of (a) S_{ps12} (S_{sp21}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ps13} (S_{sp31}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.	52
3.18	Measured spectra of S_{ss23} (S_{ss32}) indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.	53
3.19	Modal-equivalent circuit for circuit simulation.	54

3.20	Simulation result of (a) S_{nn11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.	56
3.21	Simulation result of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.	57
3.22	Simulation result of (a) S_{ns12} (S_{sn21}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ns13} (S_{sn31}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.	58
3.23	Simulation result of (a) S_{ps12} (S_{sp21}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ps13} (S_{sp31}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.	59
3.24	Simulation result of S_{ss23} (S_{ss32}), indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.	60
3.25	Measured and simulation spectra of S_{ps12} (a) Up to 600MHz (b) At first resonance frequency.	62
4.1	PDN of SASEBO-G board from power supply to cryptographic FPGA. . .	67
4.2	Capacitor mounting position on PDN for suppressing mode conversion. . .	69
4.3	Circuit diagram of PDN based on Fig. 4.2.	69
4.4	Real picture of capacitor mounting position on cryptographic module. (a) Capacitor mounted close to the cryptographic FPGA, (b) Capacitor mounted at the discontinuity point, (c) Capacitor mounted on the board 20 mm far from the discontinuity point.	71
4.5	Impedance of capacitor.	72
4.6	Equivalent circuit based on the circuit diagram of Fig. 4.3	73
4.7	Simplified equivalent circuit.	74
4.8	SASEBO-G board. (a) top layer (b) soldering layer.	76
4.9	Layers of SASEBO-G board. (a) Layer view (b) Side view.	77
4.10	Flow of AES operation.	78
4.11	Measurement Setup.	79
4.12	Measurement diagram for normal-mode voltage, V_n	81

4.13	Measurement diagram for common-mode current, I_c .	82
4.14	Measured Waveform of normal-mode voltage, V_n .	83
4.15	Probe output detect the measured waveform of common-mode current, I_c .	84
4.16	Correlation coefficient variation.	85
4.17	Number of disclosed bytes of secret key.	86
A.1	Evaluation system for 4-port network.	93
A.2	Reflection characteristics of (a) Normal-mode and (b) Primary-common mode	94
A.3	Transmission characteristics of (a) Normal-mode and (b) Primary-common mode.	95
A.4	Transmission characteristics of mode conversion between normal-mode and primary-common mode.	95
A.5	Reflection characteristics of mode conversion between normal-mode and primary-common mode.	96
B.1	Evaluation system for imperfect transmission line (Combination 1).	98
B.2	Measured spectra of (a) S_{nn11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.	99
B.3	Measured spectra of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.	100
B.4	Measured spectra of (a) S_{ns12} (S_{sn21}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ns13} (S_{sn31}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.	101
B.5	Measured spectra of (a) S_{ps12} (S_{sp21}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) S_{ps13} (S_{sp31}), indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.	102
B.6	Measured spectra of S_{ss23} (S_{ss32}) indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.	102

List of Tables

3.1	Pair connection between LAN cable and Ethernet connector.	37
3.2	Imbalance factors of STP cable and connector section.	43
3.3	Measurement conditions of the vector network analyzer.	48
3.4	Modal parameters of STP cable and connector section.	55
3.5	Coefficient of mode conversion source at connector section.	55
4.1	Different measurement conditions.	70
4.2	Variable in Fig. 4.6 and Fig. 4.7	74
4.3	Common parameters for the measurement of the waveform of V_n and I_c . . .	80
4.4	Measurement equipment and condition.	80
4.5	Different measurement conditions.	84
B.1	Different Combinations.	97

List of Variable

Variable	Meaning
I_n	common-mode current
I_p	primary-common mode current
I_{p1}	primary-common mode current through conductor #1
I_{p2}	primary-common mode current through conductor #2
I_s	secondary-common mode current
I_{s1}	secondary-common mode current through conductor #1
I_{s2}	secondary-common mode current through conductor #2
I_{s3}	secondary-common mode current through conductor #3
V_n	normal-mode voltage
I_c	common-mode current
ΔV_c	common-mode electromotive force
h_1	imbalance factor defined by primary-common mode
h_2, h_3	imbalance factor defined by secondary-common mode
Δh	imbalance difference between two transmission lines
V_1, V_2, V_3	actual voltage
I_1, I_2, I_3	actual current
V_n, V_p, V_s	modal voltage
V_{na}, V_{pa}, V_{sa}	modal voltage of cable section
V_{nb}, V_{pb}, V_{sb}	modal voltage of connector section
I_n, I_p, I_s	modal current
I_{na}, I_{pa}, I_{sa}	modal current of cable section
I_{nb}, I_{pb}, I_{sb}	modal current of connector section
$\mathbf{T}_v, \mathbf{T}_i$	mode conversion matrix
$\mathbf{T}_{va}, \mathbf{T}_{ia}$	mode conversion matrix of the cable section
$\mathbf{T}_{vb}, \mathbf{T}_{ib}$	mode conversion matrix of the connector section
ε	effective permittivity
Z	modal characteristic impedance
Z_T	transfer impedance
S_{nn11}	reflection characteristics of normal-mode at Logical port 1
S_{pp11}	reflection characteristics of primary-common mode at Logical port 1
S_{ss22}	reflection characteristics of secondary-common mode at Logical port 2

S_{ss33}	reflection characteristics of secondary-common mode at Logical port 3
$S_{np11}(S_{pn11})$	transmission characteristics of mode conversion between the normal-mode at Logical port 1 and primary-common mode at Logical port 1
$S_{ns12}(S_{sn21})$	transmission characteristics of mode conversion between the normal-mode at Logical port 1 and secondary-common mode at Logical port 2
$S_{ns13}(S_{sn31})$	transmission characteristics of mode conversion between the normal-mode at Logical port 1 and secondary-common mode at Logical port 3
$S_{ps12}(S_{sp21})$	transmission characteristics of mode conversion between the primary-common mode at Logical port 1 and secondary-common mode at Logical port 2
$S_{ps13}(S_{sp31})$	transmission characteristics of mode conversion between the primary-common mode at Logical port 1 and secondary-common mode at Logical port 3
$S_{ss23}(S_{ss32})$	transmission characteristics of mode conversion between the secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3
C_1, C_2, C_3	common capacitor on PDN
C_x	capacitor at the discontinuity point and 20 mm far from the discontinuity point
Z_{power}	impedance of the power supply
Z_x	impedance of the decoupling capacitor C_x
Z_e	Thevenin's equivalent impedance
V_e	Thevenin's equivalent voltage source
Z_s	internal impedance of the noise source
I_{source}	noise source
Z_{cable}	impedance of the power cable
Z_{con}	impedance of the connector on the board
L	ESL of the total trace on the SASEBO-G board
L_1	ESL of the trace between the two ports "d" and "b"
L_2	ESL of the trace between the two ports "b" and "e"

Chapter 1

General Introduction

1.1 Background

Electromagnetic compatibility (EMC) is a major problem for the designers of electrical and electronic equipment. These EMC issues include two problems. One is electromagnetic interference (EMI) due to undesirable electromagnetic radiated and conducted emissions from electronic devices, and might affect the operation of other devices and the device itself. Moreover, the other one is Electromagnetic Susceptibility (EMS), also known as the immunity of electronic devices. It is essential for every electronic device not to be affected by the surrounding external electromagnetic environment. Unfortunately, the electromagnetic environment surrounding the electrical and electronic equipment becomes worse than ever because the electromagnetic interference (EMI) is increasing due to a large amount of conducted or radiated electromagnetic noise.

Along with the increase in EMI, EMI regulation levels of various standards become stringent. Thus, the design of every piece of electronic equipment should meet the requirement of an acceptable radiated emission level. Several organizations determine this adequate level of radiated emission. For example, VCCI (Voluntary Control Council for Interference by Information Technology Equipment) in Japan, FCC (Federal Communications Commission) in the U.S.A, and CENELEC (Comite European de Normalisation Electrotechnique) in Europe, etc., which also highlights the importance and urgency of EMC related issues. If any electronic equipment is found to be higher radiated emission than the acceptable level, the equipment is not allowed to be sold or manufactured. Therefore, electromagnetic compatibility (EMC) design to control the EMI becomes increasingly essential.

Hence, to predict and reduce radiated emissions, we should understand the reason for EMI generation. Common-mode noise is one of the major reason for EMI issues, generated due to mode conversion at the connector section that connects the cable (communication/power) with the printed circuit board (PCB). This common-mode noise-induced due to mode conversion in a printed circuit board (PCB) with attached cables is one of the significant factors of electromagnetic interference (EMI) issues [1–4] that the electro-

magnetic emissions from a system interfere with the regular operation of other systems. Furthermore, Common-mode also becomes a major threat for hardware security as the secret information leaked outside the cryptographic module via common-mode current. In order to solve this issue, it is essential to suppress the mode conversion effectively through mode-conversion analysis. Mode conversion is obtain from the product of imbalance difference, Δh between two transmission line and the normal-mode voltage, V_n at the interface of the power delivery network (PDN) where the power cable connected with the device. Mode conversion can be suppressed by reducing the value of Δh or the value of V_n .

The purpose of this thesis is to suppress the mode conversion effectively to solve the EMI issues in signal transmission system by reducing the value of imbalance factor difference, and enhance hardware security of cryptographic module by reducing the value of the normal-mode voltage, V_n .

1.2 Motivation

Recently, we are entirely dependent on the communication system for communicating with each other, and for our daily work such as online meetings, online classes, online shopping, online payment, and many other confidential and non-confidential work. Moreover, the recent world pandemic also forces us to work all of our tasks remotely. Therefore, it is noticeable that people exchange enormous amounts of information globally by using communication equipment. For this reason, they use a cell phone, laptop, or desktop as a communication device and connect them with the internet through different communication cables. It is observed from the Fig. 1.1 that different communication device is connected to the internet through the communication cable. LAN cable is widely used as a communication cable that connects with the communication equipment through an connector.

The structural difference between the cable section and the connector section causes imbalance difference and mode conversion occurs at the interface. Therefore, the common-mode current is generated and flowing through the device. This common-mode current often causes electromagnetic interference (EMI) issues and interrupts the normal operation of the system. As a result, it degrades the system performance and causes disturbances to other systems. Besides, the risk of hardware security attacks due to EMI has increased. Hardware security (HWS) attacks such as side-channel attacks (SCAs) [5] are concerned because different electronic equipment is used indoors and outdoors and is open and easy to access physically. Recently, the vulnerability of CPUs to SCA has been reported [6].

Not only the EMI regulation level of electronic equipment but also SCA resistance criteria are needed to monitor. Various organizations monitored the SCA resistance level stringently. Such organizations are IPA (Information-technology Promotion Agency) in Japan, NIST (National Institute of Standards and Technology) in the U.S. Therefore, it

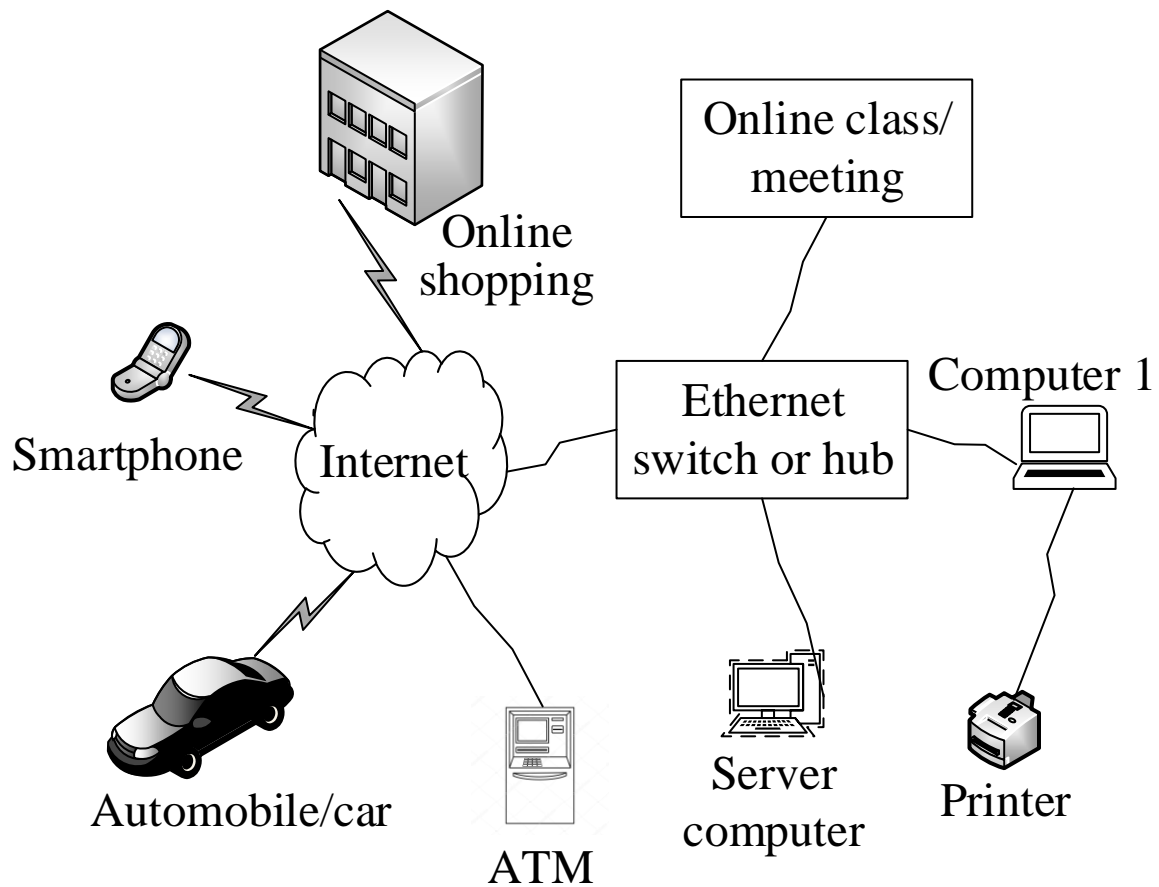


Figure 1.1 Communication system for exchange information.

is essential to solve the EMI issues and enhance the hardware security by suppressing mode conversion at the interface where the imbalance factors are different between two connected transmission lines.

Therefore, in this thesis work, we have studied the following two issues to solve the EMI problem in signal transmission line and enhance hardware security of cryptographic module:

- (A) Mode conversion at connector section due to imbalance difference between cable and connector section.
- (B) Secret information leakage outside the cryptographic module via the common-mode current in a power cable.

The main objective of this thesis is to achieve (A) and (B). If (A) and (B) are ideally achieved, then EMI issues are expected to solve signal transmission line and also counteract the secret information leakage from outside the cryptographic module. Thus,

EMI and immunity issues are solved by achieving (A), and enhance hardware security by achieving (B).

For issue (A)

It is observed from Fig.1.2 that the LAN cable is connected with PCB through an Ethernet connector. It is observed that the LAN cable is directly connected with the male connector, and the male connector is connected with the female connector that is mounted on PCB. The male and female connectors are connected to become a connector section that connects the LAN cable with PCB. The male and female connector may be shielded and unshielded, whereas the LAN cable may also be shielded and unshielded. For achieving (A), we consider a 4-conductor transmission line where shielded LAN cable is connected with the shielded connector.

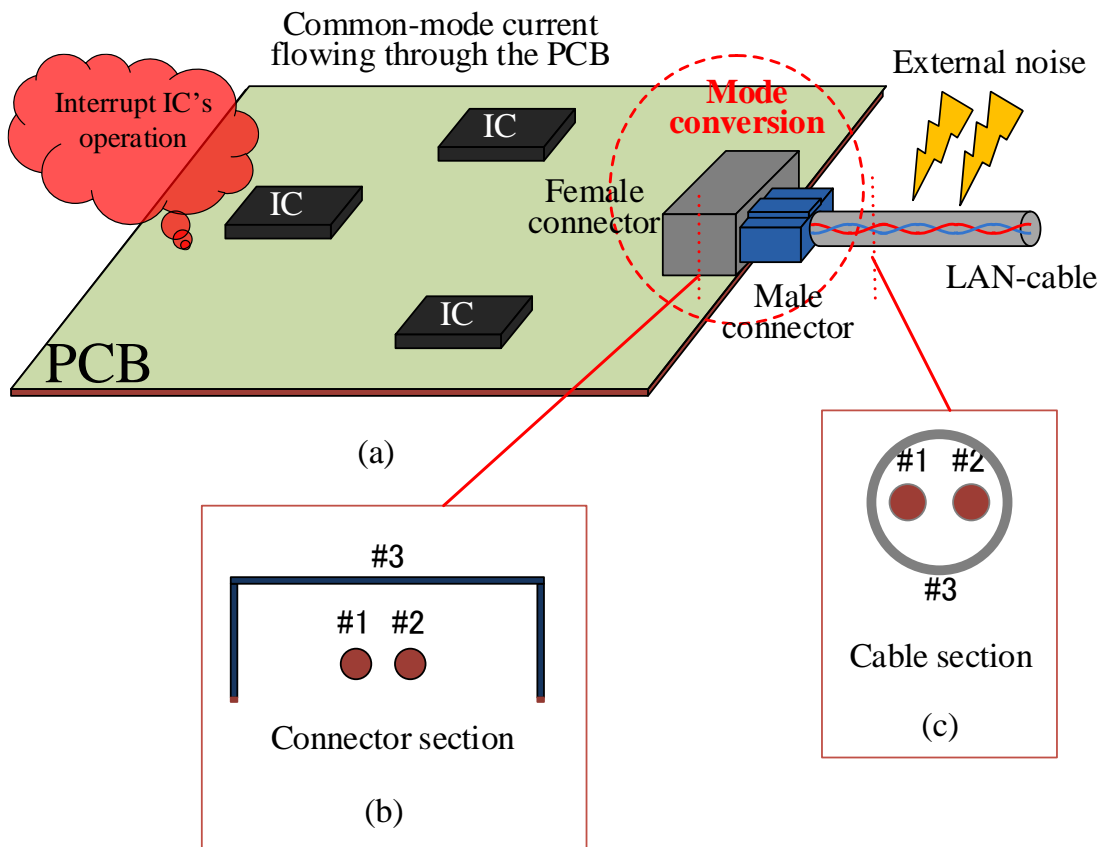


Figure 1.2 Noise issues in signal transmission system (a) 4-conductor transmission line (b) cross-sectional view of the connector section (c) cross-sectional view of the cable section

Fig. 1.2 (b) and (c) show the cross-section of the Ethernet connector and LAN cable, respectively. It is noticeable that the structural difference between the cable section and

the connector section causes imbalance difference at the interface and result in mode conversion at the connector section. Common-mode current-induced due to mode conversion in a printed circuit board (PCB) with attached cables, often causes electromagnetic interference (EMI) issues that the electromagnetic emissions from a system interfere with the regular operation of other systems. In order to solve the issues, it is important to suppress the mode conversion at the interface between two transmission line. Mode conversion is suppressed by reducing the value of imbalance factor difference, Δh or the value of the normal-mode voltage, V_n at the discontinuity point. To achieve (A), mode conversion is suppressed by reducing the value of imbalance difference based on imbalance matching between two transmission lines.

Several models were developed to analyze mode conversion. Two equivalent models have been proposed in [7] to investigate the mode conversion from differential mode (called normal mode in this thesis paper) to common mode in PCBs. Such models are commonly referred to as current-driven and voltage-driven models. The current-driven and voltage-driven models were experimentally validated by investigating common-mode current on the attached cables in [2, 8]. Many researchers [2, 8–12] observed the current-driven model as a dominant source of radiation emission from PCB with an attached cable between these two models. In addition, a voltage-driven model was developed to estimate the radiated emissions from the PCB with the attached cables [13].

On the other hand, the novel model, called the imbalance difference model, was proposed to determine radiated emissions due to common-mode current-induced due to mode conversion in the trace-board structure having two transmission lines with the structural difference [14, 15]. In the model, the current division factor, also known as the imbalance factor, was introduced to analyze mode conversion based on the difference in the current division factor. Then, the model was validated by demonstrating the EMI reduction due to the guard-traces designing based on the model [16, 17].

The imbalance difference model can significantly simplify the mode conversion analysis focusing on different imbalance factors of the transmission lines but treats only normal-to-common mode conversion. In [18, 19], we introduced a modal-equivalent circuit model with mode conversion sources for analyzing mode conversion considering common-to-normal mode conversion as well as normal-to-common mode conversion in a 3-conductor transmission system. A similar approach for mode-conversion analysis between the two orthogonal modes is also provided [20, 21].

In addition, we first developed the modal-equivalent circuit for a 4-conductor transmission system to analyze mode conversion among three orthogonal modes of normal mode, primary-common mode, and secondary-common mode [22]. It was elucidated that pigtail termination of 2-m shielded-twisted-pair (STP) cable affects the mode conversion among the three orthogonal modes in the 4-conductor transmission system with the STP cable. However, as far as the balanced cable is used with Ethernet (RJ45) connectors, mode conversion only occurs between primary- and secondary-common modes. Furthermore, it was experimentally confirmed in [23] that the improve-shielding around the Ethernet

connectors achieved imbalance matching with the cable section and result in suppression of the mode conversion between primary- and secondary-common modes. Then, the modal-equivalent circuit model for the 4-conductor transmission system is used to evaluate the relationship of mode conversion suppression with the shield improvement around the connector section quantitatively from the viewpoint of the imbalance matching.

For issue (B)

It is observed from Fig. 1.3 that a power delivery network (PDN) deliver power to the cryptographic module through the power cable and traces on the module that are connected through the on-board power connector. The structural difference causes the discontinuity in the imbalance factor between the cryptographic module and the power cable on PDN. Therefore, mode conversion occurs, and generates common-mode current, I_c that flows through the power cable. Attackers can acquire the waveform of the common-mode current flows through the power cable and analyze with correlation power analysis (CPA), [24] a primary side-channel analysis method for hardware security attack, such as side-channel attack (SCA).

During encryption or decryption of those cryptographic modules, secret information can be leaked as side-channel information [25] via common-mode current in a power cable [26,27]. If the attacker can retrieve the secret information outside the cryptographic module via common-mode currents on the connected power cable, it would be a major threat to hardware security because attackers would access the connected power cables even if they cannot access the module directly. Therefore, it is essential to suppress mode conversion at the discontinuity point to reduce common-mode current, and enhance the hardware security of the cryptographic module. To achieve (B), V_n at the discontinuity point on the PDN, is reduced to suppress mode conversion.

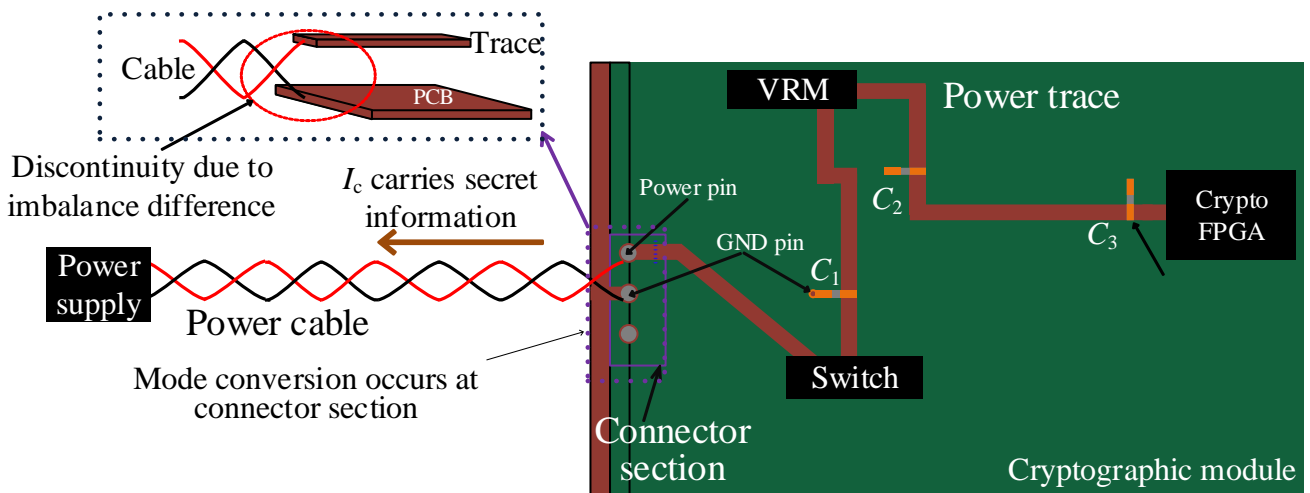


Figure 1.3 Information leakage due to mode conversion at the discontinuity point on the PDN.

Many articles and research works have been published on side-channel attacks (SCA), and countermeasures against them by focusing on algorithms and implementation at both hardware and software levels [25, 28, 29]. It was reported in [30–34] that the attacker is able to measure the side-channel information if the attacker has direct access to the cryptographic module. Some research works [26, 35–37] proposed countermeasure against SCA by using a decoupling circuit on the power traces. However, it is always not possible to acquire side-channel information closely as the cryptographic modules with countermeasures such as electromagnetic shielding and tamper-sensing mesh, can prevent attackers from intruding on their security boundaries. Hence, it is not possible to obtain side-channel information with such countermeasures. However, if the attacker can access the side-channel information far from the cryptographic module, it becomes vulnerable to side-channel attacks. Based on this concept, in [31, 32], proposed an attack, known as electromagnetic analysis (EMA) attack, that is successfully able to measure side-channel information without close access to the module even if there remains a possibility to extract secret information due to EM radiation from the cryptographic module. However, the value of EM radiation is below the value specified in EMC guidelines [38, 39]. Moreover, it may increase the probability of extracting the secret information by analyzing the acquired radiation waves.

We consider here to measure common-mode currents [40] on cables attached to cryptographic modules as shown in Fig. 1.3. It was confirmed in [26, 27, 41] that the common-mode current on cables attached to cryptographic modules contains secret information. It is also known that common-mode current is one of the dominant factors on noise emissions [2, 9, 42–44]. Therefore, there is a possibility that the signal contains the secret information can propagate long-distance via common-mode current as of the side channel information for the attacker. In that case, the attacker in the remote place can acquire the waveform of common-mode current and analyze its characteristics to reveal the secret information.

In [26] the author placed a decoupling capacitor near the cryptographic FPGA to countermeasure against SCA when the secret information leaks outside the cryptographic module via common-mode current. This method reduces the supply voltage fluctuations and provides insufficient reduction of common-mode current in a power cable. Therefore, we need to reduce the common-mode current generated due to mode conversion at the discontinuity point on the PDN, as shown in Fig. 1.3. A capacitor is placed at this discontinuity point on PDN of the imbalance factor to reduce the normal-mode voltage, V_n and hence suppressed mode conversion. Therefore, the flow of common-mode current in a power cable is also reduced, and attackers have less side-channel information to reveal the secret information. The mode conversion suppression technique is applied at the discontinuity point on the PDN to enhance hardware security by improving SCA resistance when information leakages occur far from the cryptographic module via the common-mode current.

1.3 Structure of the Thesis

Fig. 1.4 shows the outline of this thesis. The background and motivation of this thesis are introduced in this chapter. At first, Chapter 2 describes the modal-equivalent circuit model for analysis mode conversion at the interface where two transmission lines with different imbalance factors are connected. Chapter 3 proposed an imbalance matching method at the connector section to improve EMI issues by suppressing mode conversion at the Ethernet connector. The proposed imbalance matching method is validated by comparing the experimental result with the simulation result, obtained from the modal-equivalent circuit model. In chapter 4, the mode conversion suppression technique is applied at the discontinuity point on the PDN where imbalance factor changes, to enhance hardware security. Due to mode conversion at this discontinuity point, the common-mode current flows with the side-channel information through the power cable, and causes secret information leaks outside the cryptographic module. Finally, Chapter 5 summarizes the thesis work with a general conclusion.

Chapter 2 explain the modal-equivalent circuit model for analysis mode conversion in a transmission line. In a transmission line system, mode conversion occurs when two transmission lines with different imbalance factors are connected. In this case, the current division factor, also known as the imbalance factor, is used as an imbalance parameter to evaluate mode conversion. This chapter explains the mode conversion mechanism for analysis mode conversion at the interface when two transmission lines with different imbalance factors are connected. Then, the construction of the modal-equivalent circuit for a 4-conductor transmission-line system is explained. Based on the modal-equivalent circuit model, we suppressed mode conversion in chapter 3. Finally, we enhanced hardware security by applying the mode conversion suppression technique at the imbalance factor discontinuity point in chapter 4.

Chapter 3 proposed an imbalance matching method at the connector section to suppress mode conversion by using a modal-equivalent circuit model. There is inadequate shielding around the connector section, which causes an imbalance difference with the cable section, and occurs mode conversion at the Ethernet connector. This chapter improved the footprint of female connector on the PCB structure, and also improved shielding at the edge of the male and female connectors to accomplish imbalance matching at the connector section. From the viewpoint of imbalance matching at the connector section, the improvements should make the imbalance factor of the connector section be close to that of the cable section and suppress mode conversion. The modal-equivalent circuit model with the imbalance factor of the transmission line is used to estimate mode conversion at the connector section and improve EMI issues of the signal transmission-line systems. The improvement based on imbalance matching at the connector section on mode-conversion suppression was experimentally and numerically validated in this chapter.

Chapter 4 applies the mode conversion suppression technique at the discontinuity point on the power delivery network (PDN) where the imbalance factor of the power

cable is different from the imbalance factor of the trace on the cryptographic module, to enhance hardware security. Mode conversion occurs at the discontinuity point on PDN where imbalance factor changes, and conveys secret information as side-channel information from the normal-mode noise to the common-mode current. As a result, common-mode current with the side-channel information flows through the power cable and causes information leakage from the cryptographic module. The correlation power analysis (CPA), one of the most effective analysis methods, is used to analyze the acquired common-mode current waveform to retrieve the secret information. To enhance the SCA resistance of the cryptographic module, we reduced the common-mode current on the power cable by suppressing mode conversion at the discontinuity point. A capacitor at the discontinuity point should suppress mode conversion by reducing the normal-mode voltage. Therefore, reduce the flow of common-mode current through the power cable, and counteract SCA from outside the module. This method is validated experimentally in this chapter.

Chapter 5 concludes this thesis with a summary of the key points.

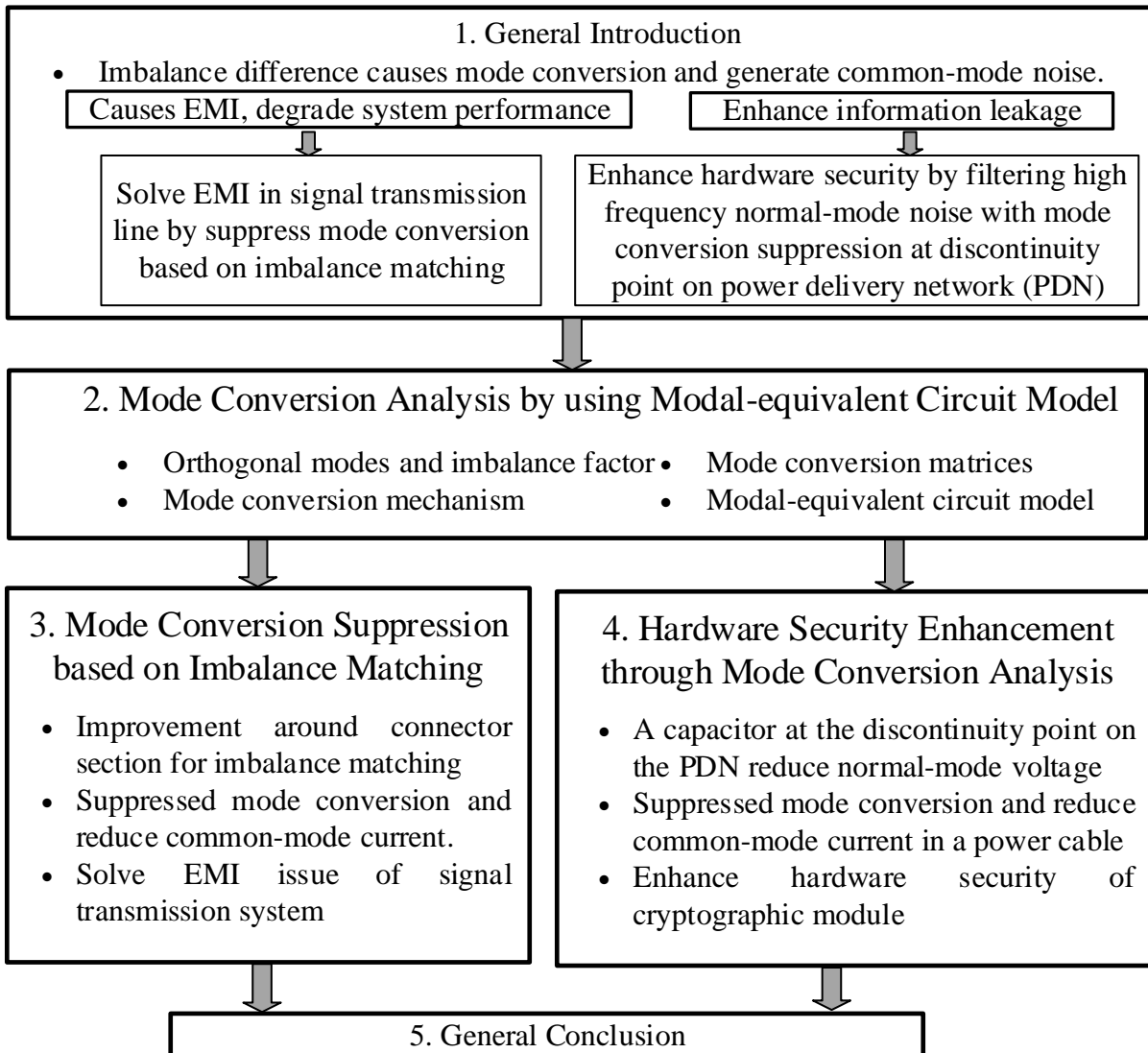


Figure 1.4 Structure of thesis.

Chapter 2

Mode Conversion Analysis by using Modal-equivalent Circuit Model

2.1 Introduction

This chapter will discuss the mode conversion mechanism for analysis mode conversion by using modal-equivalent circuit model. When two transmission lines with different imbalance factors are connected, mode conversion occurs at the interface. The common-mode current generated due to mode conversion often causes electromagnetic interference (EMI) issues and interfere with the normal operation of other systems. Furthermore, the generated common-mode current also enhance the risk of secret information leakage outside the cryptographic module. To solve the EMI issues in signal transmission line and security issues in cryptographic module, it is essential to suppress the mode conversion effectively through mode-conversion analysis by using modal-equivalent circuit model.

At first, we will define the parameter, h , current division factor (also known as imbalance factor) [14, 15] to represent the degree of imbalance of a transmission line. Then, we will define mode conversion that causes EMI in signal transmission systems and information leakage from the cryptographic module. In this section, we will also describe the factor that is responsible for mode conversion.

Section 2.4 will describe the mode conversion mechanism for analysis mode conversion at the connector section that connects the cable (communication/power) with the printed circuit board (PCB) by using modal-equivalent circuit model. However, mode conversion can be suppressed by matching the imbalance factor between two transmission lines as well as by reducing normal-mode voltage and common-mode current at the discontinuity point on power delivery network (PDN). Then, we describe the construction of the modal-equivalent circuit model by inserting voltage-controlled voltage source and current-controlled current source at the mode conversion point with the parameter h .

Section 2.5 will describe the modal-equivalent circuit model to mitigate the EMI issues in the signal transmission system by suppressing mode conversion at the connector section that connects the shielded-twisted-pair (STP) cable with the PCB. Furthermore, the

modal-equivalent circuit model is used to enhance hardware security by reducing the normal-mode voltage, V_n at the discontinuity point on the power delivery network (PDN).

2.2 Imbalance Factor of Transmission line

Watanabe et al. [14, 15] introduced the concept of an imbalance factor to quantify the electrical imbalance of various transmission line configurations. He showed that only the imbalance factor is not responsible for mode conversion. Instead, it is changes in imbalance factor between transmission lines that facilitate this mode conversion.

2.2.1 Definition of Imbalance Factor

Current flowing through a transmission line, is divided into two orthogonal mode current namely, normal mode current and common-mode current. These normal and common-mode currents of a transmission line is located above the system ground as shown in Fig. 2.1. As shown in this figure, I_n indicates the normal-mode current and I_c indicates the common mode current.

It is observed from this figure that the normal-mode currents flow in one signal line and return through another signal line. This current flows in opposite direction but always the same in magnitude. On the other hand, the common-mode currents flows through both signal lines and return through system ground as shown in Fig. 2.1. This current is flowing in the same direction through both signal lines but not always the same in magnitude. It depends on the parameter, known as current division factor is denoted by h . The parameter h , is also known as imbalance factor, and define as “the ratio of common mode current flowing through one conductor to total common-mode current of the transmission line”. This parameter h denotes the degree of imbalance in the transmission line and determined with the cross-sectional geometry of the transmission line.

The imbalance factor is determined from the capacitances of each conductor to ground. For example, the imbalance factor, h for two conductor transmission line can be described in terms of the per-unit-length capacitances as [15],

$$h = \frac{C_{1g}}{C_{1g} + C_{2g}}, \quad (2.1)$$

The capacitance matrix is obtained from the cross section of the transmission line.

2.2.2 Imbalance Factor for Different Transmission Line Structure

In this section, we described the imbalance factor for some commonly used transmission line. Some commonly used transmission line with their imbalance factor are given below:

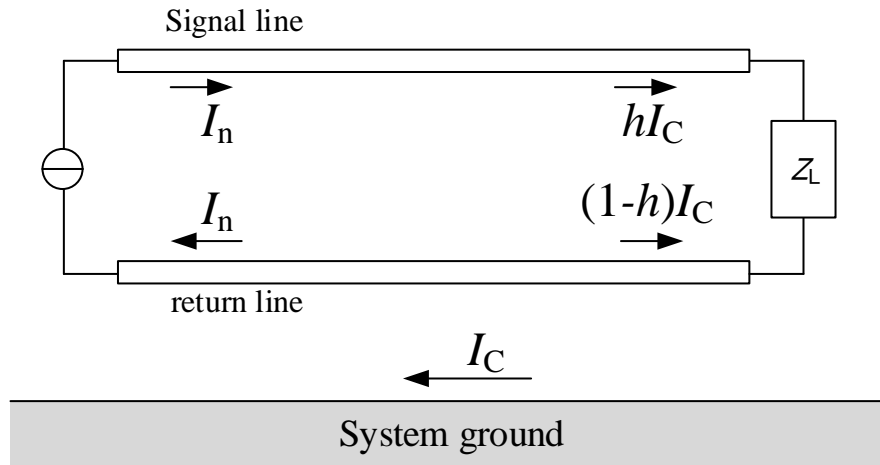


Figure 2.1 Current is divided between two orthogonal modes.

Coaxial Cable

The normal-mode current flows inner conductor and inside surface of the outer conductor. All the common-mode current flows on outside surface of the outer conductor. For this transmission line the value of imbalance factor, $h = 0$.

Balanced Pair Line

The structure is symmetric, so the common-mode current flows equal magnitude on each line. Thus, imbalance factor for this type of transmission line will be $h = 0.5$. In my research work, this type of transmission line is considered for analysis mode conversion mechanism in Ethernet communication system.

Ideal Microstrip Line (MSL)

An ideal MSL structure has a infinite size ground plane. The mirror current of the signal traces flows on the ground plane. So, all the common-mode current flows on ground plane. Thus, in this case the value of imbalance factor, $h = 0$. [17].

Microstrip Structure with a Limited Width Ground Plane

The mirror current of the signal traces almost flows on the ground plane. This current is not perfect because of the insufficient size of ground plane. So, a part of the common-mode current flows on the signal trace and rest flows on the ground plane. Thus, the value of h is between 0 and 0.5.

2.3 Mode conversion due to Imbalance Difference

The factors that are responsible for mode conversion in the transmission line are described in this section. Mode conversion often causes EMI issues in signal transmission systems and information leakage from the cryptographic module. Therefore, we need to investigate the reason of mode conversion and suppress it effectively to solve both issues.

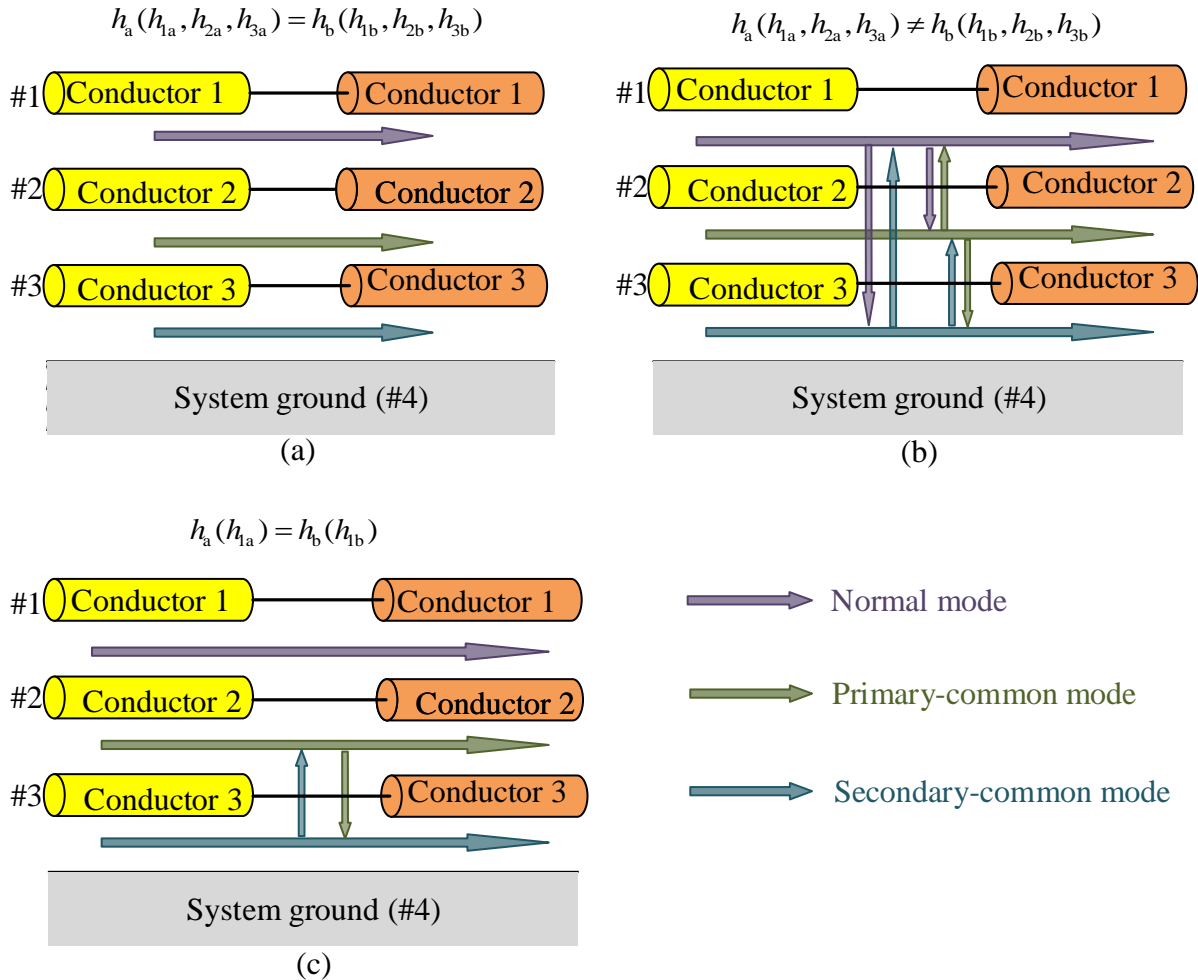


Figure 2.2 Mode conversion occur due to imbalance difference.

When two transmission lines with different imbalance factors are connected, mode conversion occurs at that interface point. It is observed from Fig. 2.2 that mode conversion depends on the difference of imbalance factor between two transmission lines. When two transmission lines with the same imbalance factor are connected, no mode conversion occurs, and hence simple transmission of signal as shown in Fig. 2.2 (a). However, when two transmission lines with different imbalance factors are connected, mode conversion occurs at the interface, as shown in Fig. 2.2 (b). As shown in Fig. 2.2 (b), the imbalance

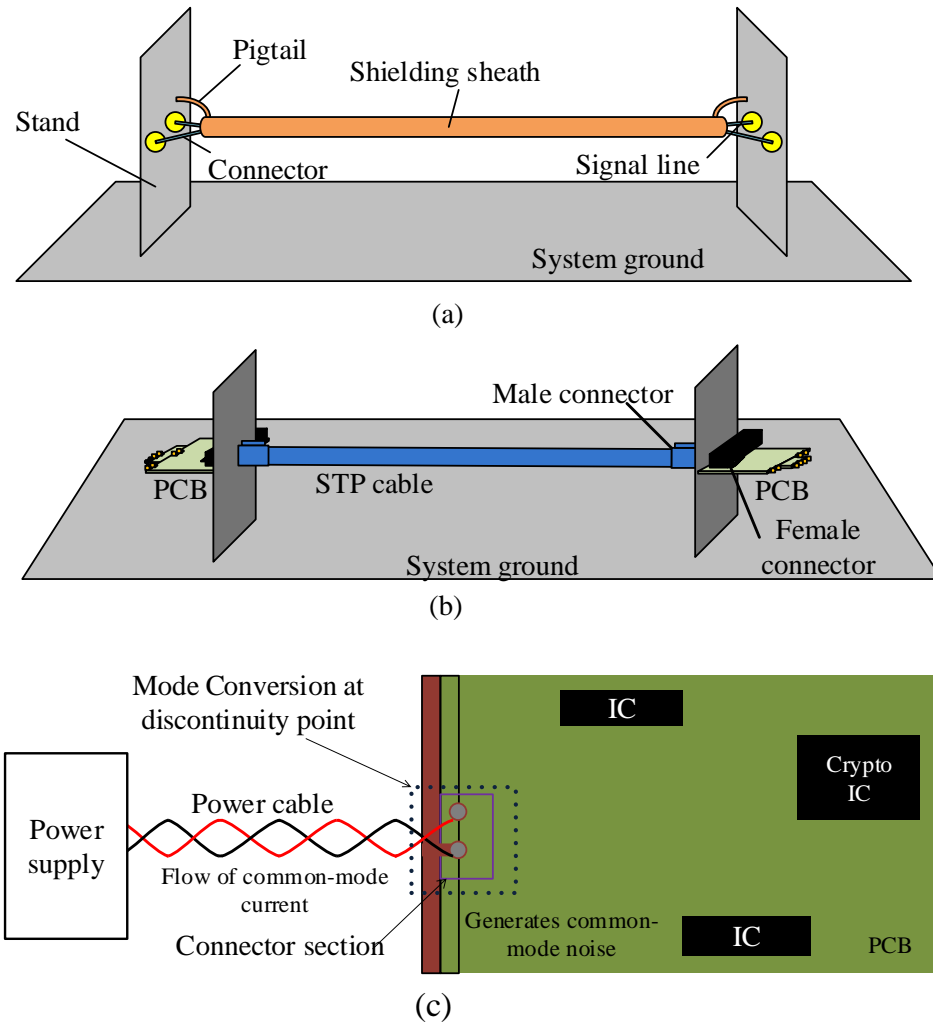


Figure 2.3 Factors that causes mode conversion (a) Mode conversion at pigtail termination (b) Mode conversion at connector section (c) Mode conversion at the discontinuity point on PDN.

factor between two transmission lines is different due to their structural difference at the interface and interrupt transmission of signal. In this condition, the flow of modal currents is not continuous at the interface, and each mode is affected by other modes, results in mode conversion at the interface point.

However, for a 4-conductor transmission system, when two transmission lines are symmetric in their imbalance factor, mode conversion does not occur with normal mode. Hence, mode conversion only occurs between primary-common mode and secondary-common mode, as shown in Fig. 2.2 (c). Therefore, chapter 3 investigates mode conversion under balanced conditions and only considers mode conversion between primary-common and secondary-common modes.

Fig. 2.3 shows some research work that explains how imbalance difference between two transmission lines causes mode conversion. It is observed from Fig. 2.3 (a), a pair (Shielded

Twisted Pair: STP) of shielded cable is terminated to ground through pigtail connection, and mode conversion occurs at the pigtail termination point [22] due to imbalance difference between the cable and the pigtail termination point. In my previous work [23], as shown in Fig. 2.3(b), mode conversion occurs at the connector section that connects the cable with the PCB through an Ethernet connector. Mode conversion occurs at the connector section due to the difference in imbalance factor between the cable section and the connector section. In this case, we improved shielding around the connector section for imbalance matching between the cable section and the connector section that reduces the value of imbalance difference and suppress mode conversion. The modal-equivalent circuit model for the 4-conductor transmission line is used to evaluate the mode conversion suppression at the connector section quantitatively from the viewpoint of imbalance matching.

Mode conversion also occurs at the discontinuity point on power delivery network (PDN), where the power cable connects with the trace on the cryptographic module through an on-board power connector, as shown in Fig. 2.3(c). Due to the imbalance difference between the cable and the trace, mode conversion occurs at the discontinuity point on PDN and generates common-mode current that flows through the power cable and causes information leakage [26,27,41]. Therefore, to enhance hardware security in the cryptographic module, it is essential to countermeasure against information leakage by suppressing mode conversion at the discontinuity point on the PDN. In this case, we mount a capacitor at the discontinuity point between the power line and the GND to reduce the normal-mode voltage, V_n and result in suppression of mode conversion. In Chapter 4, we investigate the hardware security enhancement based on the mode conversion mechanism.

2.4 Modal-equivalent Circuit Model for Analysis Mode Conversion

This section described about the mode conversion mechanism for 4-conductor transmission system. Then, described the construction of modal-equivalent circuit model for 4-conductor transmission system to evaluate mode conversion.

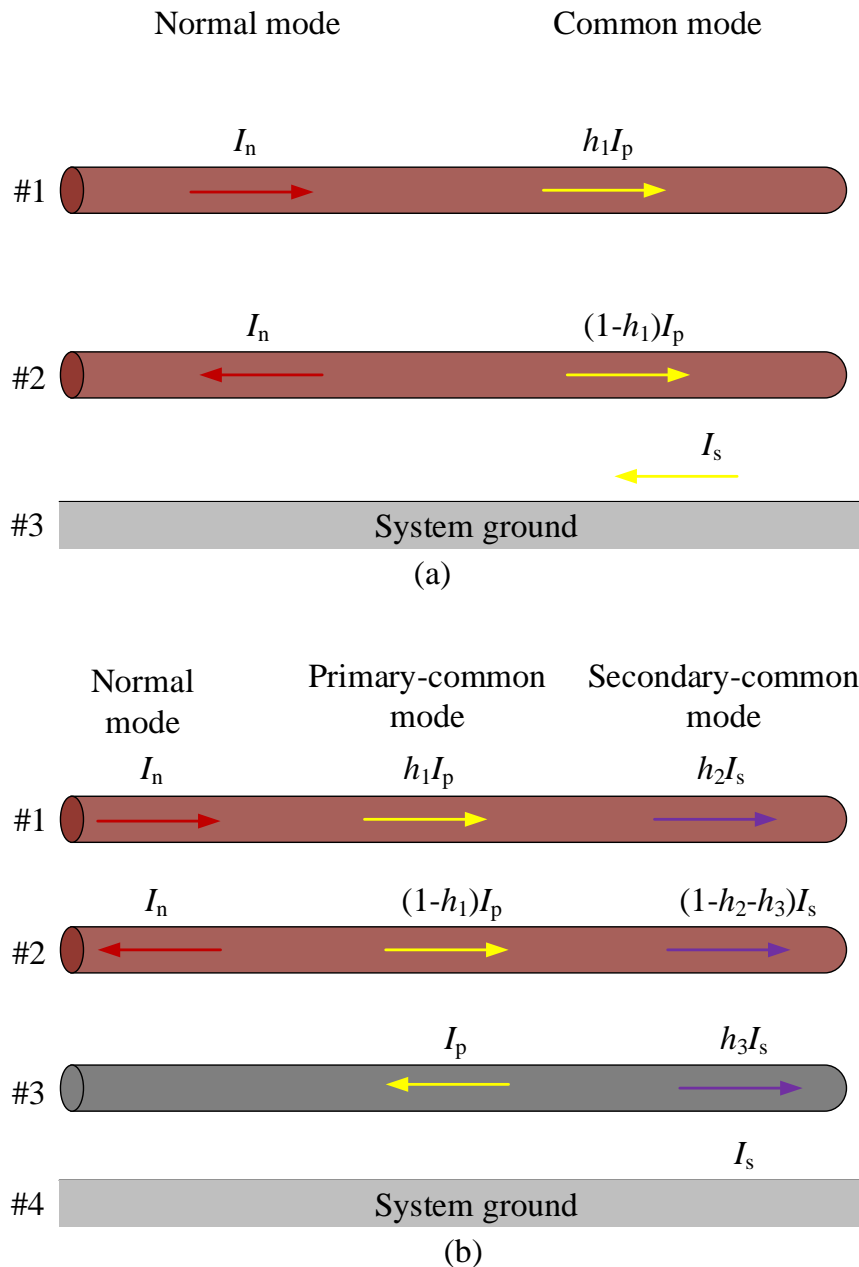


Figure 2.4 Orthogonal modes (a) 3-conductor transmission system (a) 4-conductor transmission system.

2.4.1 Mode Conversion Mechanism

In this section, at first, we will explain the orthogonal mode of multi-conductor transmission line. The n-conductor transmission system contains (n-1) orthogonal modes that propagates along the transmission system by keeping the property of orthogonality. Fig. 2.4 shows the orthogonal modes of a transmission system. Fig. 2.4(a) shows the orthogonal modes of 3-conductor transmission system that consists of two conductors and one system ground. Each conductor is named as conductor #1, conductor #2, as shown in Fig. 2.4(a). 3-conductor transmission system has two orthogonal modes, normal-mode and common-mode.

On the other hand, a 4-conductor transmission system consists of three orthogonal modes: normal mode, primary-common mode, and secondary-common mode. Normal mode and primary-common mode are the same as the normal mode and common mode of 3-conductor transmission system, but 4-conductor transmission system has one more additional common-mode named secondary-common mode. A 4-conductor transmission systems consist of three conductors and a system ground. Each conductor is named as conductor #1, conductor #2, and conductor #3 as shown in Fig. 2.4(b).

In normal mode, conductor #1 is the signal line and conductor #2 is the return line. This mode defines the normal transmission of signal. In primary-common mode, conductor #1 and conductor #2, are the signal line and conductor #3 is the return line. This mode defines the imbalance factor, h_1 from the ratio of the current flowing through the conductors #1 and #2, which is the signal line and the current flowing these two lines are defined as I_{p1} , and I_{p2} , respectively, as shown in Fig. 2.4(b). The primary-common mode current I_{p1} , and I_{p2} expressed as

$$I_{p1} = h_1 I_p \quad (2.2)$$

$$I_{p2} = (1 - h_1) I_p \quad (2.3)$$

In secondary common mode, conductor #1, conductor #2 and conductor #3, are the signal line and system ground is the return line. This mode defines imbalance factor h_2 and h_3 from the ratio of current flowing through conductor #1, conductor #2, and conductor #3, which is the signal line and the current flowing these three lines are defined as I_{s1} , I_{s2} , and I_{s3} , [22] respectively, as shown in Fig. 2.4(b).

$$I_{s1} = h_2 I_s \quad (2.4)$$

$$I_{s2} = (1 - h_2 - h_3) I_s \quad (2.5)$$

$$I_{s3} = h_3 I_s \quad (2.6)$$

The imbalance factors for each orthogonal mode in the 4-conductor transmission system can be defined as.

$$h_1 = \frac{I_{p1}}{I_p} = \frac{I_{p1}}{I_{p1} + I_{p2}} = \frac{(C_{11} + C_{12})(C_{23} + C_{33}) - C_{13}(C_{12} + C_{13} + C_{22} + C_{23})}{(C_{11} + 2C_{12} + C_{22})C_{33} - (C_{13} + C_{23})^2} \quad (2.7)$$

$$h_2 = \frac{I_{s1}}{I_s} = \frac{I_{s1}}{I_{s1} + I_{s2} + I_{s3}} = \frac{C_{11} + C_{12} + C_{13}}{C_{11} + C_{22} + C_{33} + 2(C_{12} + C_{13} + C_{23})} \quad (2.8)$$

$$h_3 = \frac{I_{s3}}{I_s} = \frac{I_{s3}}{I_{s1} + I_{s2} + I_{s3}} = \frac{C_{31} + C_{32} + C_{33}}{C_{11} + C_{22} + C_{33} + 2(C_{12} + C_{13} + C_{23})} \quad (2.9)$$

Here, the capacitance matrix C of the 4-conductor transmission system is obtained from the cross-sectional structure of the transmission line and defined as follows.

$$C = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix} \quad (2.10)$$

where $C_{ij}=C_{ji}$.

Therefore, the actual voltages and currents of conductors #1, #2, and #3 are denoted as $V_1, I_1, V_2, I_2,$ and $V_3, I_3,$ respectively. Moreover, $V_n, I_n, V_p, I_p,$ and V_s, I_s are the modal voltages and the modal currents, where $n, p,$ and s indicate the normal mode, the primary-common mode, and the secondary-common mode, respectively. Based on the mode-decomposition technique [45, 46] as describe for 3-conductor transmission system, the actual voltage and actual current are converted into a modal voltage and modal current in a 4-conductor system, but the difference with the 3-conductor transmission system is that the number of elements of the vector and the matrix increases as the number of conductor increases in 4-conductor system. Therefore, the actual line voltages V (V_1, V_2, V_3) and the actual line currents I (I_1, I_2, I_3) are associated with the mode voltages V_m (V_n, V_p, V_s) and mode currents I_m (I_n, I_p, I_s) using the mode-conversion matrices \mathbf{T}_v and \mathbf{T}_i [47] as follows:

$$V = \begin{bmatrix} V_1 \\ V_2 \\ V_3 \end{bmatrix} = \begin{bmatrix} 1 - h_2 - h_1 h_3 & h_3 & 1 \\ -h_2 - h_1 h_3 & h_3 & 1 \\ h_1 - h_2 - h_1 h_3 & h_3 - 1 & 1 \end{bmatrix} \begin{bmatrix} V_n \\ V_p \\ V_s \end{bmatrix} = \mathbf{T}_v V_m, \quad (2.11)$$

$$I = \begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} = \begin{bmatrix} 1 & h_1 & h_2 \\ -1 & 1 - h_1 & 1 - h_2 - h_3 \\ 0 & -1 & h_3 \end{bmatrix} \begin{bmatrix} I_n \\ I_p \\ I_s \end{bmatrix} = \mathbf{T}_i, \quad (2.12)$$

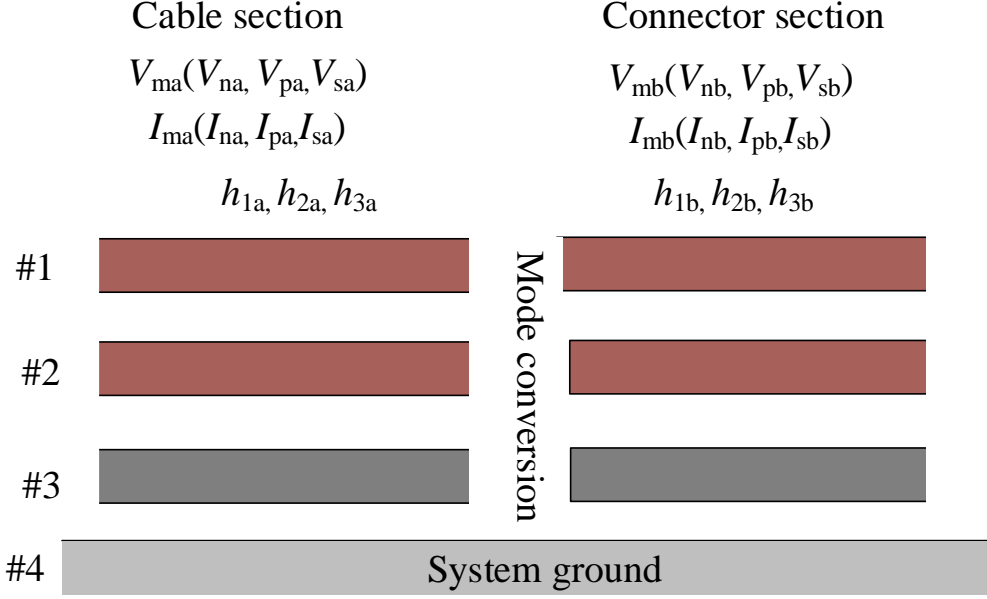


Figure 2.5 Modal voltage and modal current for transmission line with different imbalance factor.

where mode conversion matrix \mathbf{T}_v and \mathbf{T}_i is written as

$$\mathbf{T}_v = \begin{bmatrix} 1 - h_2 - h_1 h_3 & h_3 & 1 \\ -h_2 - h_1 h_3 & h_3 & 1 \\ h_1 - h_2 - h_1 h_3 & h_3 - 1 & 1 \end{bmatrix}, \quad (2.13)$$

$$\mathbf{T}_i = \begin{bmatrix} 1 & h_1 & h_2 \\ -1 & 1 - h_1 & 1 - h_2 - h_3 \\ 0 & -1 & h_3 \end{bmatrix}, \quad (2.14)$$

The matrices in equation (2.11) and (2.12) should satisfy the modal orthogonality [48], i.e., $(\mathbf{T}_i)^T \mathbf{T}_v = 1$.

It is observed from Fig. 2.5 that when two transmission lines with different imbalance factor are connected, mode conversion occurs at the interface. Here, the transmission line A indicates the cable section and transmission line B indicates the connector section. In the 4-conductor transmission system, the modal voltage, V_{ma} and current, I_{ma} for a transmission line with imbalance factor, h_a , and the modal voltage, V_{mb} and current, I_{mb} for a transmission line with imbalance factor, h_b is defined as follows.

$$\mathbf{V}_{ma} = \begin{bmatrix} V_{na} \\ V_{pa} \\ V_{sa} \end{bmatrix}, \mathbf{I}_{ma} = \begin{bmatrix} I_{na} \\ I_{pa} \\ I_{sa} \end{bmatrix}, \mathbf{V}_{mb} = \begin{bmatrix} V_{nb} \\ V_{pb} \\ V_{sb} \end{bmatrix}, \mathbf{I}_{mb} = \begin{bmatrix} I_{nb} \\ I_{pb} \\ I_{sb} \end{bmatrix}$$

The orthogonal mode conversion matrix for 4-conductor transmission system is expressed in the similar way as in 3-conductor transmission system [18, 19]. The following equation shows the mode conversion matrix for 4-conductor transmission system

$$\begin{bmatrix} V_{na} \\ V_{pa} \\ V_{sa} \end{bmatrix} = \mathbf{T}_{ia}^T \mathbf{T}_{vb} \begin{bmatrix} V_{nb} \\ V_{pb} \\ V_{sb} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -\Delta h_1 & 1 & 0 \\ -\Delta h_{2b} & \Delta h_3 & 1 \end{bmatrix} \begin{bmatrix} V_n \\ V_{pb} \\ V_{sb} \end{bmatrix}, \quad (2.15)$$

$$\begin{bmatrix} I_{na} \\ I_{pa} \\ I_{sa} \end{bmatrix} = \mathbf{T}_{va}^T \mathbf{T}_{ib} \begin{bmatrix} I_{nb} \\ I_{pb} \\ I_{sb} \end{bmatrix} = \begin{bmatrix} 1 & \Delta h_1 & \Delta h_{2a} \\ 0 & 1 & -\Delta h_3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} I_{nb} \\ I_{pb} \\ I_{sb} \end{bmatrix}, \quad (2.16)$$

where \mathbf{T}_{va} and \mathbf{T}_{ia} are the mode-conversion matrices of the cable section and \mathbf{T}_{vb} and \mathbf{T}_{ib} are those of the connector section.

The coefficient of the mode conversion sources [22] can be written as

$$\Delta h_1 = h_{1b} - h_{1a}, \quad (2.17)$$

$$\Delta h_2 = h_{2b} - h_{2a}, \quad (2.18)$$

$$\Delta h_3 = h_{3b} - h_{3a}, \quad (2.19)$$

$$\Delta h_{2a} = \Delta h_2 + h_{1a} \Delta h_3, \quad (2.20)$$

$$\Delta h_{2b} = \Delta h_2 + h_{1b} \Delta h_3, \quad (2.21)$$

2.4.2 Construction of Modal-equivalent Circuit Model for 4-conductor Transmission Line

A modal-equivalent circuit is used to analysis mode conversion for the transmission line containing 4 conductors or less. The modal-equivalent circuit model constructs an equivalent circuit for the transmission line that represent the existing transmission line. Furthermore, in the modal-equivalent circuit model, the mode conversion is expressed by inserting a mode conversion excitation source on each interface. This mode conversion excitation source is a voltage control voltage source and a current control current source containing the imbalance factor as parameter. The advantage of the modal-equivalent circuit is that the mode conversion is estimated only by the current-control current source and the voltage-control voltage source, and this makes it easy to give reasonable effective measures. In this section, we describe the construction of modal-equivalent circuit model for a 4-conductor transmission line in the similar way as in a 3-conductor transmission

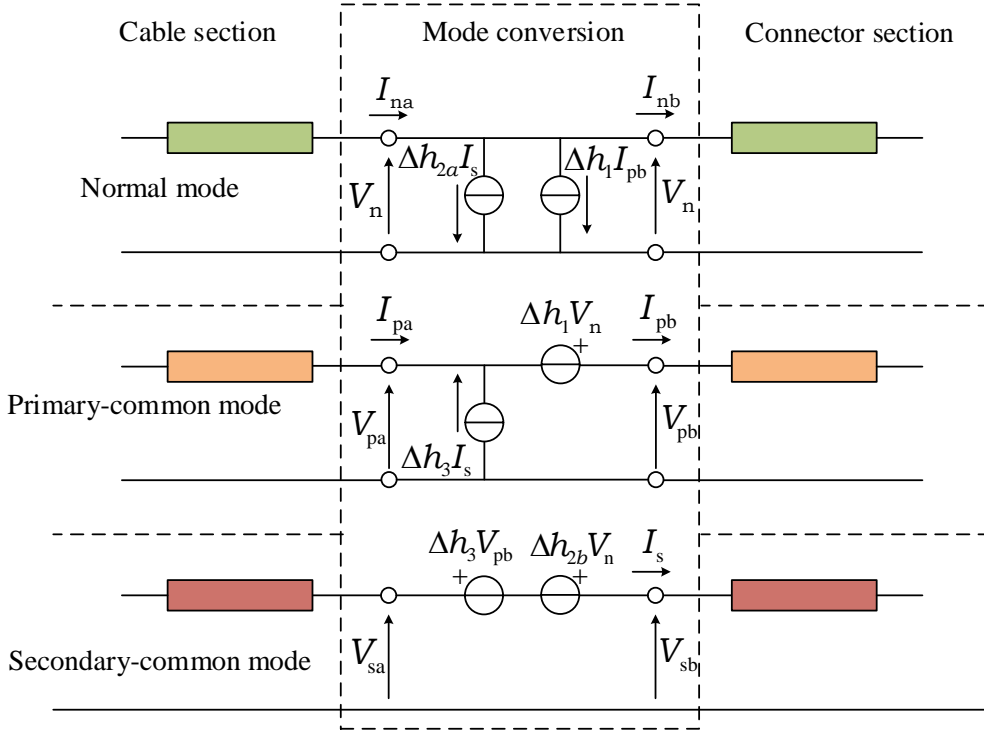


Figure 2.6 Mode-equivalent circuit of a 4-conductor transmission system.

system [19], by inserting mode conversion sources at the interface where two transmission line with different imbalance factor are connected.

Fig. 2.6 shows the modal-equivalent circuit of a 4-conductor transmission system [22] obtained from the relationships of equation (2.15) and (2.16). The mode conversion sources on Fig. 2.6 are obtained from the product of the modal voltage or modal current and the difference between the adjacent imbalance factors. The mode conversion sources are inserted at the interface for each orthogonal mode, as shown in this figure. It is observed from Fig. 2.6 that,

- In the normal mode, two current sources are inserted as shown in the schematic at the top of the Fig. 2.6. These sources are obtained by multiplying the primary common-mode current and the secondary common-mode current with the difference between the adjacent imbalance factors called the coefficient of mode conversion excitation source. In this way the normal mode is affected by the primary common-mode current and the secondary common-mode current.
- In the primary common mode, one current source and one voltage source are inserted

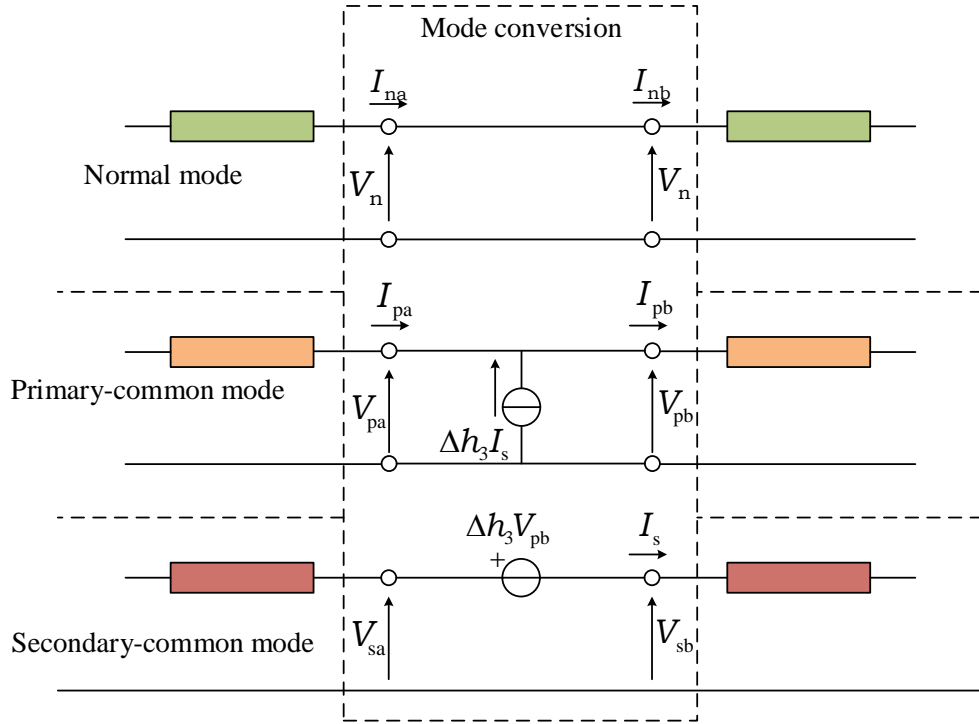


Figure 2.7 Mode equivalent circuit under condition $h_{1a}=h_{1b} = 0.5$.

as shown in the schematic in the middle of the Fig. 2.6. In this way, the primary common mode is affected by the normal mode voltage and the secondary common-mode current.

- Finally, in the secondary common mode, two voltage sources are inserted as shown in the schematic at the bottom of the Fig. 2.6. In this way, each mode is affected by every mode and the mode conversion excitation source influences each other mode and expresses the mode conversion.

The size of the mode conversion between each mode is determined by the value of imbalance difference, where the imbalance difference between the normal and primary common mode is Δh_1 , between the normal and secondary common mode are Δh_{2a} and Δh_{2b} , and between the primary common mode and the secondary common mode is Δh_3 .

Under balanced condition “ $h_{1a}=h_{1b}=0.5$ ”

In a 4-conductor transmission system, a balanced condition “ $h_{1a}=h_{1b}=0.5$ ” holds when two transmissions #1 and #2 are symmetric in their imbalance factor. In this

condition, the coefficient of mode conversion excitation source Δh_1 between normal mode and primary-common mode become:

$$h_{1b} = h_{1a}, \quad (2.22)$$

$$\Delta h_1 = h_{1b} - h_{1a} = 0, \quad (2.23)$$

Furthermore, under this condition, the imbalance factor h_2 and h_3 on the secondary-common mode must satisfy the following condition [22].

For transmission line A, that is the cable section,

$$h_{2a} = \frac{1 - h_{3a}}{2} \quad (2.24)$$

After solve equation (2.24),

$$h_{3a} = (1 - 2h_{2a}) \quad (2.25)$$

Similarly, for transmission line B, that is the connector section,

$$h_{2b} = \frac{1 - h_{3b}}{2} \quad (2.26)$$

After solve equation (2.26),

$$h_{3b} = (1 - 2h_{2b}) \quad (2.27)$$

Therefore, the coefficient of mode conversion excitation source between normal mode and secondary-common mode Δh_{2a} is obtained from equation (2.20), (2.25) and (2.27),

$$\Delta h_{2a} = \Delta h_2 + h_{1a} \Delta h_3 = (h_{2b} - h_{2a}) + 0.5(h_{3b} - h_{3a}) = (h_{2b} - h_{2a}) + 0.5(1 - 2h_{2b} - 1 + 2h_{2a}) = 0, \quad (2.28)$$

Similarly, for the coefficient of mode conversion excitation source between normal mode and secondary-common mode Δh_{2b} is obtained from equation (2.21), (2.25) and (2.27),

$$\Delta h_{2b} = \Delta h_2 + h_{1b} \Delta h_3 = (h_{2b} - h_{2a}) + 0.5(h_{3b} - h_{3a}) = (h_{2b} - h_{2a}) + 0.5(1 - 2h_{2b} - 1 + 2h_{2a}) = 0, \quad (2.29)$$

It is observed from the above discussion that, under balanced condition “ $h_{1a} = h_{1b} = 0.5$ ”, the coefficient of mode conversion excitation source between normal mode and primary-common mode is Δh_1 , the coefficient of mode conversion excitation source between normal mode and secondary-common mode Δh_{2a} and Δh_{2b} are all become zero i.e. $\Delta h_1 = \Delta h_{2a} = \Delta h_{2b} = 0$. Therefore, there remain only the mode conversion sources having Δh_3 between the primary-common mode and the secondary-common mode, as shown in Fig. 2.7. Therefore, in this case, mode conversion only occurs between the primary-common mode and the secondary-common mode, as shown in Fig. 2.8 and can be evaluated only by the value of Δh_3 .

It is observed from Fig. 2.8 that under balanced condition $h_{1a}=h_{1b}=0.5$, mode conversion does not occur with normal-mode. Therefore, under the balanced condition, mode conversion only occurs between primary-common mode and secondary-common mode that can be evaluated only by the value of Δh_3 . It is also observed that mode conversion from secondary-common mode to primary-common mode causes immunity issues and mode conversion from primary-common mode to secondary-common mode causes emission issues. In this research work, we investigate this immunity issues and improve the immunity in signal transmission system by suppressing mode conversion at Ethernet connector.

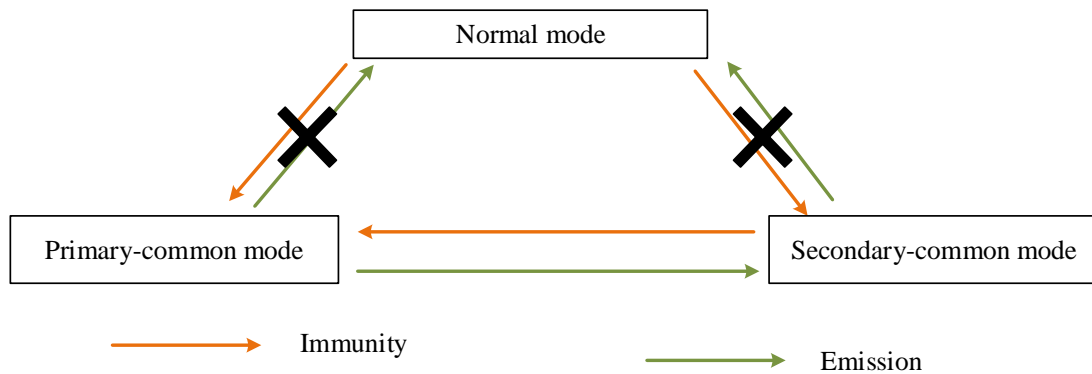


Figure 2.8 Mode conversion when imbalance factor $h_{1a}=h_{1b}=0.5$.

2.5 Application of Modal-equivalent Circuit Model

This section describes the application of the modal-equivalent circuit model to solve EMI issues and enhance hardware security. At first, in chapter 3, the EMI issues are solved by suppressing mode conversion at the connector section based on imbalance matching between the cable section and connector section that reduces the value of imbalance difference. Finally, the modal-equivalent circuit model is used to enhance the hardware security of the cryptographic module by reducing the normal-mode voltage at the discontinuity point on the PDN.

2.5.1 Mode Conversion Suppressing at Ethernet Connector to Solve EMI Issues

Mode conversion occurs due to imbalance difference between two connected transmission lines, causes EMI issues in the signal transmission system. Therefore, it is important to solve the EMI problem by suppressing mode conversion based on imbalance matching between two connected transmission lines. Chapter 3 focuses on the Ethernet connector used to connect the STP cable with the PCB. Mode conversion occurs at Ethernet connector due to imbalance difference between the cable section and connector section. We consider a balanced transmission line, and hence mode conversion does not occur with normal mode under this condition, and only mode conversion between primary and secondary common modes is dominant.

In Chapter 3, we proposed an imbalance matching method at the connector section by improve-shielding around the connector section. This will make the imbalance factor of the connector section, h_{3b} matched with the imbalance factor of the cable section, h_{3a} and suppress mode conversion to solve the immunity and emission issues in Ethernet communication. In order to investigate mode conversion suppression, we consider the three cases described in section 3.3.3. The mixed-mode S -parameter is used as an evaluation index in this experiment. We investigate mode conversion suppression at the connector section based on imbalance matching. In order to validate this method, we estimate mode conversion at the connector section by using a modal-equivalent circuit model that is developed based on the mode conversion mechanism. Chapter 3 will explain in detail our proposed imbalance matching method around the Ethernet connector based on the mode conversion mechanism.

2.5.2 Mode Conversion Suppression Technique to Enhance Hardware Security

In recent years, EMC (electromagnetic compatibility) design has become more important as EM leakage and manipulation of information are becoming realistic threats to hardware security. Information leakage from cryptographic IC may occur due to sev-

eral reasons. Mode conversion at the discontinuity on the power delivery network (PDN) where imbalance factor changes, is one of the most important reasons. Due to mode conversion at the discontinuity point, common-mode current flows through the power cable that contain the side-channel information of the cryptographic IC. An attacker can analyze the characteristics of the common-mode current and retrieve the information. One of the most common security attacks is the side-channel attack (SCA), which extract secret information from cryptographic IC by conducting correlation power analysis (CPA), one of the most popular analysis methods to the waveform of the common-mode current acquired from the power cable. To counteract SCA, and enhance hardware security, it is essential to reduce the common-mode current on the power cable by suppressing mode conversion.

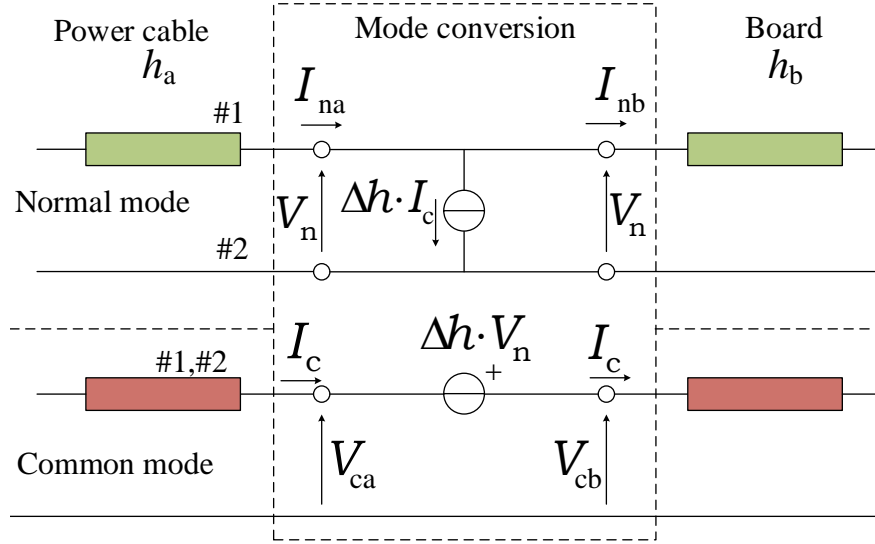


Figure 2.9 Modal-equivalent circuit for 3-conductor transmission system.

Modal-equivalent circuit model is used to analysis mode conversion mechanism on PDN of a cryptographic module. To deliver the power to cryptographic FPGA, the power cable is connected with the trace on the cryptographic module through on-board connector. Fig. 2.9 shows the model-equivalent circuit of a 3-conductor transmission system, where a current-controlled current source, $\Delta h I_c$ is inserted to the normal-mode circuit and a voltage-controlled voltage source, $\Delta h V_n$ is inserted to the common-mode circuit [19] so that the following relationship holds at the interface.

$$V_{ca} = V_{cb} - \Delta h V_n, \quad (2.30)$$

$$I_{na} = I_{nb} - \Delta h I_c, \quad (2.31)$$

where $\Delta h = h_b - h_a$ is the difference of the imbalance factors between power cable (h_a) and board (h_b), V_n is normal-mode voltage at the connected point of the cable and board,

I_c is the common-mode current flowing through the cable, (V_{ca}, V_{cb}) and (I_{ca}, I_{cb}) are the modal voltages and modal currents, respectively. The common mode electromotive force, $\Delta V_c (= V_{cb} - V_{ca})$ is generated by mode conversion at the discontinuity point. The amount of mode conversion is given by the product of Δh and V_n . Mode conversion can be suppressed by reducing the value of Δh [23] or by reducing the value of normal mode voltage V_n [49]. A decoupling capacitor was used to suppress the mode conversion by reducing the normal-mode voltage at the discontinuity point [49].

Chapter 4 applied the mode conversion suppression technique at the discontinuity point on PDN where the imbalance difference changes for SCA countermeasure and enhance hardware security. We suppressed the mode conversion at the discontinuity point on PDN by reducing the normal-mode voltage [49]. A capacitor is installed at the discontinuity point on PDN to reduce the normal-mode voltage and suppress mode conversion. Therefore, the common-mode current with side-channel information is reduced and attackers have less side-channel information to retrieve secret key information. Result in enhancement of SCA resistance. Chapter 4 will explain in detail the countermeasure method against SCA and enhance the hardware security of the cryptographic module.

2.6 Conclusion

This chapter describes mode conversion at the interface where two transmission lines with different imbalance factors are connected. First, we define the imbalance factor, h , as the parameter for presenting the imbalance of the transmission line. Second, the imbalance factor, h , defined as the ratio of common-mode current on the signal lines to total common-mode current, is used to evaluate mode conversion. We described this in Section 2.2.

Next, in section 2.3, we define mode conversion that causes EMI issues in signal transmission line and security issues in cryptographic module. We explained the reason of mode conversion.

In section 2.4, mode conversion mechanism of a 4-conductor transmission system was explained. Then, the construction of a modal-equivalent circuit model for a 4-conductor transmission line was explained for analysis mode conversion. It is evident from modal-equivalent circuit that mode conversion electromotive force is proportional to the product of imbalance difference between two transmission lines and the magnitude of normal mode voltage at the discontinuity point of the imbalance factor. Therefore, mode conversion can be suppressed by approaching the imbalance difference close to zero based on imbalance matching between two transmission lines or by approaching the normal mode voltage close to zero at the discontinuity point where imbalance factor changes.

In section 2.5, the EMI issues of the signal transmission system and the hardware security of the cryptographic module were solved by suppressing mode conversion based on the mode conversion mechanism.

Chapter 3

Mode Conversion Suppression at Connector Section based on Imbalance Matching

3.1 Introduction

When an STP cable is connected with a printed circuit board (PCB) via an Ethernet (RJ45) connector, mode conversion occurs at the connector section due to imbalance difference between the cable section and the connector section. Common-mode current-induced due to mode conversion at Ethernet connector often causes electromagnetic interference (EMI) issues in the signal transmission system. This EMI interferes with the normal operation of other systems. In order to suppress EMI below a prescribed level, it is essential to suppress the mode conversion at the Ethernet connector. It is described in chapter 2 that the mode conversion amount is evaluated from the product of the imbalance difference and the normal-mode voltage. Therefore, mode conversion can be suppressed by reducing the value of imbalance difference or the value of the normal-mode voltage. For the signal transmission system, the mode conversion is suppressed by reducing the value of imbalance difference that is expected to obtain by matching the imbalance factor between the cable section and the connector section. This chapter proposed an imbalance matching method at the connector section for reducing the value of imbalance difference. Therefore, mode conversion is suppressed at the connector section and solves the EMI issues in the signal transmission system.

In recent years, several researchers have proposed various methods to suppress the mode conversion by matching the imbalance factor between two transmission lines. It is observed in [50] that an unbalanced structure in the differential interconnection on the PCB causes mode conversion because of the PCB design [51], mismatch of two trace lengths in a differential line [52], and design of the ground plane. The author proposed a differential line structure to suppresses mode conversion at GHz range by matching the trace width and ground proximity. Then, in [53], the author showed that the mismatch of

two trace lengths in a differential line and the asymmetric ground via configurations causes imbalance difference and results in mode conversion. The author proposed a changing ground via configuration to achieve imbalance matching and result in suppression of mode conversion. Then, the authors in [54] proposed the mode conversion suppression method by adding a shunt capacitor between the single line and the ground.

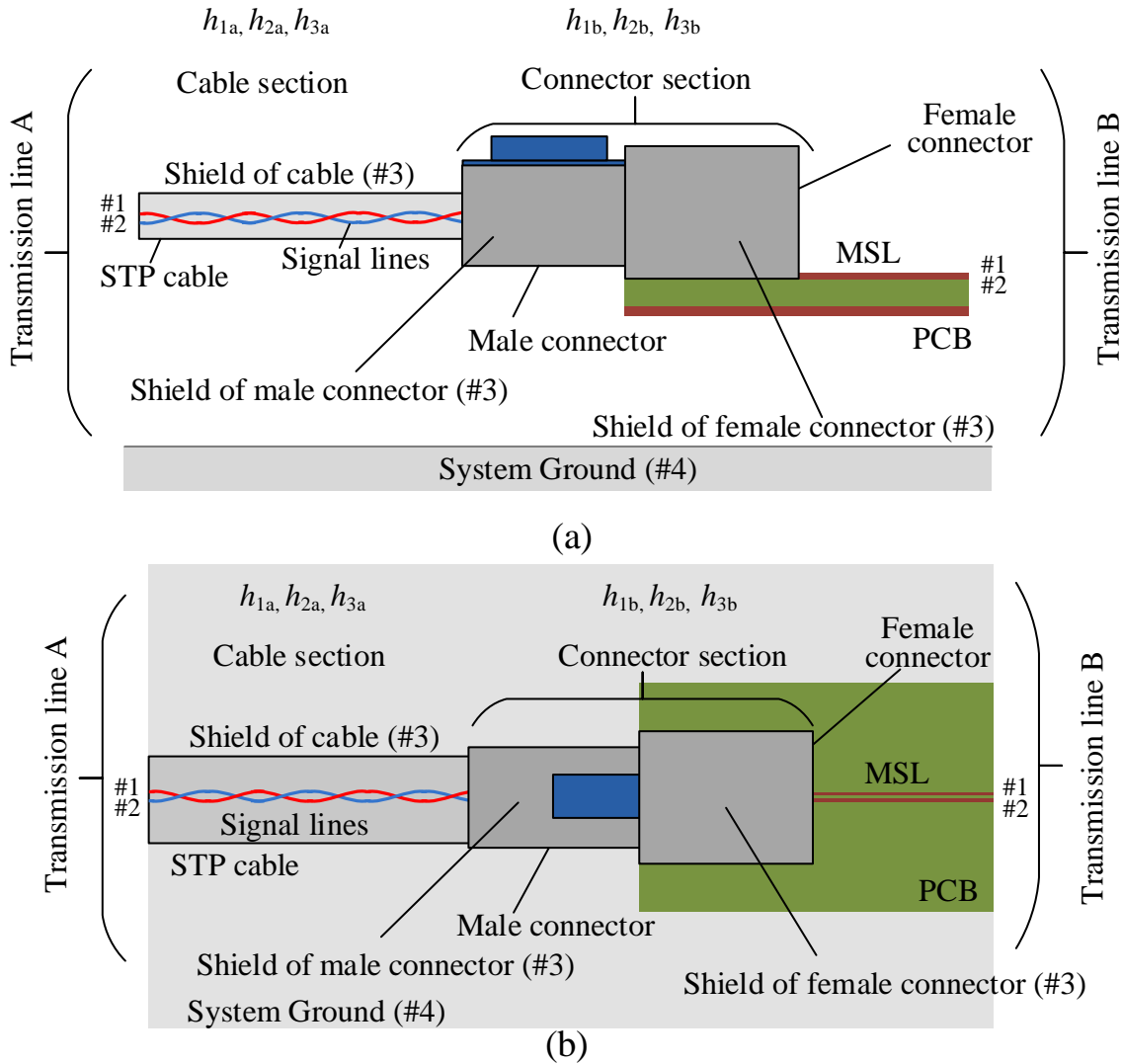


Figure 3.1 Analysis of mode conversion at the connector section of a 4-conductor transmission line (a) side view (b) top view.

Imbalance difference occurs due to line imbalance [20, 55] and imbalance in the terminal networks [56] (termination imbalance) that was analyzed in [21]. It was described in [57] that a balanced transmission line terminated with unbalanced loads as well as manufacturing uncertainty [58], adjacent structures [20], or special design [59] causes balance

state mismatch of the transmission line and occurs mode conversion. Another reason [60] for imbalance difference in the transmission line, is the connection between the coaxial cable and pigtail structure. It was also shown in [61] that pigtail has a dominant role in the coupling, crosstalk, common-mode radiation emission causes due to mode conversion. The mathematical model of the common-mode radiation from a shielded cable caused by the pigtail was studied in [62,63]. Pigtail connections cause discontinuity in the transmission line resulting in mode conversion. Then our research group [22] also investigated that pigtail termination of 2-m shielded-twisted-pair (STP) cable affects the mode conversion in the 4-conductor transmission line. The matching imbalance factor suppressed mode conversion at pigtail termination.

This chapter investigates mode conversion at the Ethernet connector different from pigtail termination case [22], which connects STP cable with the PCB. Fig. 3.1 shows the cascade connection between two transmission lines with different imbalance factors, where transmission line A is the STP cable, and transmission line B is the Ethernet (RJ45) connector. Fig. 3.1(a) shows the side view, and Fig. 3.1(b) shows the top view of the transmission system. It is observed that the male connector is connected with the STP cable, and the female connector is mounted on the PCB. The male connector and the female connector are connected to become one connector that connects the cable with the PCB. It is also observed from this figure that the imbalance factors h_{1a} , h_{2a} , and h_{3a} of the cable section are not equal to the imbalance factors h_{1b} , h_{2b} , and h_{3b} of the connector section, because of the structural difference between two transmission lines. The actual voltages and the actual currents are continuous at the connector section of the cascade connection. However, the modal voltages and currents are discontinuous at the connector section, which causes mode conversion as described in Section 2.4.1.

In this chapter, we improve EMI issues by suppressing mode conversion at the connector section by making the imbalance factor of the connector section closer to that of the cable section from the viewpoint of imbalance matching. This imbalance matching method reduces the value of imbalance difference and suppressed mode conversion. The mixed-mode S -parameter with normal-mode, primary-common mode, and secondary-common mode is used as an evaluation index to investigate mode conversion suppression at the connector section by matching the imbalance factor with the cable section. For analysis, we use LAN cable and RJ45 Ethernet connector. When all conductors of LAN cables are modeled, and mode equivalent circuits are created, the number of parameters required is dramatically increased, resulting in a more complex form. Therefore, we apply a mode equivalent circuit of four-conductor transmission systems for a pair of STP cables to easily analyze the mode conversion of LAN cables. The next section describes the replacement of LAN cable to a 4-conductor transmission line.

This chapter aims to improve EMI issues by suppressing mode conversion at the connector section based on imbalance matching with the cable section so that the value of imbalance difference is expected close to zero. This work treats two common-modes, and the secondary-common mode of the two is recognized as a significant factor of EMI issues

with the emission issues through the STP cable and the immunity issues induced by the so-called common-mode current. Suppressing the mode conversion with the secondary-common mode at the Ethernet connector can solve the EMI issues. It is confirmed in this chapter that the proposed imbalance matching method is expected to suppress mode conversion at the connector section that is validated through comparing the measurement and simulation result obtained from the modal-equivalent circuit model that is described in Chapter 2.

Section 3.2 explains in detail about the cable and connector used in this experiment. Then, the proposed imbalance matching method for suppressing mode conversion at Ethernet connector is described in section 3.3. Section 3.4 explains the measurement system and measurement result to evaluate mode conversion suppression at the connector section. Finally, section 3.5 estimate the mode conversion amount at the connector section by using a modal-equivalent circuit model for validating the proposed imbalance matching method.

3.2 LAN Cable and Ethernet Connector

In this section, we describe the LAN cables and Ethernet connector used in this experiment. In this experiment, Cat 7 LAN cable with transmission bandwidth 600 MHz and Cat 5 Ethernet connector with transmission bandwidth 100 MHz is used.

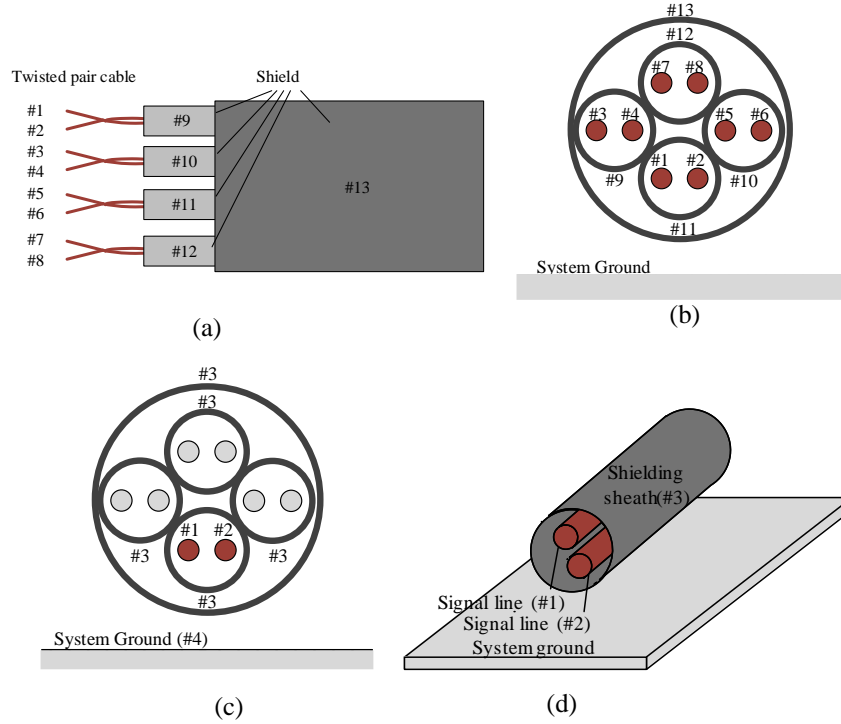


Figure 3.2 LAN cable for analysis mode conversion in Ethernet communication. (a) LAN cable with 4-pair of STP cable (b) Cross-sectional view of LAN cable (c) Single pair STP-cable (d) Single STP-cable is considered as 4-conductor transmission line

3.2.1 LAN Cable for analysis Mode Conversion

As observed from Fig. 3.2(a), four pairs of twisted-pair cables are installed on LAN cables, and the Ethernet standard and LAN cable shielding method and transmission band are standardized according to ISO/IEC 11801 [64]. Category 7 LAN cables have four pairs of STP cables plus another shield and a conductor count of 13 conductors. Therefore, there are three orthogonal modes for each pair of STP cables. Hence, there are so many orthogonal modes that it is practically impossible to model all conductors and construct a modal-equivalent circuit.

For this reason, it is necessary to replace the transmission line with five conductors or more to 4-conductor transmission lines to make the analysis easy and efficient. In a multi-conductor line, the size of the coupling is determined by the value of the capacitance between each line.

In LAN cable, four pairs of STP cables are covered with a single shield. The cross-section of LAN cable is shown in Fig. 3.2(b). It is observed that there are 13 conductors in the LAN cable, including the shield of each pair of STP cables and the shield of the cable that covers all pairs of STP cable. In order to make analysis efficient and easy, this LAN cable can be defined as a single pair STP cable by focusing on the targeted pair on the LAN cable. All shields have the same potential, so coupling with other cables is weak, and we can ignore them. Now the STP cable can be viewed as a four-conductor transmission system that covers two signal lines with a shielding sheath of metal foil as shown in Fig. 3.2(d).

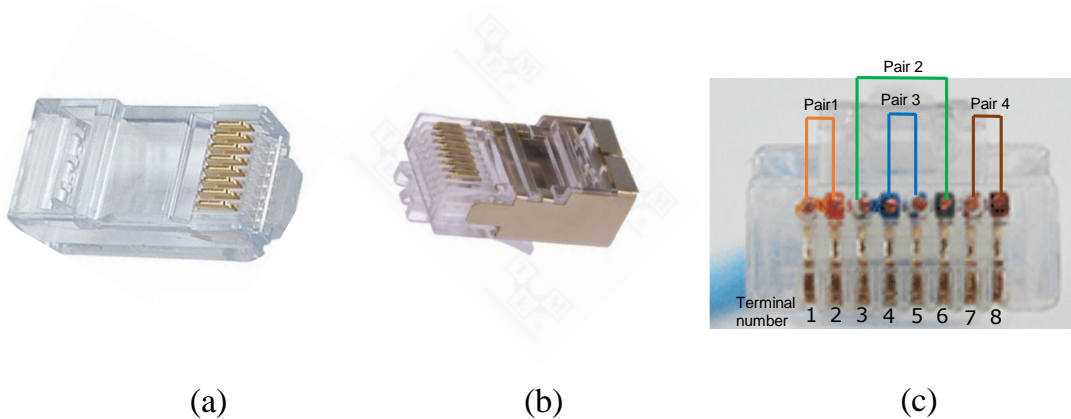


Figure 3.3 Ethernet connector of male type (a)unshielded (b)shielded (c) pin configuration.

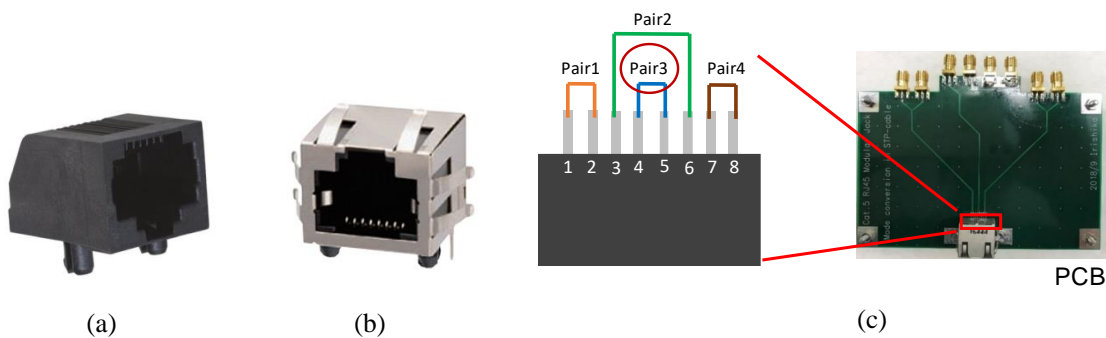


Figure 3.4 Ethernet connector of female type (a)unshielded (b)shielded (c) pin configuration.

3.2.2 Ethernet Connector for analysis Mode Conversion

Ethernet connectors are called RJ45 connectors and are standardized in ISO/IEC 8877 [65]. The RJ45 connector consists of 8 pins. There are two types of RJ45 connectors: male and female connectors with both shielded and unshielded. Fig. 3.3 shows the figure

of Ethernet connector of male type [67, 68], and Fig. 3.4 shows the figure of Ethernet connector of female type [66].

Fig. 3.3(a) shows the unshielded male connector, Fig. 3.3(b) shows the shielded male connector and Fig. 3.3(c) shows the pin connection of male connector. The eight pins of the male connector are connected with the LAN cable that contains four pairs of STP cables. The female connector is commonly called a modular jack. Fig. 3.4(a) shows the unshielded female connector and Fig. 3.4(b) shows the shielded female connector. The female connector is mounted on PCB and connects with the differential line on the PCB. Fig. 3.4(c) shows the pin connection of female connector on the PCB. It is observed from this figure that eight pins of the female connector are connected with the four pairs of differential lines on the PCB. As describe in the previous section, we use one pair of STP cables to avoid complexity in analysis. We use pair 3 of the differential line for analysis as we use in the cable.

3.2.3 Connection Scenario between LAN Cable and Ethernet Connector

It is observed from Fig. 3.3 and Fig 3.4 that the pin configuration of the male and female connector with the conductor number is in order from #1, #2, #3, #4, #5, #6, #7, #8. And the cable also shows order from #1, #2, #3, #4, #5, #6, #7, #8 as shown in Fig. 3.2(b). The connection between the cable section pair and connector section pair is shown in Table 1. For our experiment, we consider pair 3, where pair 3 of the connector section contains conductor numbers #4 and #5, and pair 3 of the cable section contains conductor numbers #1 and #2.

Table 3.1 Pair connection between LAN cable and Ethernet connector.

Cable section pair	Connector section pair2
Pair 1 (#3 and #4)	Pair 1 (#1 and #2)
Pair 2 (#5 and #6)	Pair 2 (#3 and #6)
Pair 3 (#1 and #2)	Pair 1 (#4 and #5)
Pair 4 (#7 and #8)	Pair 1 (#7 and #88)

3.3 Improvement around Connector Section for Imbalance Matching

This section described the proposed imbalance matching method at the connector section to reduce the value of imbalance difference between the cable section and the connector section. We improved shielding around the connector section for imbalance matching between the connector section and the cable section. In fact, we improved the footprint of the female connector on the PCB surface to accomplish imbalance matching at the connector section. Furthermore, we improved shielding at the edge of male and female connector for more improvement. From the viewpoint of imbalance matching at the connector section, the improvements should make the imbalance factor of the connector section be close to that of the cable section. Therefore, the value of imbalance difference is reduced and suppresses mode conversion.

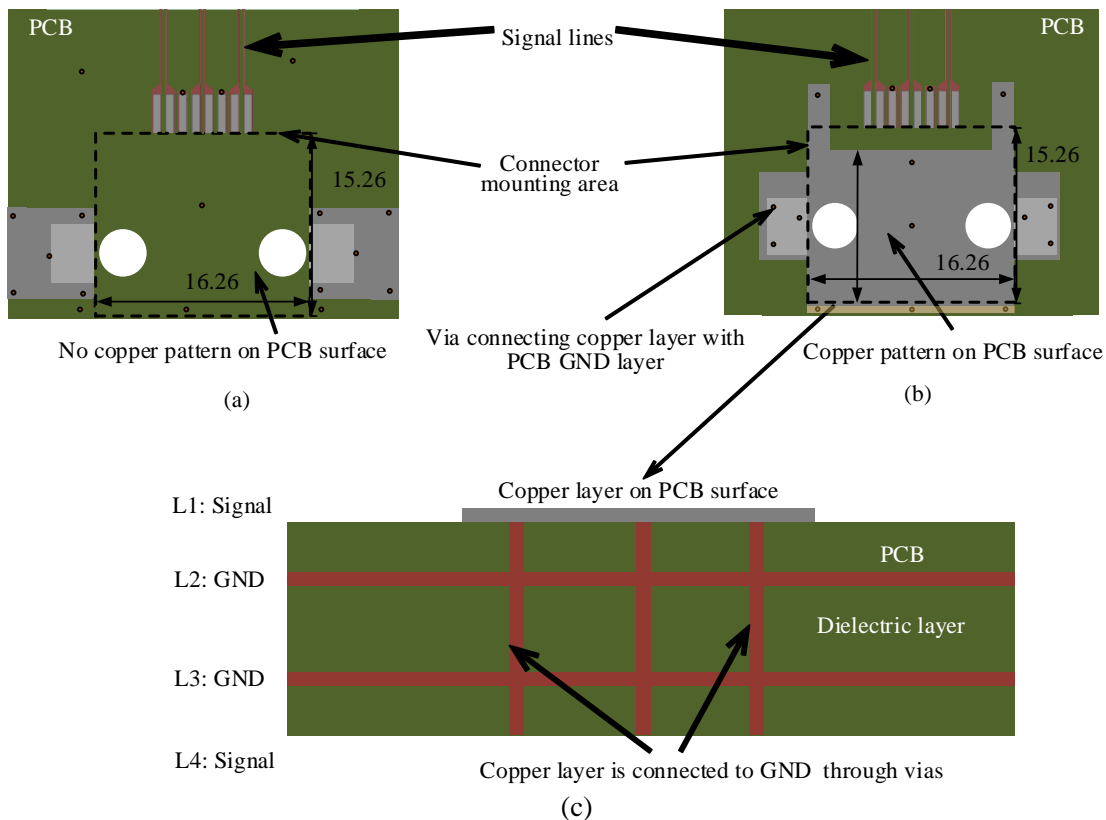


Figure 3.5 Footprint of female connector (a) original footprint of female connector on PCB surface (b) improved footprint of female connector on PCB surface (c) cross-sectional view of PCB layer.

3.3.1 Improvement of Female Connector Footprint on PCB Surface

Fig. 3.5(a) shows the original footprint of female connector on PCB surface. It is evident from this figure that the footprint of the female connector on the PCB surface is insufficient, which seems to cause mode conversion. Therefore, the footprint of the female connector on PCB surface needs to be improved to match the imbalance factors between the connector section and the cable section. The footprint of the female connector is improved by placing a copper pattern below the female connector mounting area, as shown in Fig. 3.5(b), and connected with the PCB GND layer through vias. The dashed lines on the improved footprint indicate the female connector mounting position on the PCB surface, as shown in this figure. The copper pattern is set to 20×20 mm and kept bigger than the female connector so that it can be firmly soldered around the connector. IEEE standard [69] did not describe about the footprint of female connector on the PCB surface. Therefore, our improved footprint of female connector on PCB surface do not conflict with the IEEE standard [69].

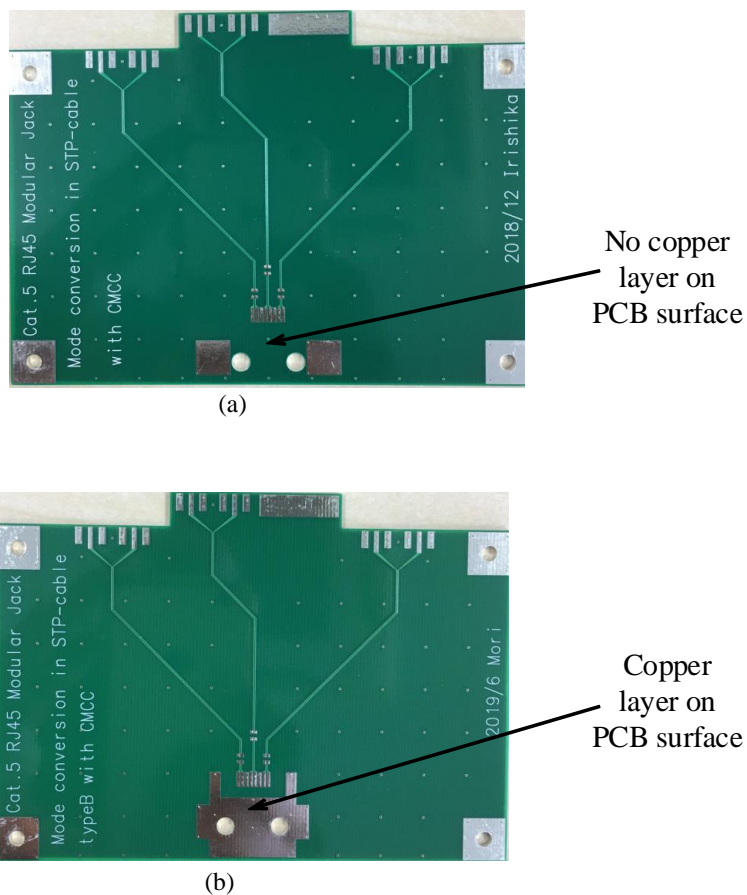


Figure 3.6 PCB used in this experiment (a) before improvement (b) after improvement

Fig. 3.5(c) shows the cross-sectional view of the improved PCB where the copper pattern on the PCB surface is connected with the PCB GND layer through vias. The

improved PCB pattern will remove the gap between the connector mounting area of the female connector on the PCB surface and the shield of the female connector. Fig. 3.6 shows the PCB that is used in this experiment. Fig. 3.6(a) and Fig. 3.6(b) shows the PCB before and after improvement, respectively.

3.3.2 Improvement of Shielding around Connector

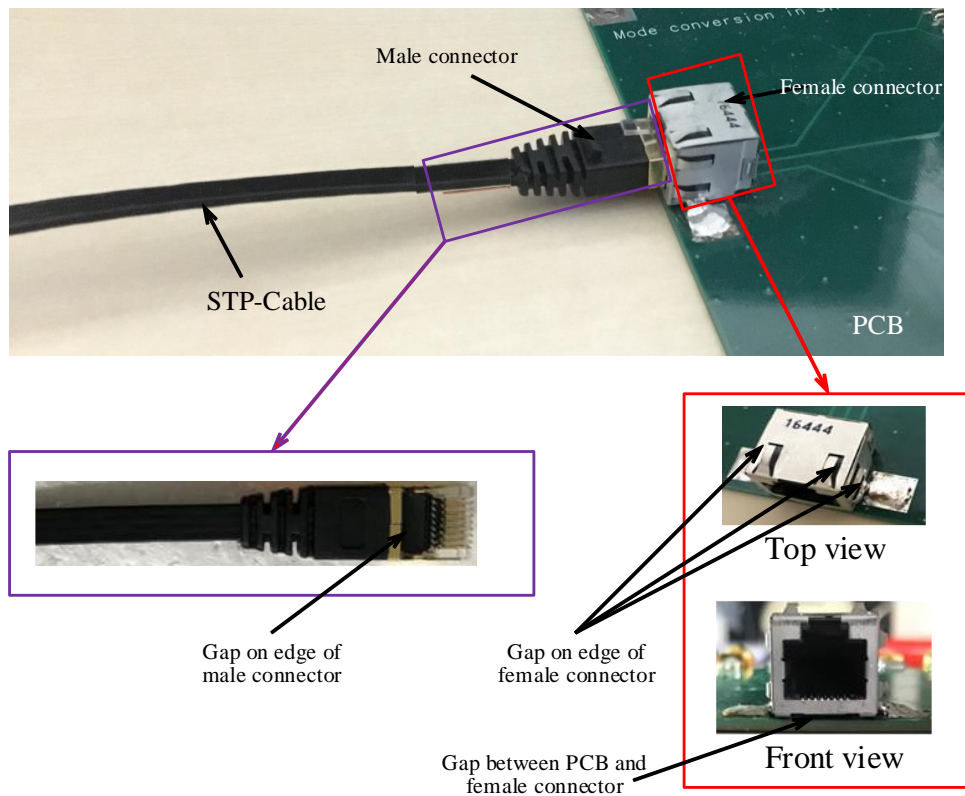


Figure 3.7 Original connector with improved PCB structure.

The inadequate shielding on the PCB surface was improved, as described in the previous section. However, there remains inadequate shielding at the connector section. This section describes the improvement of shielding around the connector section for imbalance matching. This section describes the improvement of shielding around male and female connectors for imbalance matching. Then describe the cross-section of the connector section. This improvement around both connectors improves the imbalance factor at the connector section.

Fig. 3.7 shows the original shielded Ethernet male and female connector. It is observed from Fig. 3.7 that the male-type RJ45 connector is directly connected with the STP-cable, and the female-type RJ45 connector (TE Connectivity/6339160-1) is mounted on the PCB. The Male and female connectors are connected to become one connector that connects the STP cable with the PCB. It is noticeable from the figure that there is an

insufficient shield on the edge of the male connector. Moreover, there is a gap between the underside of the female connector and the PCB, as shown in Fig. 3.7. It is also observed from this figure that there remains inadequate shielding on the edge of the female connectors, which causes mode conversion. The inadequate shielding around the connector will decrease the value of h_{3b} .

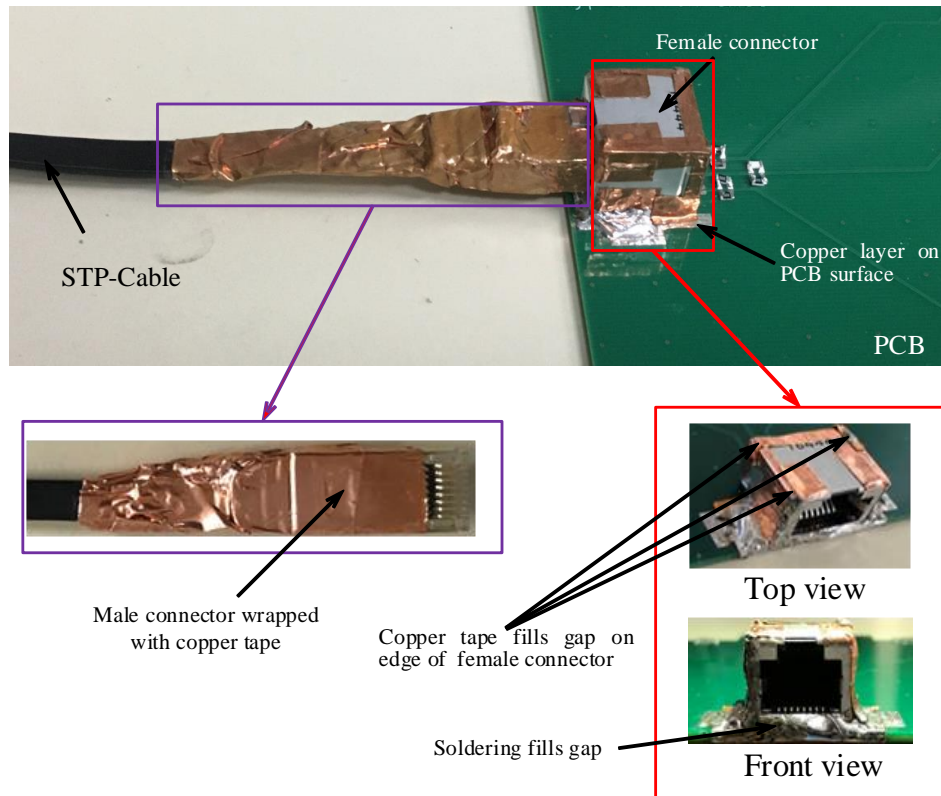


Figure 3.8 Improved shielding around connector.

Fig. 3.8 shows the improved shielding around the connector section. The shielding of the male connector is improved by wrapping the entire circumference with copper tape to cover the shield of the STP cable body and the shield of the male connector, as shown in Fig. 3.8. It is also observed that the gaps between the PCB and the underside of the connector was filled by soldering, and the gap on the edge of the connector shield was filled by wrapping the edge of the connector shield with copper foil tape as shown in Fig. 3.8. The improved shielding around the connector will make the value of h_{3b} close to h_{3a} .

Fig. 3.9 shows the cross-sectional view at the connector section. Fig. 3.9 (a) shows the cross-section before improvement and Fig. 3.9 (b) shows the cross-section after shield-improvement.

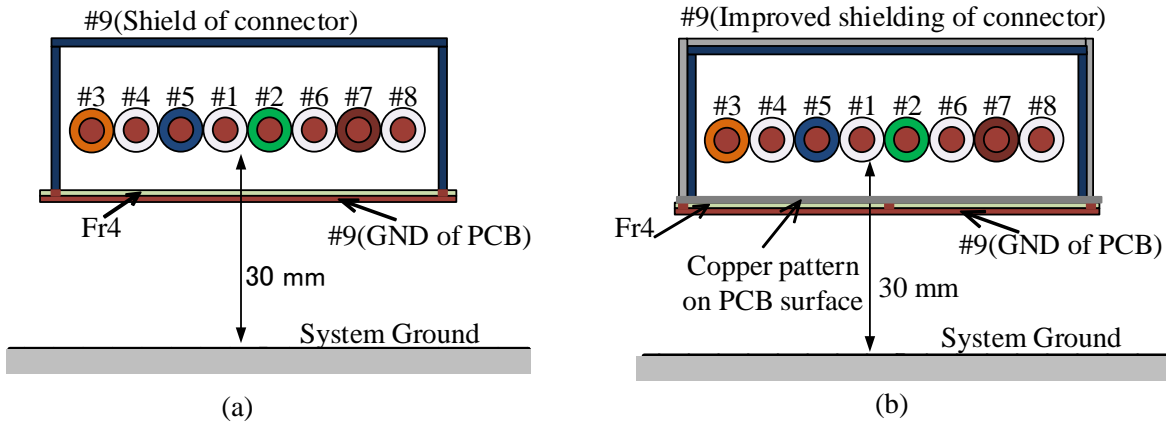


Figure 3.9 Improved shielding around male connector (a) original connector (b) shield improved connector.

3.3.3 Imbalance Matching Due to Improvement around Connector Section

This section explains the impact of the improvement for imbalance matching at the connector section. In this experiment, the following three different conditions are evaluated:

- Case 1: original connector with original footprint of female connector on PCB surface
- Case 2: original connector with improved footprint of female connector on PCB surface
- Case 3: shield-improved connector with improved footprint of female connector on PCB surface

After the improvement of removing the gap at the footprint of the female connector on the PCB surface as described in Section 3.3.1 (Case 2), the imbalance factor at the connector section should become larger than that of Case 1, then the difference with $h_{3a} = 1$ at the cable section will decrease. After the further improvement of the shielding at the edge of the connector by soldering and wrapping with copper tape as described in Section 3.3.2 (Case 3), the imbalance factor at the connector section should become larger than that of Case 2, then the difference with $h_{3a} = 1$ will decrease furthermore. Thus, the magnitude of the mode conversion sources between the primary-common and secondary-common mode become close to zero, resulting in suppression of mode conversion.

Table 3.2 summarizes the imbalance factors of the STP cable and connector section obtained from ANSYS Q3D Extractor, a commercial quasi-static 3D electromagnetic field solver. It is observed from Table 3.2 that the balanced condition holds as $h_{1a} = h_{1b} = 0.5$ and mode conversion does not occur with normal mode. The imbalance factor was

Table 3.2 Imbalance factors of STP cable and connector section.

STP cable		Connector section		
		Case 1	Case 2	Case 3
h_{1a}	0.5	h_{1b}	0.5	0.5
h_{2a}	0	h_{2b}	0.045	0.017
h_{3a}	1	h_{3b}	0.910	0.967
Δh_3			0.090	0.033
				0.008

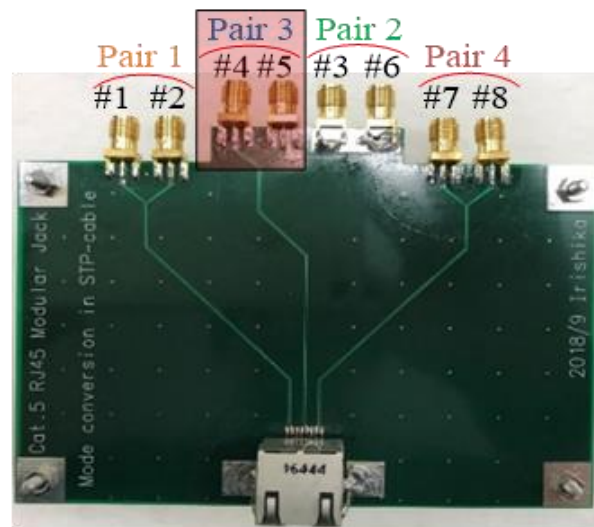
calculated by using equations (2.7) to (2.9). The twisted pair cable is covered by a shield, and the imbalance factor h_a of the cable part is $h_{1a} = 0.5$, $h_{2a} = 0$ and $h_{3a} = 1$.

It is also observed from Table 3.2 that the imbalance factor at the connector section, $h_{3b} = 0.910$ for Case 1, and the difference with the imbalance factor at the cable section ($h_{3a} = 1$) is estimated as $\Delta h_3 = 0.090$, which causes mode conversion at the connector section. In Case 2, the imbalance factor at the connector section becomes $h_{3b} = 0.967$, then the difference with $h_{3a} = 1$ is estimated as the decrease from 0.090 to 0.033. In Case 3 after the further improvement, the imbalance factor at the connector section becomes $h_{3b} = 0.992$, then the difference with $h_{3a} = 1$ is estimated as the decrease from 0.033 to 0.008.

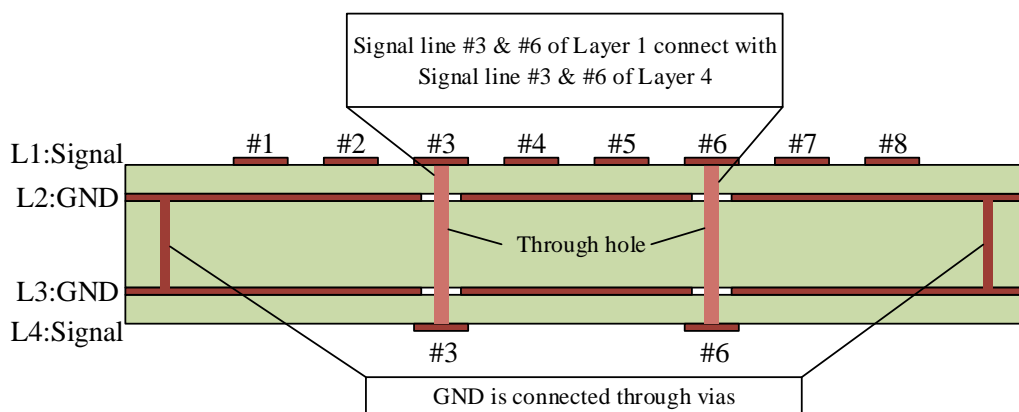
It is noticeable that improvement of the connector section by focusing on the imbalance factor results in the reduction of the difference in the imbalance factors between the connector and cable sections, which leads to a reduction in mode-conversion excitation according to imbalance matching. Therefore, the proposed imbalance matching method is expected to validate in the next section.

3.4 Measurement of Mode Conversion Suppression

In this section, the validation of the imbalance matching method for suppressing mode conversion at the connector section is carried out with the measurement results. Therefore, we will first explain the evaluation system to measure the mode conversion amount at the connector section of a 4-conductor transmission system. Then we will explain the measurement result for the mixed-mode S -parameter, which is the evaluation index in this experiment.



(a)



(b)

Figure 3.10 Printed Circuit Board (PCB) used for measurement (a) top view (b) cross-sectional view.

3.4.1 Evaluation System

We will explain the measurement scenario to measure the mode conversion at the connector section and investigate the effect of imbalance matching between the cable and the connector section on mode conversion suppression. At first, we will explain the PCB as shown in Fig. 3.10. that is used in this experiment. Then explain the stand as shown in Fig. 3.11. that is used to hold the PCB above the system ground. Furthermore, finally, explain the evaluation system as shown in Fig. 3.12, used to measure the mixed-mode S -parameters to evaluate mode conversion suppression at the connector section based on imbalance matching as described in the previous section.

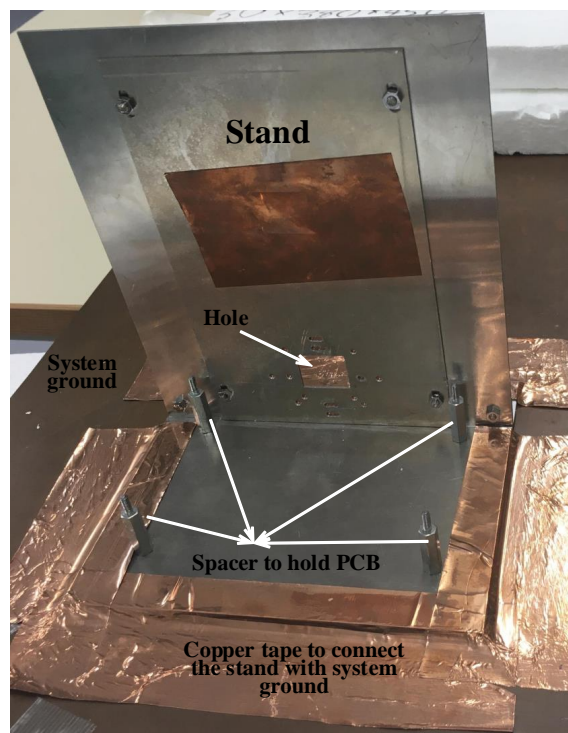


Figure 3.11 Stand used to hold PCB above system ground.

Fig. 3.10 shows the printed circuit board (PCB) with the female RJ45 connector mounted on it to connect the STP cable through a male RJ45 connector. Moreover, four pairs of twisted pair wires of the STP cable are connected to the differential lines on the printed circuit board through the female RJ45 connector, as shown in Fig. 3.10(a). These differential lines are designed with the normal-mode characteristic impedance of $100\ \Omega$ to match that of the STP-cable. In addition, the GND surface of the printed circuit board is also connected with the system ground through the stand. As a result, the differential line of the Pair 1, 3, and 4 on the printed circuit board shows the same characteristics of the normal mode for signal transmission, while the Pair 2 differential lines contain vias in the path, and the characteristics of the normal mode are degraded compared with other

differential lines. Therefore, we use pair 3 differential line for experimental measurement that is connected to STP-cable through Ethernet connector.

Fig. 3.10(b) shows the cross-section view of the PCB used in this experiment. It is observed from this figure that Layer 1 and Layer 4 are the signal line, and Layer 2 and Layer 3 are the GND layer that connected through vias. A dielectric layer separates each layer. This GND layer of this PCB is also connected with the system ground. As observed, signal lines #3 and #6 are placed on Layer 4, and other signal lines are placed on Layer 1. The Layer 1 signal line #3 and #6 are connected with Layer 4 signal line #3 and #6 through vias.

Fig. 3.11 shows the stand that is made with an aluminum plate and placed on the system ground. The stand is connected with the system ground by using copper tape, as shown in this figure. A square hole of 20mm on each side of the stand connects the LAN cable to the female RJ45 connector mounted on the PCB. The square hole on the stand is placed 30 mm above the system ground. The PCB used in this experiment is placed 30 mm above the system ground by placing the PCB on the spacer. Four spacers have been used on each side, as shown in this figure. The GND layer of the PCB is connected with the stand through spacers.

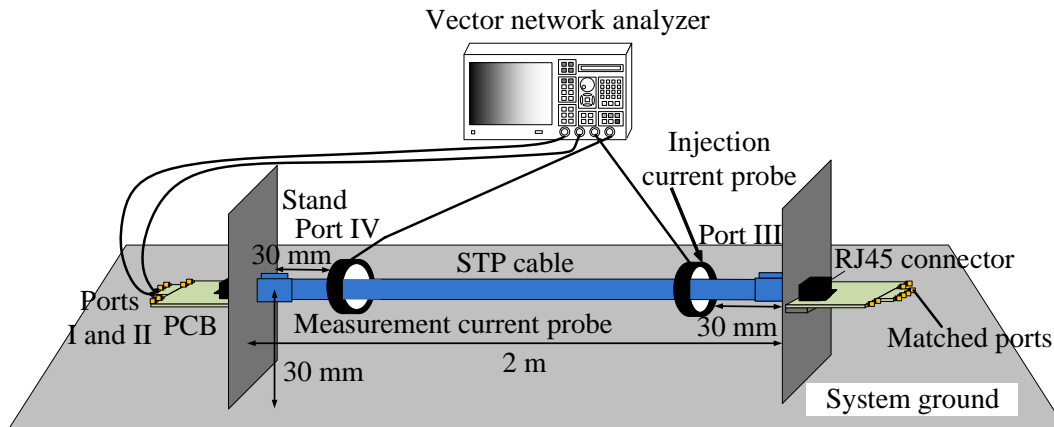


Figure 3.12 STP-cable system for validation.

Fig. 3.12 shows the STP cable system for validation. The evaluation system measured mixed-mode S -parameters to evaluate mode conversion suppression at the connector section based on imbalance matching. A 2 m long STP cable is placed 30 mm above the system ground. It is observed that the STP cable is connected with the PCB through an Ethernet connector. As the STP cable is a 4-conductor transmission line, the PCB is also defined as a 4-conductor transmission line with two differential lines as conductor #1 and #2, and the GND layer as a conductor #3. SMA connector is attached on the end of the differential transmission line where the leftmost end of the differential line is connected with Port I and Port II of a vector network analyzer (VNA, Agilent Technology/E5071C)

through coaxial cable. The other end of the differential lines is connected with two $50\ \Omega$ termination registers. The two current probes (ETS-Lindgren/94111-1L, 94111-1) clamping the STP cable are also connected to the VNA for the injection and measurement of the secondary-common mode.

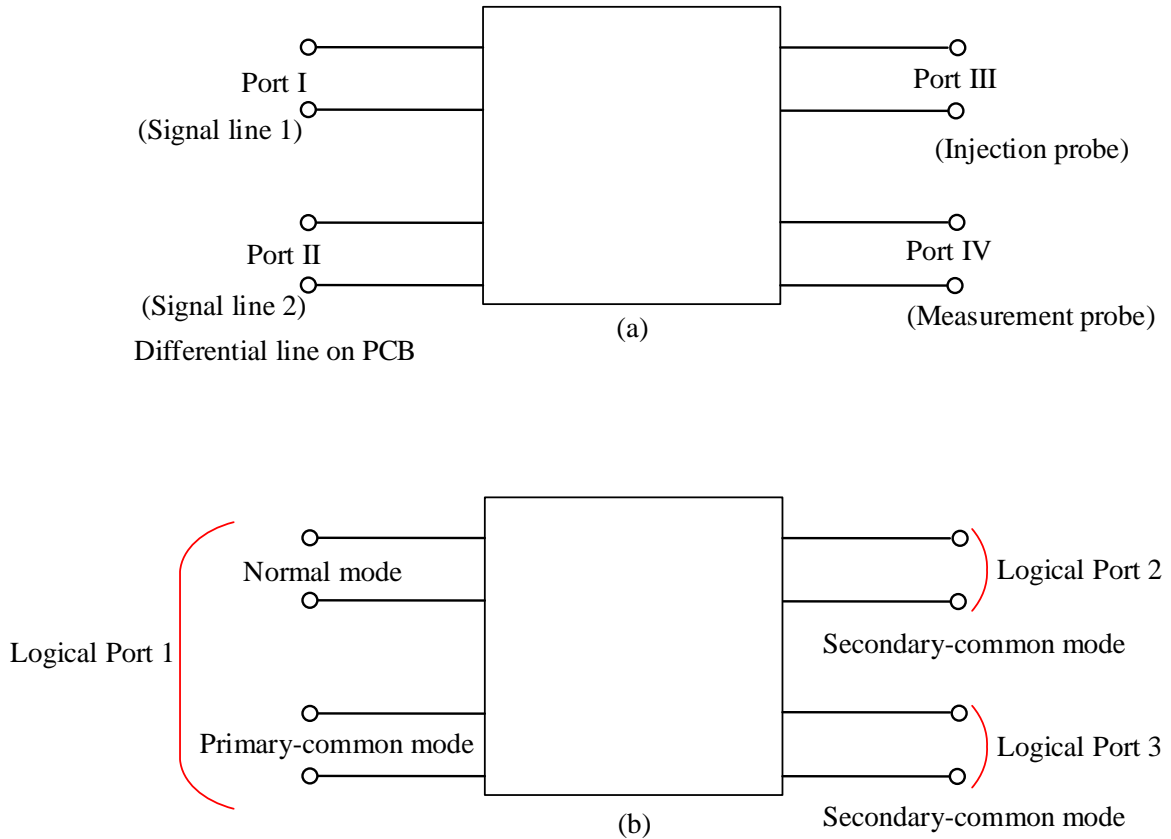


Figure 3.13 Port definitions: (a) Ports I to IV in VNA measurement of standard S -parameters; (b) Logical ports 1 to 3 for evaluation by single-ended mixed-mode S -parameters.

Fig. 3.13(a) shows the port definition of Ports I to IV in the VNA measurement of standard S -parameters (\mathbf{S}^{std}). On the other hand, Fig. 3.13(b) shows the port definition of Logical port 1 to 3 for evaluation by mixed-mode S -parameters (\mathbf{S}^{mm}). Logical port 1 corresponds to two mixed-mode ports of normal mode and primary-common mode. The conversion from four measurement ports of Port I to IV to four Logical ports 1 to 3 is carried out by using the following equation [70].

$$\mathbf{S}^{mm} = \mathbf{M} \mathbf{S}^{std} \mathbf{M}^{-1} \quad (3.1)$$

where \mathbf{M} is defined as

Table 3.3 Measurement conditions of the vector network analyzer.

Maker/model number	Agilent Technology / E5071C
Start frequency (MHz)	1
Step frequency (MHz)	500
Points (pt)	500
Output power (cBw)	-5

$$\mathbf{M} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & \sqrt{2} & 0 \\ 0 & 0 & 0 & \sqrt{2} \end{bmatrix} \quad (3.2)$$

The mixed-mode S -parameter S_{ps12} used for evaluation is obtained by the above conversion and indicates the transmission characteristic of the mode conversion from secondary-common mode at Logical port 2 to primary-common mode at Logical port 1. The subscripts p and s represent primary-common mode and secondary-common mode, and subscripts 1 and 2 represent Logical ports 1 and 2. Thus, the mode conversion means that the secondary-common mode is stimulated by injection probe at Logical port 2 (Port III in the VNA measurement), and primary-common mode is observed at Logical port 1 (Port II in the VNA measurement).

3.4.2 Measurement Result

Measurement results are obtained from the evaluation system described in section 3.4.1. The measurement conditions of the vector network analyzer, which is the measuring instrument, are shown in Table 3-3. We measure the mixed-mode S -parameter for each Case to evaluate mode conversion suppression based on imbalance matching. The vertical dashed line on the graph of the measurement results indicates the frequency, which is thought to be a half-wavelength resonance of the secondary-common mode obtained from a distance between stands of the transmission system. The green, blue and red spectra on the graph of the measurement results indicates the measurement result for Case 1, Case 2 and Case3, respectively. We obtained 16 mixed-mode S -parameters out of this 4 indicates the reflection characteristics denoted as S_{mm11} , S_{pp11} , S_{ss22} and S_{ss33} , and the rest of 12 indicates the transmission characteristics of mode conversion between each mode of the 4-conductor transmission system. The measurement was carried out in the frequency range from 0 to 500 MHz.

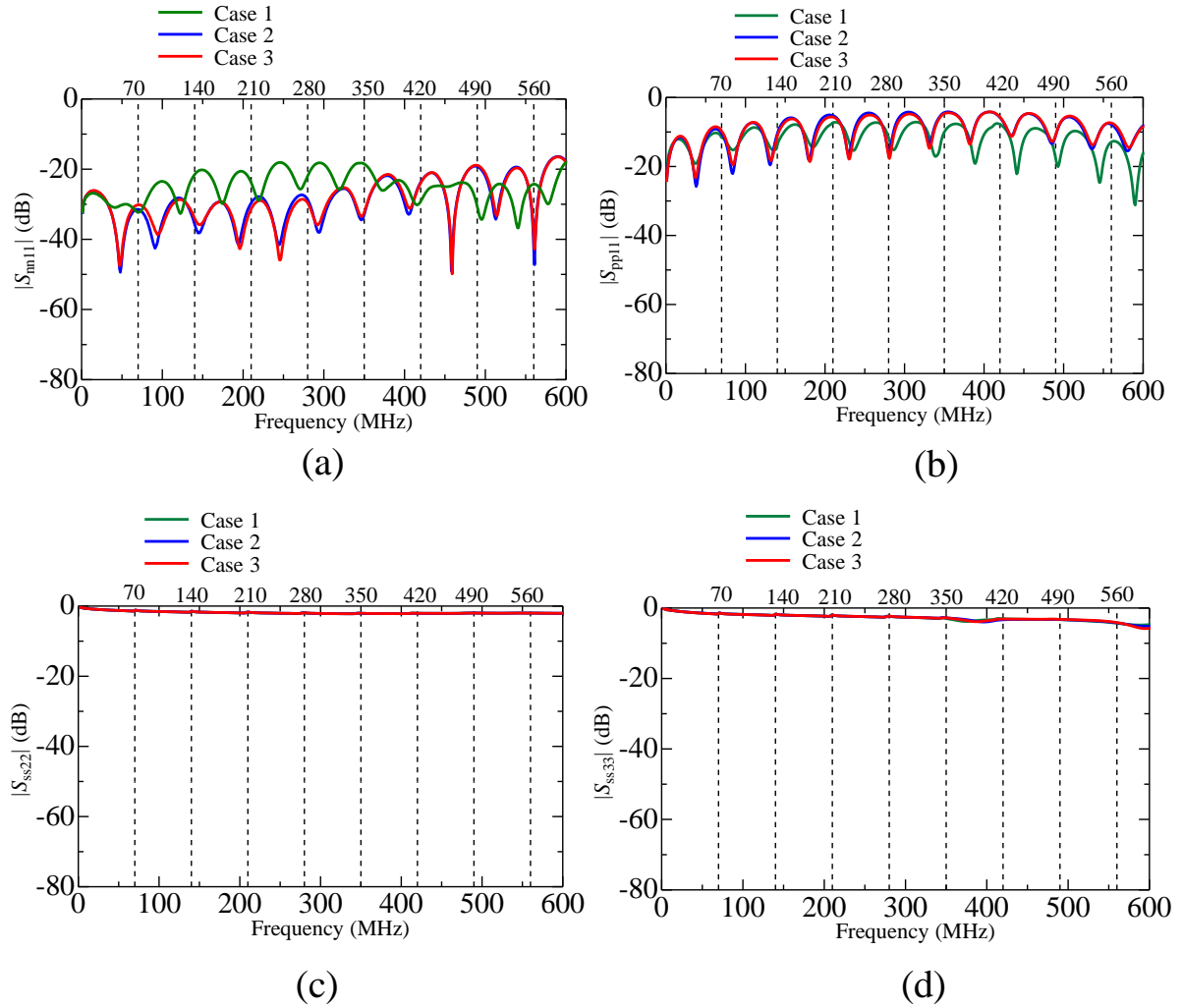


Figure 3.14 Measured spectra of (a) S_{nm11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.

Reflection Characteristics

Fig. 3.14 shows the spectra of mixed-mode S -parameter for reflection characteristics of each mode. Fig. 3.14(a) indicate the reflection characteristics, S_{nm11} , of normal mode for Logical port 1, Fig. 3.14(b) indicate the reflection characteristics, S_{pp11} , of primary-common mode for Logical port 1, Fig. 3.14(c) indicate the reflection characteristics, S_{ss22} , of secondary-common mode for Logical port 2, and Fig. 3.14(d) indicate the reflection characteristics, S_{ss33} , of secondary-common mode for Logical port 3. Fig. 3.14(a) and Fig. 3.14(b) confirmed the transmission of the differential signal through the transmission

line whereas Fig. 3.14(c) and Fig. 3.14(d) indicates that signal does not transmit through the current probe. It is observed from this figure that the imbalance matching method does affect the reflection characteristics of the transmission system as Case 1, Case 2, and Case 3 show almost the same mode conversion amount. It is noticeable from Fig. 3.14(a) that the mode conversion amount for Case 2 and Case 3 are the same but shows some difference with Case 1. Because the same PCB and female connector is used for Case 2 and Case 3 while Case 1 used different PCB and female connector.

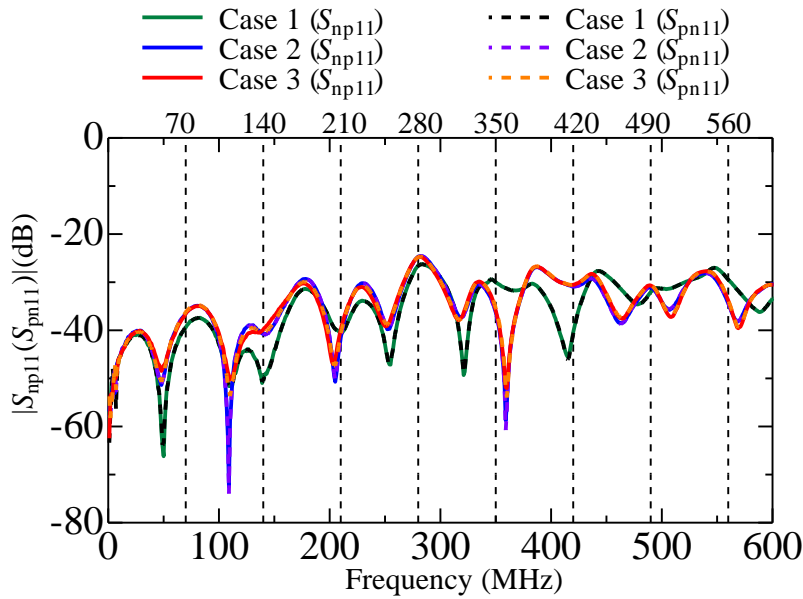


Figure 3.15 Measured spectra of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.

Transmission Characteristics

Fig. 3.15 to Fig. 3.18 shows the transmission characteristics of mode conversion between orthogonal modes. The dotted curve on the graph indicates the spectra of the symmetric mixed-mode S -parameter. Fig. 3.15 and Fig. 3.16 shows the spectra of mixed-mode S -parameter for transmission characteristics of each mode. Fig. 3.15 shows the spectra of S_{np11} (S_{pn11}) indicates the mode conversion between normal mode and primary-common mode. It is observed from this figure that mode conversion amount between the normal-mode and primary-common mode is about -40 dB, and it remain almost same for all Case. Fig. 3.16(a) and Fig. 3.16(b) shows the spectra of S_{ns12} (S_{sn21}) and S_{ns13} (S_{sn31}), respectively, indicating the mode conversion between normal mode and secondary-common mode. It is also observed that the mode conversion amount is at a deficient level close to the noise floor of the vector network analyzer, and it can be said that the mode conversion does not occur with normal mode. Moreover, the improvement around the

connector section for imbalance matching does not affect the mode conversion. Therefore, it is confirmed from Fig. 3.15, Fig. 3.16(a) and Fig. 3.16(b) that mode conversion does not occur with normal mode as we explained it in chapter 2.

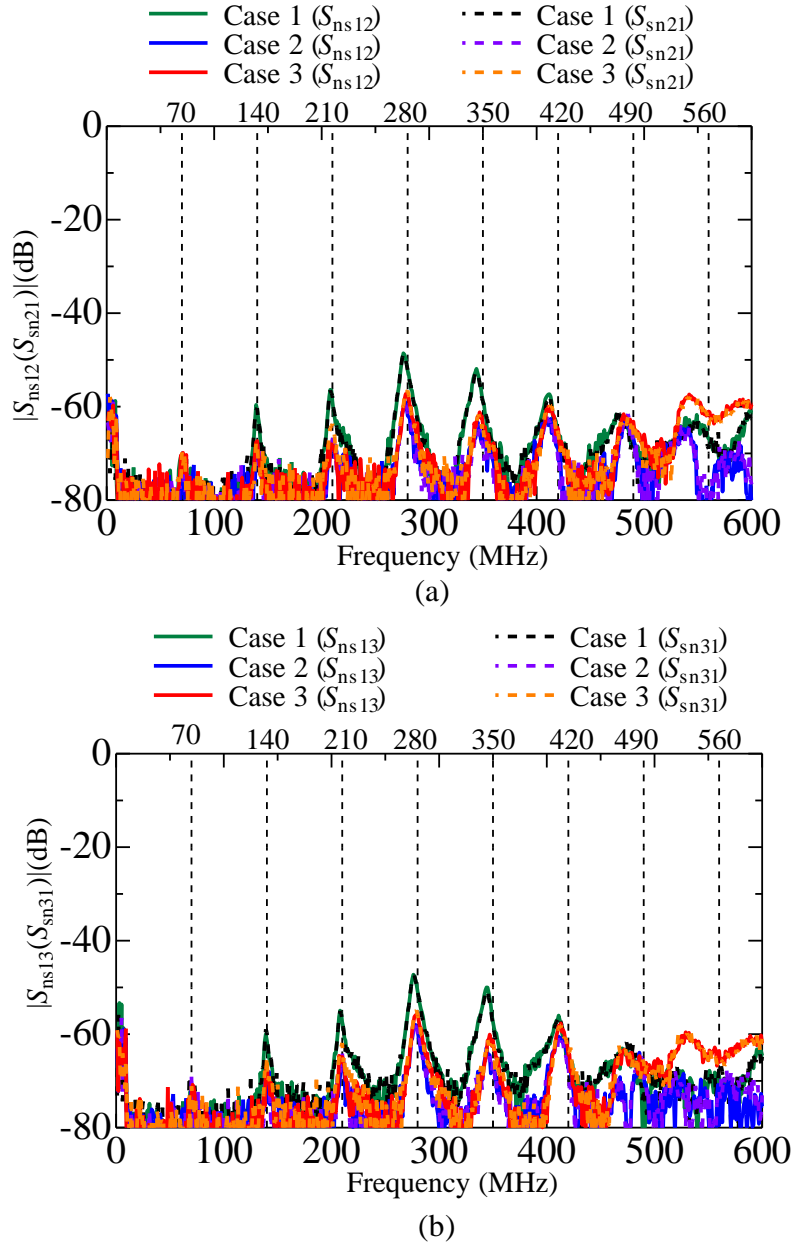
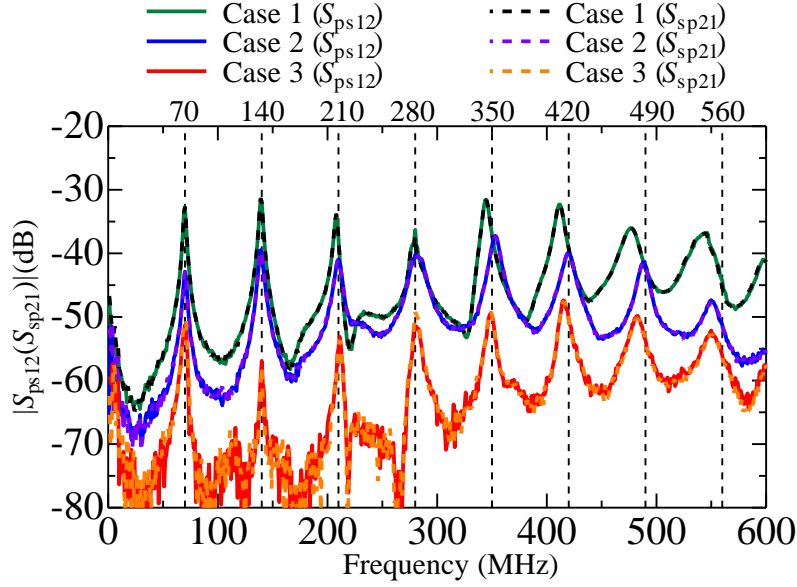
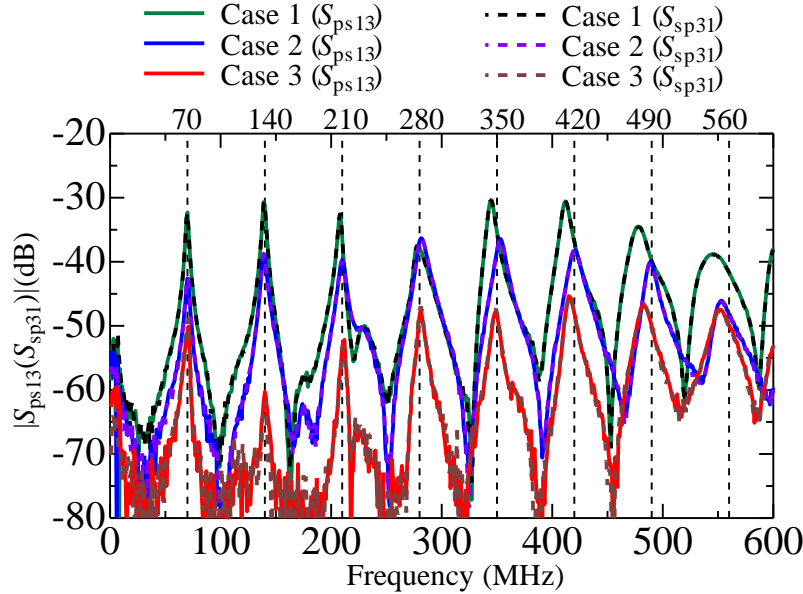


Figure 3.16 Measured spectra of (a) $S_{ns12}(S_{sn21})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ns13}(S_{sn31})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.

Fig. 3.17 shows the mode conversion between primary-common mode and secondary-



(a)



(b)

Figure 3.17 Measured spectra of (a) $S_{ps12}(S_{sp21})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ps13}(S_{sp31})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.

common mode. Fig. 3.17 (a) and Fig. 3.17 (b) shows the spectra of $S_{ps12}(S_{sp21})$ and $S_{ps13}(S_{sp31})$, respectively, indicates the mode conversion between primary-common mode and secondary-common mode. For investigating the effect of imbalance matching method

on mode conversion suppression at the connector section, the mixed-mode S -parameter, S_{ps12} is used as an evaluation index in this experiment. It is noticeable from the Fig. 3.17 (a) that all spectra are similar and have peaks at every resonance frequency with the secondary-common mode. It was experimentally confirmed that Case 3 provides the most reduction of the three, and Case 2 provides the second reduction as predicted. Furthermore, it is observed that the reduction from Case 1 to 2 indicates 8-11 dB, and the reduction from Case 2 to 3 also indicates 8-11 dB, and the reduction is not constant but almost independent of frequency.

And finally, Fig. 3.18 shows the spectra of S_{ss23} (S_{ss32}) indicates the mode conversion between secondary-common mode of Logical port 2 and secondary-common mode of Logical port 3. It is noticeable that the improvement around the connector section for imbalance matching does not affect the mode conversion. Moreover, the dotted line in the figure indicates the reciprocal value of each mixed-mode S -parameter.

It is noticeable from Fig. 3.15, Fig. 3.16, Fig. 3.17 and Fig. 3.18 that the magnitude of mode conversion amount for mixed-mode S -parameter S_{np11} and S_{pn11} , S_{ns12} and S_{sn21} , S_{ns13} and S_{sn31} , S_{ps12} and S_{sp21} , and S_{ss23} and S_{ss32} are same that also confirmed the reciprocal properties of the mixed-mode S -parameter.

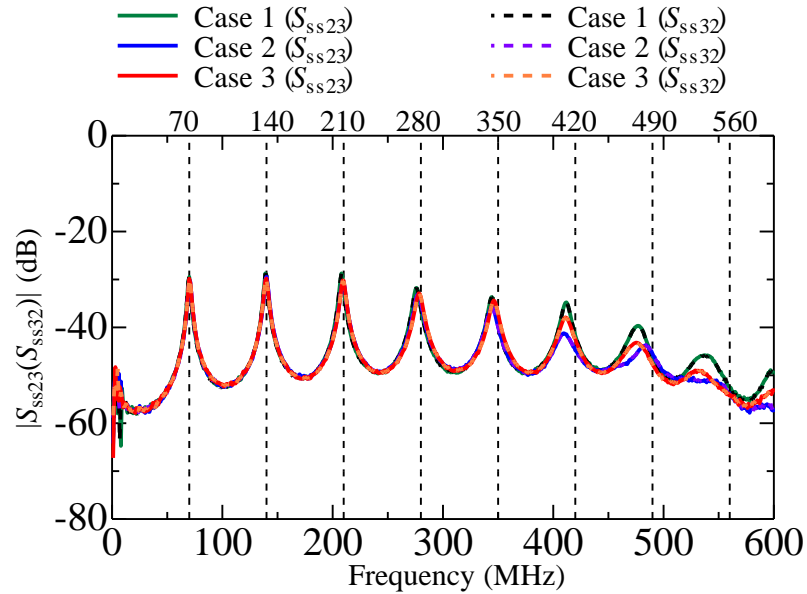


Figure 3.18 Measured spectra of S_{ss23} (S_{ss32}) indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.

3.5 Estimation of Mode Conversion by using Modal-Equivalent Circuit Model

This section estimates the mixed-mode S -parameter at the connector section by using a modal-equivalent circuit model. Then, the validation of the imbalance matching method for suppressing mode conversion at the connector section is carried out by comparing the measurement results with the simulation results obtained from the modal-equivalent circuit model.

3.5.1 Modal-equivalent Circuit Model for Estimating Mode Conversion

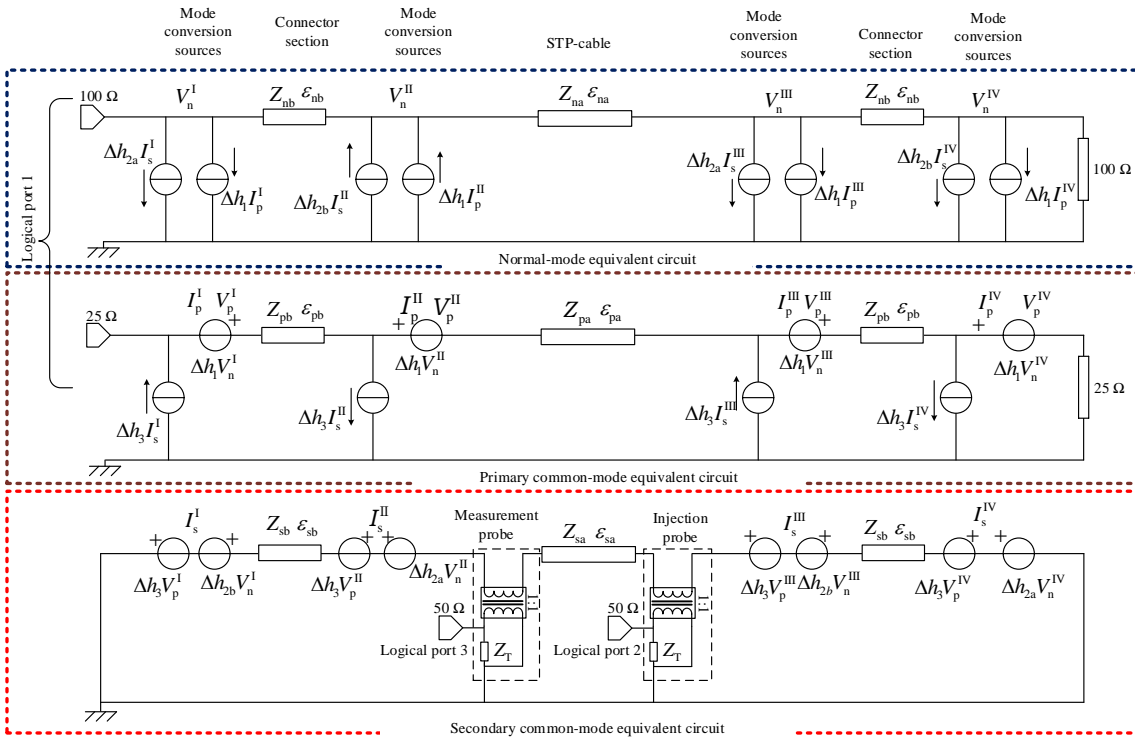


Figure 3.19 Modal-equivalent circuit for circuit simulation.

To simulate the modal-equivalent circuit shown in Fig. 3.19 based on the measurement system shown in Fig. 3.12, we used AWR Microwave Office, a commercial circuit simulator. In the equivalent circuit, the male and female connectors are implemented as one connector in the same way as the measurement system. As shown in Fig. 3.19, the mode conversion sources are inserted into four interfaces in the equivalent circuit.

In the circuit simulation, the exact dimensions as used in the measurement system were provided. In addition, ANSYS Q3D Extractor, a commercial quasi-static 3D electromagnetic field solver, was used to obtain the values of the modal parameters for Case 1,

Case 2, and Case 3. Tables 3.2, as described in section 3.3.3, and Table 3.4 summarize the parameters of the modal-equivalent circuit for Case 1, Case 2, and Case 3, used for simulation. Table 3.4 shows the modal parameters where Z denotes the modal characteristic impedance, and ε denotes the effective permittivity.

Table 3.4 Modal parameters of STP cable and connector section.

STP cable		Connector section			
		Case 1	Case 2	Case 3	
$Z_{na}(\Omega)$	101.62	$Z_{nb}(\Omega)$	142.92	143.12	143.42
$Z_{pa}(\Omega)$	51.5	$Z_{pb}(\Omega)$	128.60	123.16	124.38
$Z_{sa}(\Omega)$	204.5	$Z_{sb}(\Omega)$	64.4	53.46	53.53
ε_{na}	1.63	ε_{nb}	1.63	1.63	1.63
ε_{pa}	1.15	ε_{pb}	1.07	1.07	1.07
ε_{sa}	1.0	ε_{sb}	1.0	1.0	1.0

Table 3.5 Coefficient of mode conversion source at connector section.

	Case 1	Case 2	Case 3
Δh_1	0	0	0
Δh_{2a}	0	0	0
Δh_{2b}	0	0	0
Δh_3	0.090	0.033	0.008

Table 3.5 summarizes the value of the coefficient of mode conversion sources at the connector section based on the value of the imbalance factors of the STP cable and connector section as described in section 3.3.3. The subscripts of a and b represent the STP cable and the connector section, respectively. The value of the mode conversion excitation source coefficient is calculated by using the equation (2.17) to (2.21). It is also observed from Table 3.5 that the value of Δh_1 , Δh_{2a} and Δh_{2b} are become zero for Case 1, Case 2 and Case 3. Hence, it is validated that mode conversion does not occur with normal mode, and mode conversion only occurs between primary common-mode and secondary-common mode.

It is observed from the modal-equivalent circuit of Fig. 3.19 that 24 mode conversion sources are inserted at four interfaces in the equivalent circuit. Under the balanced condition, 16 mode conversion sources in the modal-equivalent circuit become zero, we have only 8 mode conversion sources in the modal-equivalent circuit for obtaining a simulation result that only depends on the value of Δh_3 . As described in Section 3.3.3, the magnitude of the mode conversion sources between the primary-common and secondary-common mode is approaching to zero, resulting in suppression of mode conversion.

In the modal-equivalent circuit for simulation, the current probes are characterized by an ideal transformer and the transfer impedance, Z_T of the current probes as shown

in Fig. 3.19. In the equivalent circuit, the normal-mode and primary-common mode port impedance are 100Ω and 25Ω , respectively. In the circuit simulation, the frequency responses of the transfer impedance, Z_T was used from the datasheet of the current probe.

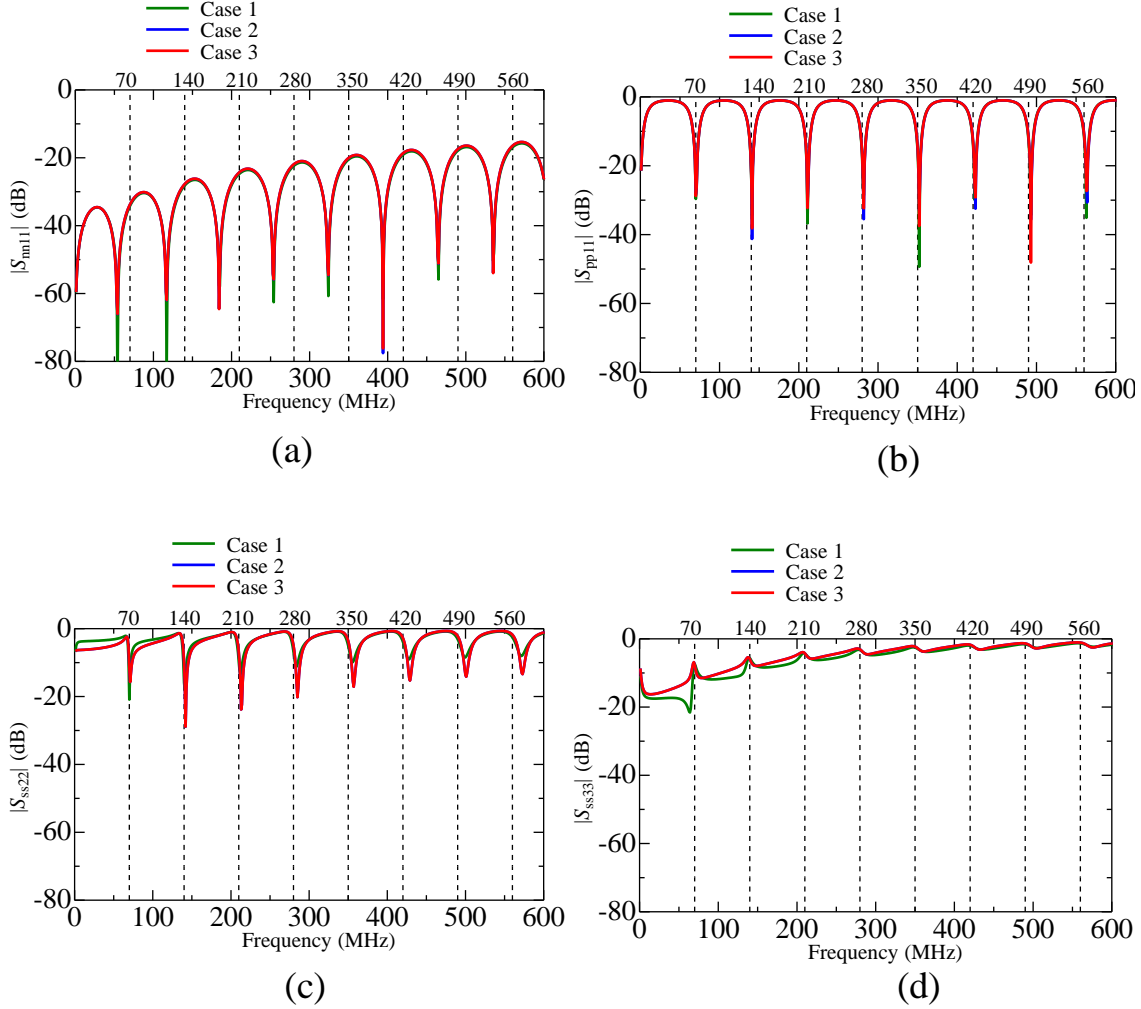


Figure 3.20 Simulation result of (a) S_{nm11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.

3.5.2 Simulation Result obtained from Modal-equivalent circuit

Simulation results are obtained from the modal-equivalent circuit as shown in Fig. 3.19. This simulation result is compared with the measurement result to confirm the validation of the imbalance matching method. We estimate the mixed-mode S -parameter for each Case to evaluate mode conversion suppression based on imbalance matching. As shown

in the simulation result graph, the vertical dashed line is inserted into the graph as in the measurement results, indicating the half-wavelength resonance frequency with the secondary-common mode. The green, blue and red spectra on the graph of the simulation results indicates the simulation result for Case 1, Case 2 and Case3, respectively.

Reflection Characteristics

Fig. 3.20 shows the simulation results of the reflection characteristics of mixed-mode S-parameters obtained from the modal-equivalent circuit model of each mode. Fig. 3.20(a) indicate the reflection characteristics of normal-mode, Fig. 3.20(b) indicate the reflection characteristics of primary-common mode, and Fig. 3.20(c) and Fig. 3.20(d) indicate the reflection characteristics of secondary-common mode. It is observed from this figure that Case 1, Case 2, and Case 3 show almost the same mode conversion amount. Therefore, the imbalance matching method does affect the reflection characteristics, as we observed from the measurement result. The mode conversion amounts are almost the same between the measurement result and simulation result. However, some discrepancy was observed with the reflection characteristics for the secondary-common mode.

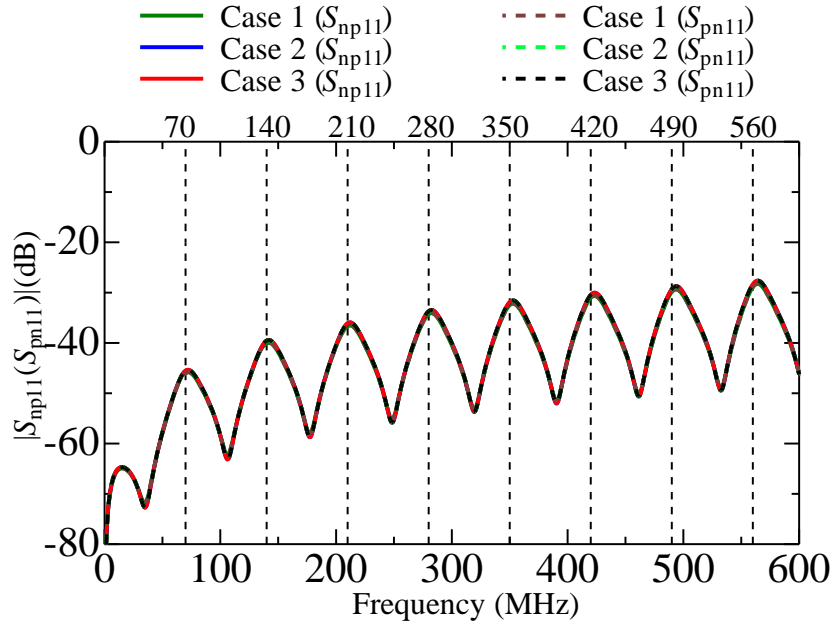


Figure 3.21 Simulation result of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.

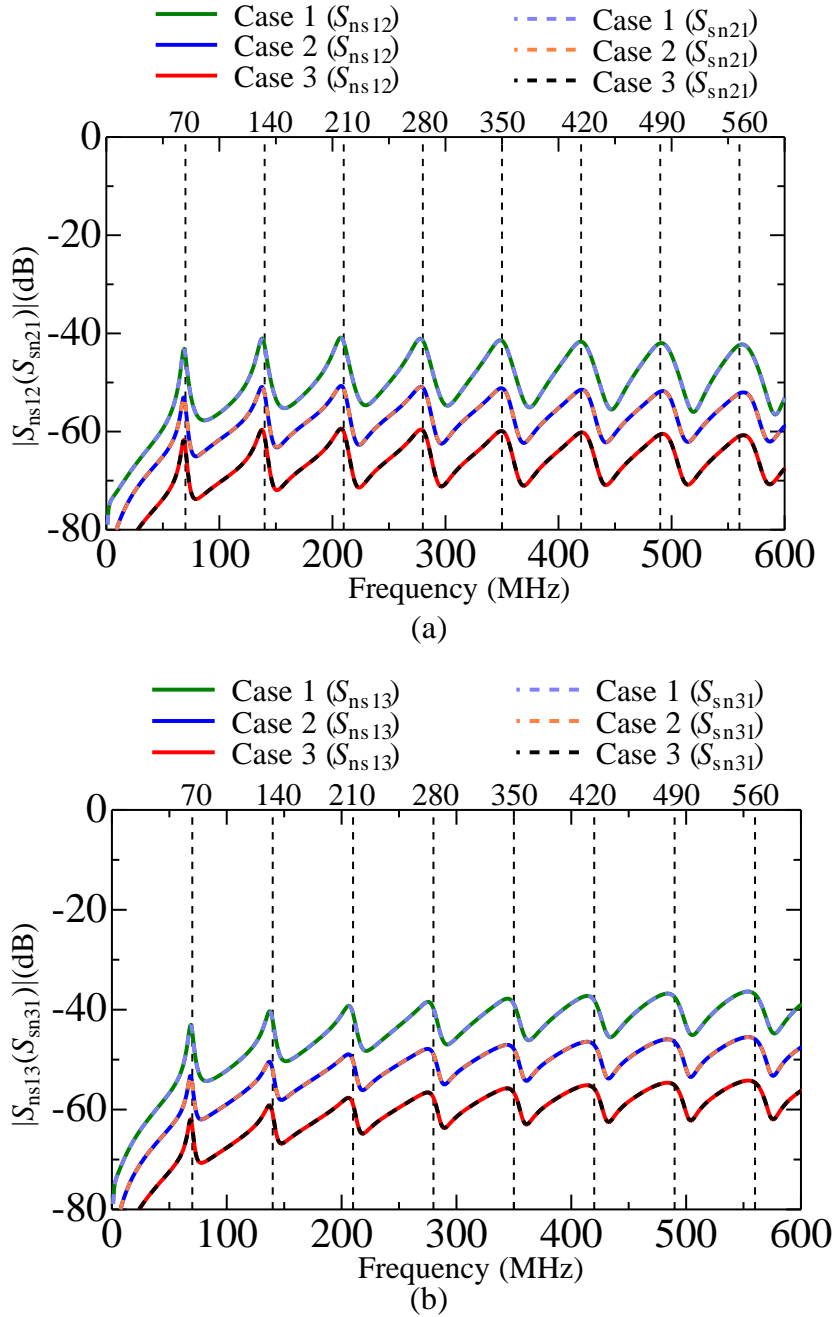


Figure 3.22 Simulation result of (a) $S_{ns12}(S_{sn21})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ns13}(S_{sn31})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.

Transmission Characteristics

Fig. 3.21 and Fig. 3.23 shows the spectra of mixed-mode S-parameter for transmission characteristics between each mode. The spectra of Fig. 3.21 that indicates the mode

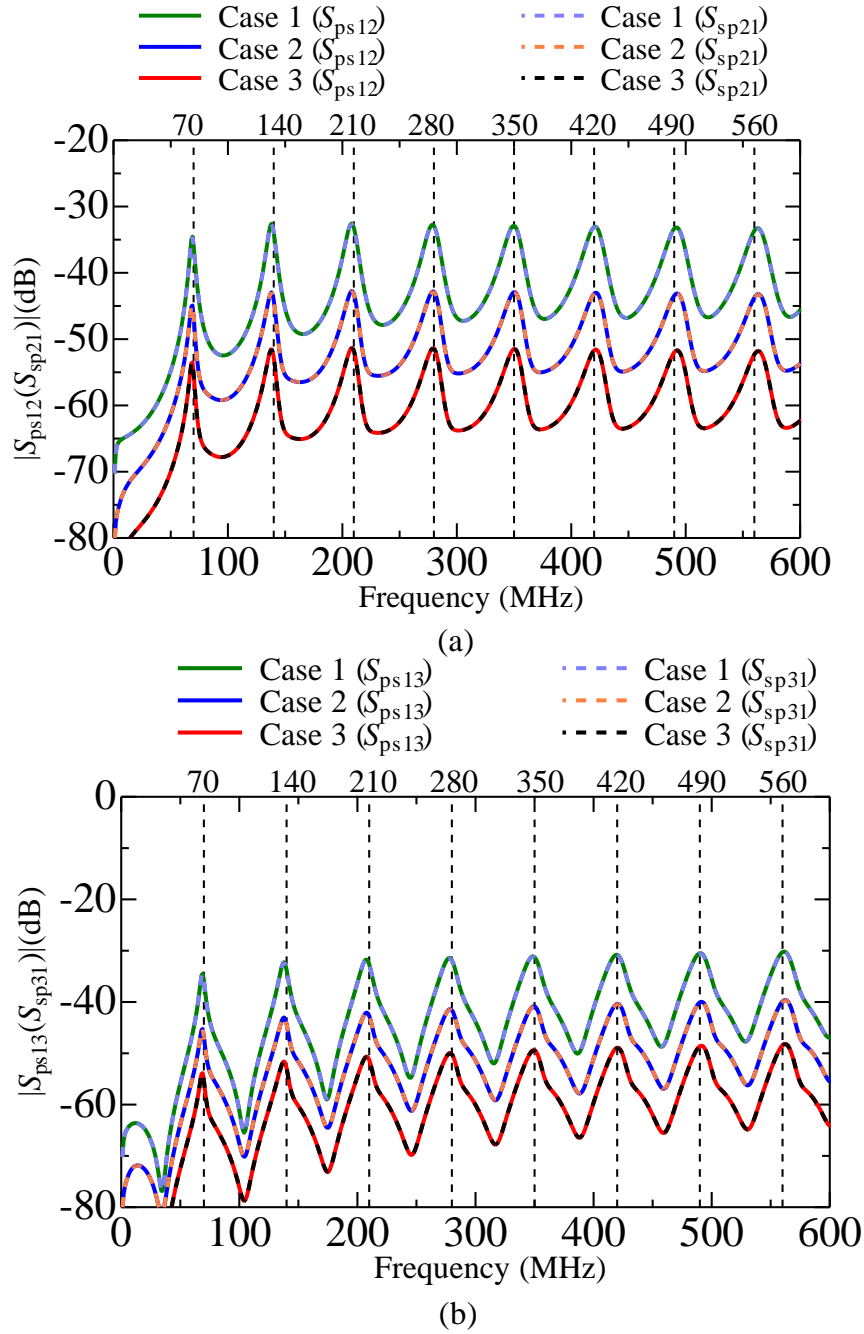


Figure 3.23 Simulation result of (a) $S_{ps12}(S_{sp21})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ps13}(S_{sp31})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.

conversion between normal mode and primary-common mode, $S_{np11}(S_{pn11})$, shows the mode conversion amount about -40 dB for Case 1, Case 2, Case 3, and it remains almost the same with the measurement result. The imbalance matching method does not affect the

mode conversion amount between normal mode and primary-common mode as the mode conversion amount for all Case are same. Fig. 3.5.2 (a) and Fig. 3.5.2 (b) shows the spectra of $S_{ns12}(S_{sn21})$ and $S_{ns13}(S_{sn31})$, respectively, indicates the mode conversion between normal mode and secondary-common mode. It is confirmed from Fig. 3.21, Fig. 3.5.2(a), and Fig. 3.5.2(b) that mode conversion does not occur with normal mode as we obtained from the measurement result.

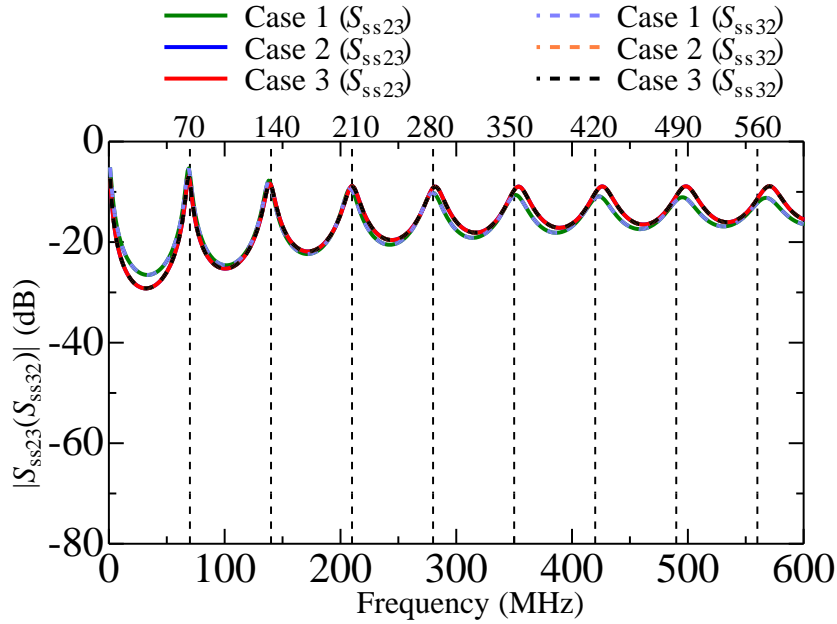


Figure 3.24 Simulation result of $S_{ss23}(S_{ss32})$, indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.

Fig. 3.23 shows the mode conversion between primary-common mode and secondary-common mode. Fig. 3.23 (a) and Fig. 3.23 (b) shows the mixed-mode S -parameter $S_{ps12}(S_{sp21})$ and $S_{ps13}(S_{sp31})$, respectively. It is observed from Fig. 3.23 (a) that all spectra have a sharp peak at every resonance frequency. Since the imbalance factor is independent of frequency, the frequency variation in the reduction amounts of mode conversion stays constant in the frequency range of interest, which indicates 10-11 dB for Case 1 to 2 and 8-9 dB for Case 2 to 3. It is noticeable from this figure that Case 3 provides the most reduction of the three, as we observed from the measurement result. In the next section, we validate the imbalance matching method by comparing the measurement result and the simulation result based on the evaluation index S_{ps12} . Furthermore, the spectra of Fig. 3.24 show the mode conversion between the secondary-common mode of Logical port 2 and secondary-common mode of Logical port 3. It is noticeable that the improvement around the connector section for imbalance matching does not affect the mode conversion amount.

The dotted line in the figure indicates the reciprocal value of each mixed-mode S -

parameter. It is observed from Fig. 3.21, Fig. 3.5.2, Fig. 3.23 and Fig. 3.24 that the simulation result obtained from modal-equivalent circuit confirmed the reciprocal properties of the mixed-mode S -parameter as we confirmed with the measurement result.

3.6 Verification of Mode Conversion Suppression Method by Comparing Measurement Result with Simulation Result

The validation of the imbalance matching method for improving EMI issues in a signal transmission line by suppressing mode conversion at the connector section is carried out by comparing the measurement results with the simulation results. The solid and dotted spectra on Fig. 3.25 indicate the measurement and simulation result, respectively. Moreover, the green, blue, and red spectra of this figure correspond to Case 1, Case 2, and Case 3, respectively. Fig. 3.25 (a) and (b) shows the measurement and simulation result for 600 MHz and 100 MHz, respectively.

It is observed from this figure that all spectra have a sharp peak at every resonance frequency. It is noticeable from this figure that there is a good agreement between the measured and estimated result in the frequency range below 600 MHz. The disagreement with the measurement results at resonance frequency is at most 5 dB. At most resonant frequencies, the disagreement is low. It can be ignored compared to the error that may occur due to the environment of the evaluation system and the values of the parameters used for simulation.

If we focus on the first resonant point as shown in Fig. 3.25 (b), there is a good agreement between the measurement and simulation result for Case 2 when we improved the footprint of the female connector on the PCB surface. The comparison demonstrates that the improvement of the footprint of the female connector on PCB surface suppresses mode conversion at the connector section to improve EMI issues in the signal transmission line. Furthermore, it is also observed from this figure that there is also a good agreement between measurement and simulation results for Case 3.

Therefore, the comparison of spectra shown in Fig. 3.25 validated that the improvement based on imbalance matching at the connector section makes the imbalance factor of the connector section closer to that of the cable section and results in the suppression of the mode conversion.

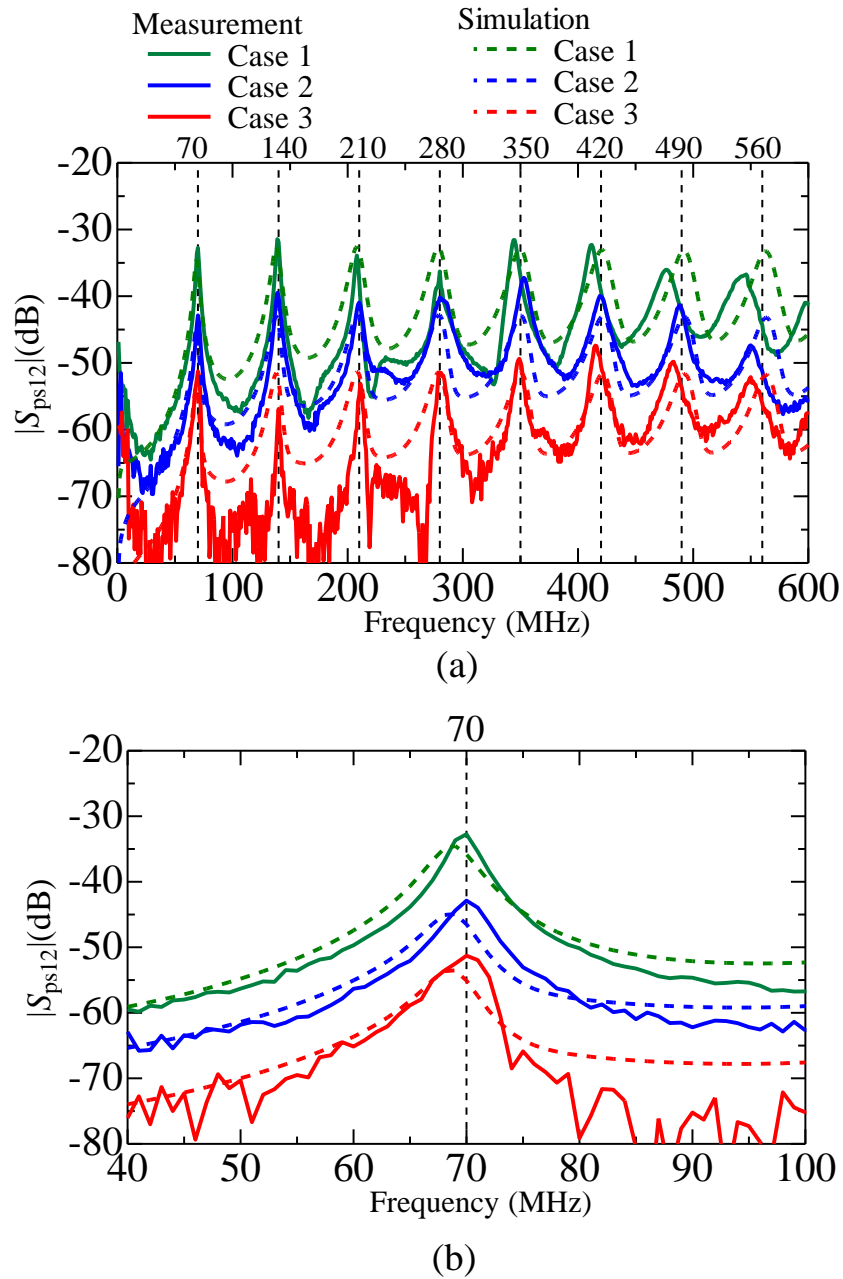


Figure 3.25 Measured and simulation spectra of S_{ps12} (a) Up to 600MHz (b) At first resonance frequency.

3.7 Conclusion

Mode conversion between the secondary-common mode and the primary-common mode at the connector section becomes problematic, and imbalance factor h_{3b} of the connector section depends on the structure of the shield that can be evaluated. The mode conversion amount can be suppressed by reducing the value of Δh_3 . Therefore, this chapter proposed an imbalance matching method at the connector section to suppress mode conversion by matching the imbalance factor of the connector section h_{3b} with the imbalance factor of the cable section h_{3a} .

Due to the inadequate shielding around the connector section, mode conversion occurs because of the difference in the imbalance factor between the connector section and the cable section. It was observed that the inadequate shielding at the footprint of the female connector on the PCB surface actually causes mode conversion. Moreover, the insufficient shield on the edge of both connectors and a gap between the underside of the female connector and the printed circuit board (PCB) also causes mode conversion. The improvement of the footprint of female connector on PCB surface and the inadequate shielding at the edge of male and female connector achieves imbalance matching between the connector and cable sections. As a result, the application of the improvement based on imbalance matching at the connector section makes the imbalance factor of the connector section closer to 1, which is the imbalance factor of the cable part and results in the suppression of the mode conversion.

It was experimentally numerically confirmed that mode conversion is suppressed by 11 dB at the first resonance frequency for Case 2 when improved the footprint of female connector on the PCB surface. This reduction level is almost the same for the rest of the resonance frequencies. Furthermore, the validation of imbalance matching for suppressing mode conversion at the connector section for Case 3 is also achieved by comparing the measurement results with the simulation results. It was observed that the simulation result obtained from the modal-equivalent circuit agrees well with the measurement result.

Therefore, the effect of the improvement based on imbalance matching at the connector section on mode-conversion suppression was experimentally and numerically validated.

Chapter 4

Enhancement of Hardware Security through Mode Conversion Analysis

4.1 Introduction

Recently leakage and manipulation of information are becoming realistic threats to hardware security even in consumer products, such as smart cards, server computers, memory cards, and automated teller machines (ATMs). Methods for attacking cryptographic modules, known as side-channel attacks (SCA), have been developed [25,28] that can make the cryptographic modules vulnerable.

SCA is a major concern for designers of cryptographic modules that contain software or hardware implementation of cryptographic algorithms. During encryption or decryption of those cryptographic modules, secret information can be leaked as side-channel information, such as through change in power consumption or electromagnetic (EM) radiation [25,28]. Previous research [26,27] confirmed the leakage of secret information outside a cryptographic module via the common-mode current in power/communication cables and that this threatens hardware security. In this scenario, an attacker can acquire the common-mode-current waveform without being in close contact with the cryptographic module. Therefore, the common-mode current in a power cable is one of the main factors of unintended EM radiation, and hence, it needs to be reduced to counteract information leakage.

To reduce the CM current on the power cable, a decoupling capacitor was placed close to the cryptographic field-programmable gate array (FPGA) [26]. However, while this technique suppresses supply-voltage fluctuation and act as a standard SCA countermeasure as well [26,36], it cannot suppress mode conversion to reduce the common-mode current. Thus, information leakage remains a possibility. To enhance the security of the cryptographic module against SCA, therefore, we need to reduce the common-mode current to make the cryptographic module tolerant against SCAs from outside the module.

To enhance the SCA resistance of a cryptographic module if an attacker is at a remote location, we apply the mode-conversion suppression technique at the discontinuity

point on a power delivery network (PDN) where the imbalance factor changes. With the encryption or decryption operation, the normal-mode noise on a power delivery network (PDN) initially contains the secret information from the cryptographic module. Due to mode conversion at the interface where the imbalance factor of the transmission line changes [19], the common-mode current generates. Then mode conversion conveys the secret information as side-channel information from the normal-mode noise to the common-mode current. The modal-equivalent circuit model assumes that the common-mode electromotive force is proportional to the product of the normal-mode voltage at the discontinuity point where the imbalance factor changes [19] and imbalance difference between two transmission line. We previously found that a capacitor at the discontinuity point on a PDN suppresses mode conversion and hence that it successfully reduces common-mode current in a power cable [49]. Therefore, the attacker has less side-channel information to reveal secret information. In this study, we experimentally investigated the effect of installing a capacitor at the discontinuity point on mode-conversion suppression, which can mitigate the threat of a cryptographic secret key being stolen through an SCA.

In this chapter, we validate the mode-conversion suppression technique that places a capacitor at the connector section to counteract SCAs. Using a cryptographic board called the side-channel attack standard evaluation board (SASEBO) [71], we confirmed the reduction of the common-mode current and the normal-mode voltage with the capacitor placed at the discontinuity point on the PDN. This chapter evaluates the common-mode current flowing through the power cable by correlation power analysis (CPA) [24], a primary side-channel analysis method for block ciphers like advanced encryption standard (AES), and clarifies that the capacitor placed at the connector section, which is the discontinuity point of PDN where the imbalance factor changes, can enhance hardware security efficiently by suppressing mode conversion successfully. It verifies experimentally that the application of the mode conversion suppression technique enhances hardware security of the cryptographic modules as it improves the SCA resistance when information leaks via common-mode current.

Section 4.2 explain the generation of common-mode current that is responsible for information leakage. We also explain the mode conversion mechanism for suppressing mode conversion by reducing normal-mode voltage, V_n and improved resistance against information leakage. In section 4.3, we discuss applying the mode conversion suppression technique at the discontinuity point on the PDN to enhance hardware security. Section 4.4 explained the measurement setup for this experiment. Finally, in section 4.5, the measurement result and CPA result of the measured waveform of the common-mode current on the power cable have been explained to validate the countermeasure method experimentally based on the mode conversion mechanism.

4.2 Information Leakage via Common-mode Current

This section described the factors that are responsible for information leakage from the cryptographic module. In this experiment, we focus on the information leakage from outside the cryptographic module via common-mode current. First, we described the generation of common-mode current based on the mode conversion mechanism.

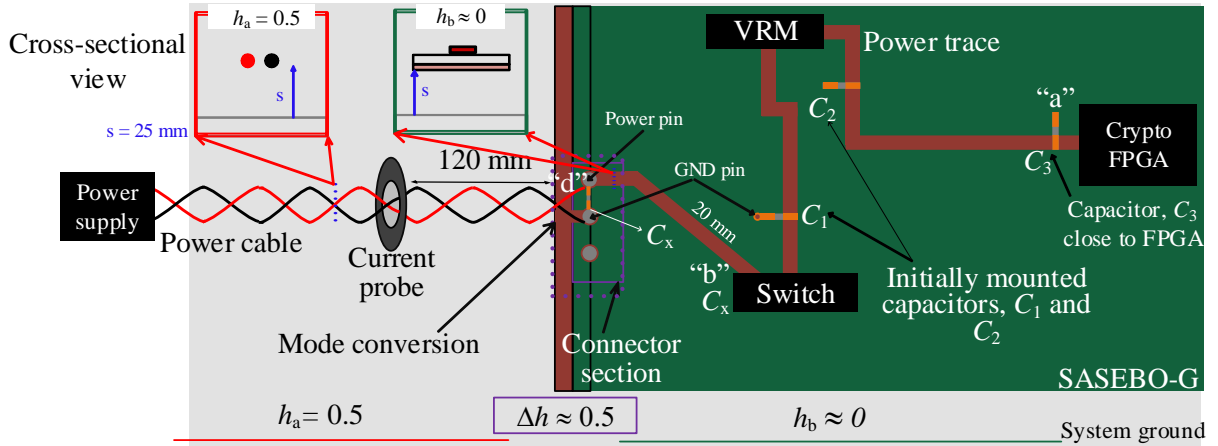


Figure 4.1 PDN of SASEBO-G board from power supply to cryptographic FPGA.

In practice, a cryptosystem is implemented on a physical device. It is very difficult to break the cryptographic algorithm. However, during cryptographic computations, the physical devices usually reveal some information in terms of power consumption and time of computation or electromagnetic leakage. This information is called side-channel information. Side-channel attacks (SCA) are among the most powerful attacks where secret information is extracted from the cryptographic chip or cryptographic system through measurement and analysis of this side-channel information.

The attacker can acquire the side-channel information by direct access to the cryptographic module [36] or outside the cryptographic module via common-mode current [26, 41, 76]. In this experiment we focus on information leakage from outside the cryptographic module via common-mode current. The attacker uses the waveform of common-mode current on the power cable as the side-channel information to reveal the secret information. The common-mode current is generated due to mode conversion at the discontinuity point on the cryptographic module. Therefore, to countermeasure against SCA when information is leaked outside the cryptographic module, it is essential to understand the generation of common-mode current and reduce it based on the mode conversion mechanism.

Fig. 4.1 illustrate PDN for delivering power to a cryptographic FPGA through the cable and traces on the board. The cable is a twisted pair cable and the trace on the board is a microstrip line connected through an on-board connector and the board is placed at 25 mm above the system ground. At the connector section, the current division

factors [14], which quantify the electrical imbalance of a transmission line as the imbalance factor, of the cable, h_a , and the board, h_b , are 0.5 and around 0, respectively, as shown in Fig. 4.1. The imbalance factor of the cable and the board are obtained from the capacitance matrices of the transmission lines [14, 15]. The difference in the imbalance factor Δh reveals the impact of the discontinuity between the cable and trace on mode conversion.

Mode conversion occurs at the discontinuity point on a PDN and conveys the side-channel information in the normal-mode noise to the common-mode current. As a result, the common-mode current flows through the power cable with the side-channel information and is thus responsible for information leakage. An attacker can acquire the waveform of the common-mode current in the cable without being in close contact with a cryptographic module and conduct CPA to retrieve the secret key information [26]. As a result, security attacks, such as SCAs, become a major concern for hardware security. We need to reduce the common-mode current efficiently to enhance hardware security. Therefore, it is essential to suppress mode conversion at the discontinuity point of the imbalance factor on a PDN to reduce the common-mode current and counteract SCAs. The following section described the mode conversion suppression technique and explains how a capacitor at the discontinuity point of PDN suppressed mode conversion by reducing normal-mode voltage.

4.3 Mode Conversion Suppression Technique at Connector Section of PDN to Enhance Hardware Security

In this section, the mode conversion suppression technique is applied at the discontinuity point (connector section) on the power delivery network (PDN) where imbalance factor changes to enhance hardware security when secret information leaks outside the cryptographic module via common-mode current. We placed a capacitor at the discontinuity point of PDN to reduce the normal-mode voltage, V_n and hence suppressed mode conversion. Therefore, common-mode current reduces and enhance hardware security.

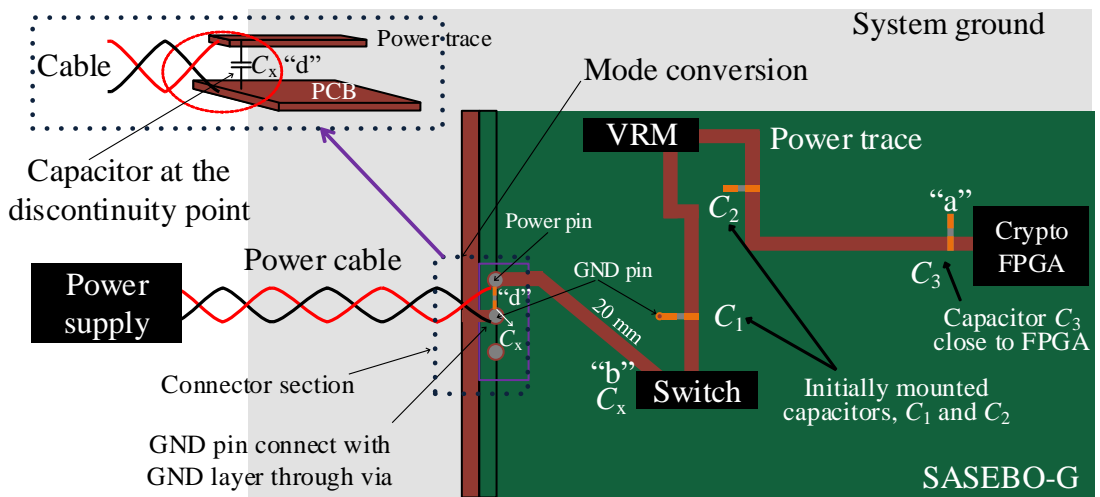


Figure 4.2 Capacitor mounting position on PDN for suppressing mode conversion.

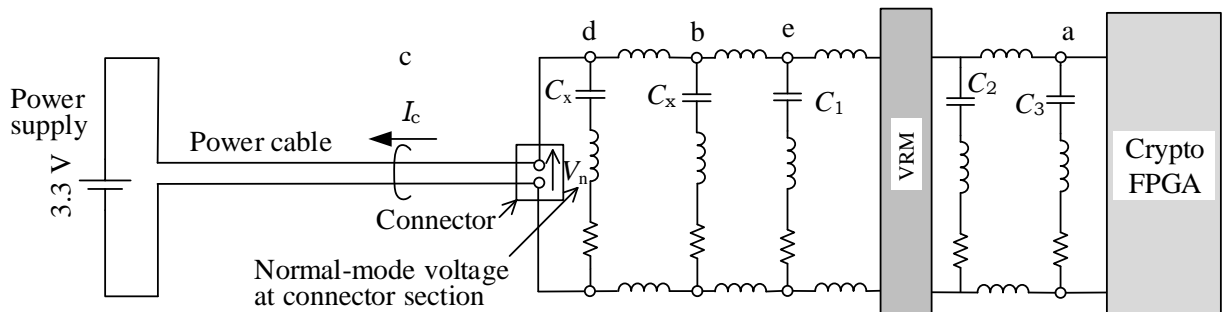


Figure 4.3 Circuit diagram of PDN based on Fig. 4.2.

4.3.1 Mode Conversion Suppression Technique to Enhance Hardware Security

In this chapter, we use the mode-conversion suppression technique at the connector section on the PDN to counteract SCA when information leaks outside the cryptographic module via common-mode current flowing through the power cable. The amount of mode conversion at the discontinuity point is given by the product of Δh and normal-mode voltage V_n [19]. Mode conversion can be suppressed by reducing V_n or Δh at the discontinuity point. In our previous study [49], we used a capacitor to suppress mode conversion by reducing V_n at the discontinuity point. In this chapter, we applied the mode-conversion suppression technique we used in that previous study as an SCA countermeasure.

Fig. 4.2 shows the capacitor-mounting position on the PDN, and Fig. 4.3 shows the corresponding circuit diagram. The left end and the right end of the circuit diagram represents the power supply, and the cryptographic FPGA, respectively. “d” and “c” on the circuit diagram indicating the measurement ports of V_n and I_c , respectively. As shown, several capacitors are mounted on the PDN. The initially mounted capacitors C_1 and C_2 are kept on the board so as not to affect the measurement results. The decoupling capacitor C_3 is mounted at “a” close to the cryptographic FPGA [26, 36], to suppress supply-voltage fluctuations. To confirm the importance of the capacitor-mounting position to counter SCAs, an additional capacitor, C_x , is also mounted on the PDN. We investigated the following three conditions:

Reference: C_1 , C_2 , and C_3 placed on the PDN

Condition 1: C_x is placed at the connector section with C_1 , C_2 , and C_3

Condition 2: C_x is placed on the board at 20 mm from the connector section with C_1 , C_2 , and C_3

Table 4.1 Different measurement conditions.

Capacitor mounting position	Reference	Condition 1	Condition 2
position "a"	C_3	C_3	C_3
position "d"	Not placed	C_x	Not placed
position "b"	Not placed	Not placed	C_x

Table 4.1 summarized the three different conditions that are used in this experiment. It is observed from Table 4.1 that C_3 is mounted at “a”, close to the cryptographic FPGA, and the other two capacitor mounting positions “d” and “b” are open, which corresponds to Reference condition. In condition 1, a capacitor, C_x is mounted at “d”

4.3 Mode Conversion Suppression Technique at Connector Section of PDN to Enhance Hardware Security

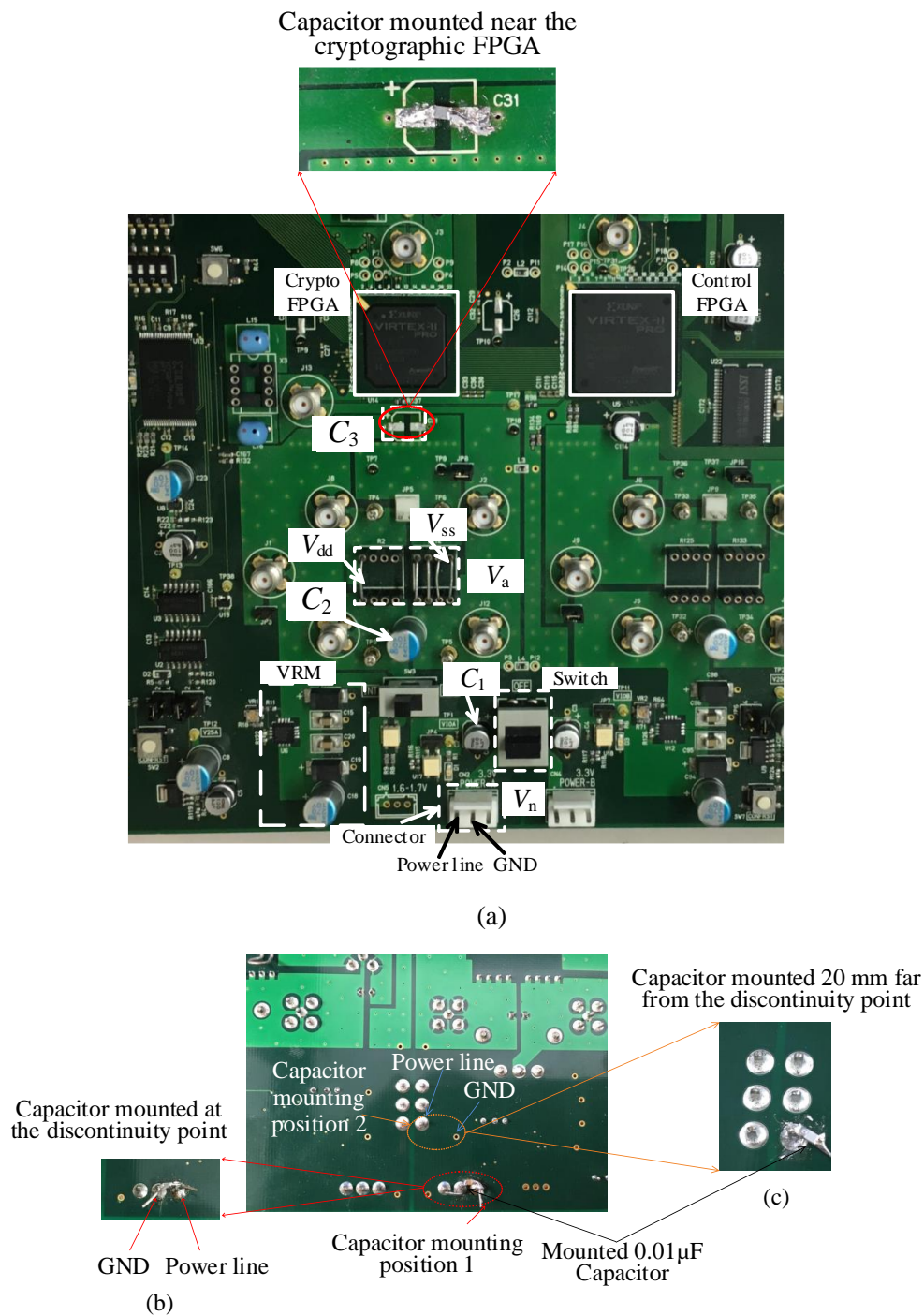


Figure 4.4 Real picture of capacitor mounting position on cryptographic module. (a) Capacitor mounted close to the cryptographic FPGA, (b) Capacitor mounted at the discontinuity point, (c) Capacitor mounted on the board 20 mm far from the discontinuity point.

and C_3 is mounted at “a” as shown in Fig. 4.2. In this case, the capacitor mounting position “b” is open. In condition 2, we placed C_3 and C_x , and the capacitor mounting

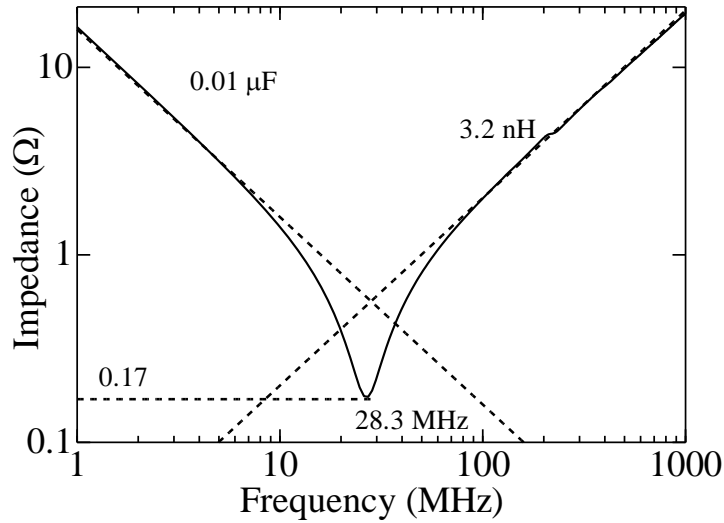


Figure 4.5 Impedance of capacitor.

position “b” is open, as described in Table 4.1. Fig. 4.4 shows the real picture of capacitor mounting position on the cryptographic module. In this figure, Fig. 4.4 (a) corresponds to Reference condition, Fig. 4.4 (b) corresponds to condition 1 and Fig. 4.4 (c) corresponds to condition 2.

The additional capacitor C_x is a 2012 sized chip capacitor and has the same value of $0.01 \mu\text{F}$ as C_3 placed close to the cryptographic FPGA. The impedance of the capacitor is shown in Fig. 4.5. It is observed from this figure that the resonance frequency of the chip capacitor is 28.3 MHz that is higher than the clock frequency of the cryptographic module. The resonance frequency of the capacitor must be higher than the clock frequency of the cryptographic module. Otherwise, the side channel information will not contain effective secret information. Because the cryptographic module starts encryption/ decryption operation at clock frequency, and the side-channel information may contain the secret key information at this frequency band. The capacitor has its equivalent series inductance (ESL) of 3.2 nH, and the resistance of 0.17Ω .

For Condition 1, C_x is placed at the connector section “d” between the power trace and ground plane on the board and should reduce V_n more than at any other location on the board trace. Hence, this location will suppress mode conversion and I_c the most. For Condition 2, C_x is placed on the board at “b” 20 mm from the connector section to determine the appropriate capacitor-mounting position on a PDN for efficiently reducing V_n and suppressing mode conversion. The noise filter is generally placed close to the noise source. In this case, the noise source is the cryptographic FPGA; hence, Condition 2 can be considered an option to reduce the normal-mode noise, not the common-mode noise. We verified the reduction of I_c to counter SCAs by suppressing mode conversion at the

connector section on a PDN.

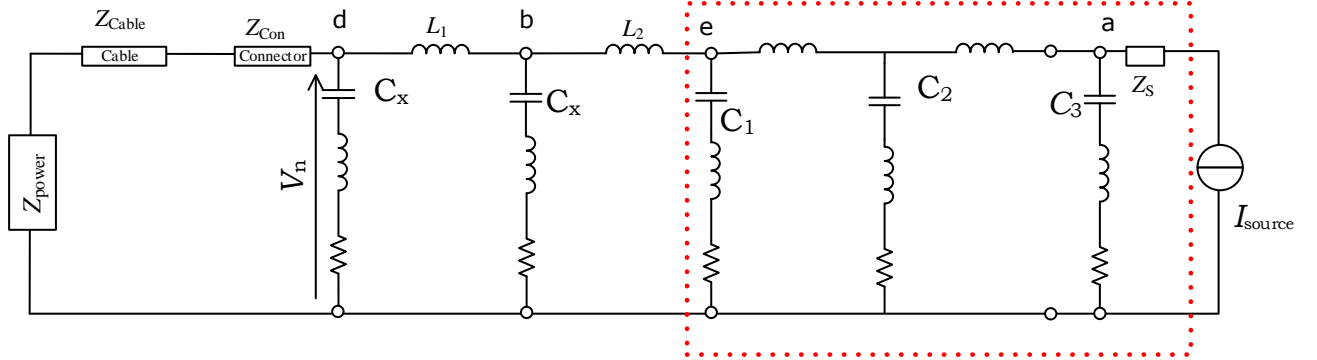


Figure 4.6 Equivalent circuit based on the circuit diagram of Fig. 4.3

4.3.2 Reduction of Normal-mode Voltage V_n by Placing Capacitor at the Discontinuity Point on the PDN

Fig. 4.6 shows the equivalent circuit based on the circuit diagram of PDN shown in Fig. 4.3. The equivalent circuit model represents the FPGA is composed with an equivalent impedance Z_s and an equivalent current source I_{source} . Fig. 4.7 represents the simplified equivalent circuit based on Fig. 4.6. Table 4.2 summarized the parameters of the equivalent circuit. In this simplified equivalent circuit, the dotted line portion of Fig. 4.6 is replaced with the Z_e and V_e , represent Thevenin's equivalent voltage source of the network between the FPGA and C_1 in Fig. 4.6 and the switching noise that caused by FPGA activity and contains the side-channel information, respectively, Z_x is the impedance of the decoupling capacitor C_x , L_1 is the ESL of the trace between the two ports "d" and "b", and L_2 is the ESL of the trace between the two ports "b" and "e". For condition 1, C_x is on Port "d", and Port "b" is open. The normal-mode voltage, V_n , at the discontinuity point at the discontinuity point is expressed by the following equations [49],

$$V_n \simeq \frac{Z_x}{Z_x + Z_e + j\omega(L_1 + L_2)} V_e, \quad (4.1)$$

And, for Condition 2, C_x is on Port "b", and Port "d" is open. The equation of the normal-mode voltage, V_n , is written as,

$$V_n \simeq \frac{Z_x}{Z_x + Z_e + j\omega L_2} V_e, \quad (4.2)$$

When we mount a capacitor at the discontinuity point on the PDN, it provides a low resistance path for the noise because Z_x is much lower than the impedance of the power-line cable. Hence, the normal-mode voltage, V_n decreases. When we place C_x at port "d", as shown in Fig. 4.7, V_n should reduce the most. When we place C_x at port "b",

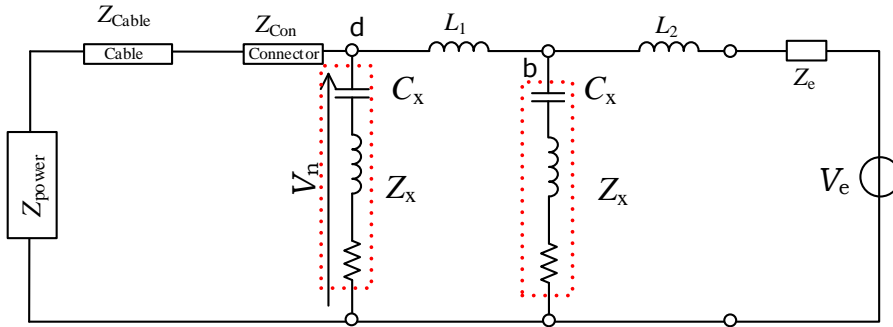


Figure 4.7 Simplified equivalent circuit.

Table 4.2 Variable in Fig. 4.6 and Fig. 4.7

Variable	Meaning
Z_{power}	Internal impedance of power supply
Z_{Cable}	Characteristic impedance of power cable
Z_{Con}	Characteristic impedance of connector on the board
Z_x	impedance of the decoupling capacitor C_x
I_{source}	Noise source
Z_s	Noise source internal impedance
L	ESL of the trace between the two ports "d" and "e"
L_1	ESL of the trace between the two ports "d" and "b"
L_2	ESL of the trace between the two ports "b" and "e"
V_e	Thevenin's equivalent voltage source
Z_e	Thevenin's equivalent impedance

the additional trace length of 20 mm for position "b" includes the additional inductance, i.e. L_1 as shown in Fig. 4.7, which lowers the denominator of equation (4.3) and increase V_n , and prevent the common-mode current, I_c suppression. Therefore, a capacitor placed at the discontinuity point on the PDN should reduce V_n than any other location on the trace line. As a result, the capacitor at this discontinuity point suppressed mode conversion successfully. Hence, I_c should reduces and this decrease will be an effective countermeasure against SCAs.

4.4 Measurement Setup

In this section, we describe the measurement setup for measuring the waveform of normal-mode voltage, V_n at the connector section on PDN where imbalance factor of the transmission line changes and the common-mode current, I_c on the attached power cable. At first, we explain the cryptographic module that is used in this experiment. Then, explain the encryption algorithm and power analysis method. And, finally explain the measurement conditions and setup.

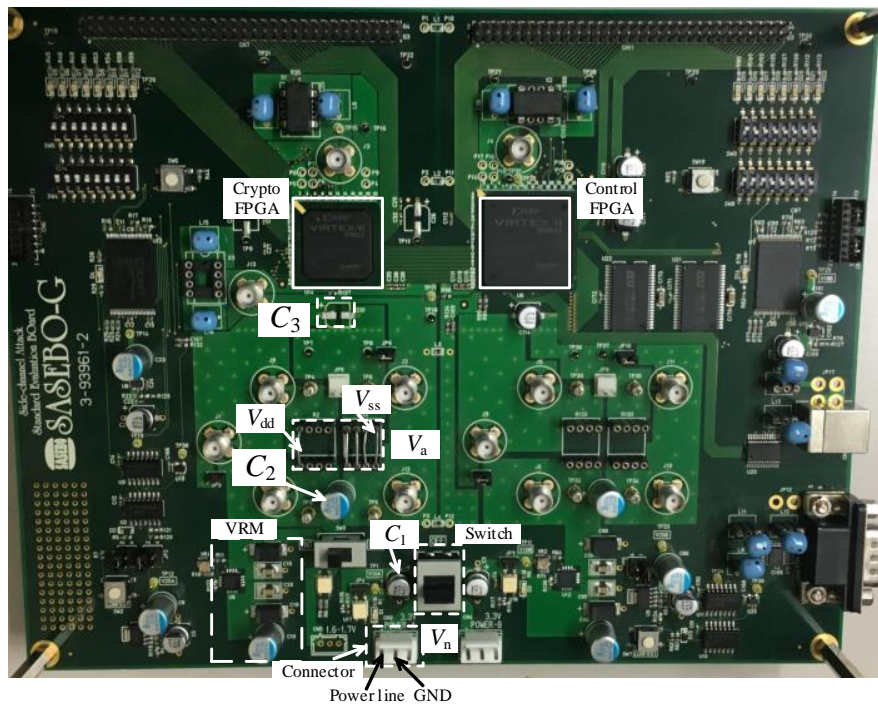
4.4.1 Test Board for Analysis

The targeted cryptographic device used in this experiment is the side-channel standard evaluation boards (SASEBO) [71]. The SASEBO-G is equipped with two FPGAs, namely FPGA1 and FPGA2. One is for operating AES encryption processes and the other for controlling the encryption operation. FPGA1 in the Virtex-II Pro (xc2vp7), Xilinx is used for encryption, and FPGA2 in the Virtex-II Pro (xc2vp30), Xilinx used for communication and controlled the encryption/decryption operation. Fig. 4.8 shows the appearance of SASEBO-G. The two FPGAs have independent dedicated GND and Vcc wiring and are designed so that each power consumption does not influence as much as possible.

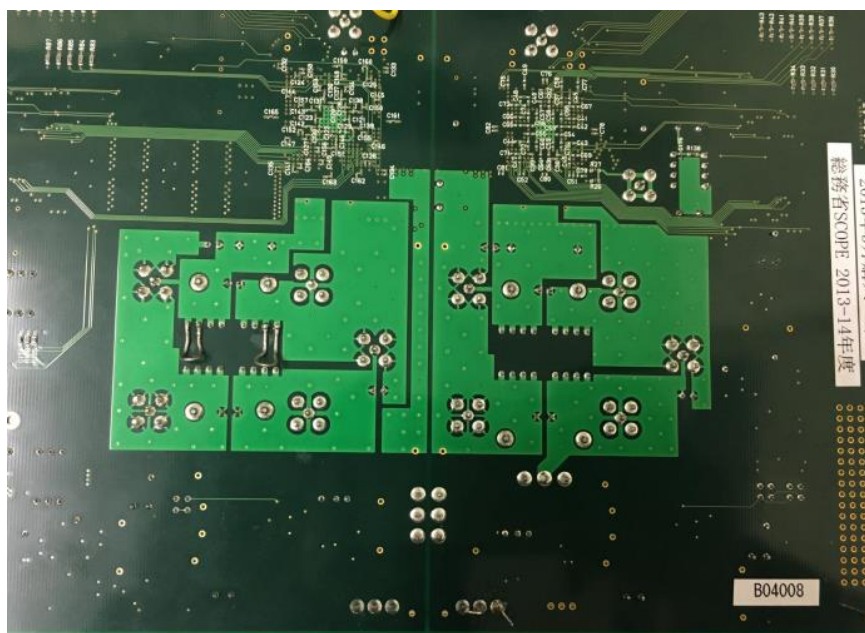
As shown in Fig. 4.8(b), though several capacitors are usually mounted on the backside of the encryption FPGA, in this experiment, they are unmounted for accurate measurement. In this experiment, we mounted capacitor at the discontinuity point on PDN to get an efficient countermeasure against information leakage. A composite-based AES-128 circuit is implemented on the encryption FPGA as an encryption circuit. This AES circuit was generated from Verilog-HDL files written at RTL level by a logic synthesis tool (Xilinx, ISE 10.1). For measuring side-channel traces accurately, the encryption FPGA has no function other than the AES. Besides, this circuit operates with a clock of 24 MHz, and needs 3.3 V of power supply.

It is also observed from Fig. 4.8(a) that between the cryptographic FPGA and the voltage regulator module (VRM), only a common capacitor C_2 is permanently mounted as a decoupling capacitor, and another capacitor, C_3 is mounted on the single pair of pads close to the cryptographic FPGA as shown in Fig. 4.8(a). Between the VRM and the measurement point, an electrolytic capacitor, C_1 is also mounted. We also mount an additional capacitor, C_x at the discontinuity point between the power trace and ground layer of the board, on PDN and 20 mm far from the discontinuity point on the board. We mount the capacitor on the soldering layer as shown in Fig. 4.8(b). In this study, 2012 sized chip capacitor of $0.01 \mu\text{F}$ as described previously, is used as the decoupling capacitor C_3 close to the FPGA, and as the additional capacitor C_x at the discontinuity point and 20 mm far from the discontinuity point.

Fig. 4.9 shows the layer structure of the SASEBO-G board. Fig. 4.9 (a) represent the layer structure and Fig. 4.9 (b) shown the side view. As shown in Fig. 4.9 (b), SASEBO-G



(a)



(b)

Figure 4.8 SASEBO-G board. (a) top layer (b) soldering layer.

consists of 8 layers, the 2nd layer is the GND layer, and the 5th to 7th layers are the power supply layers. It is observed from this figure that FPGA is connected with VRM through layer 5. The power connector on the board connects with the VRM through layer 7 and

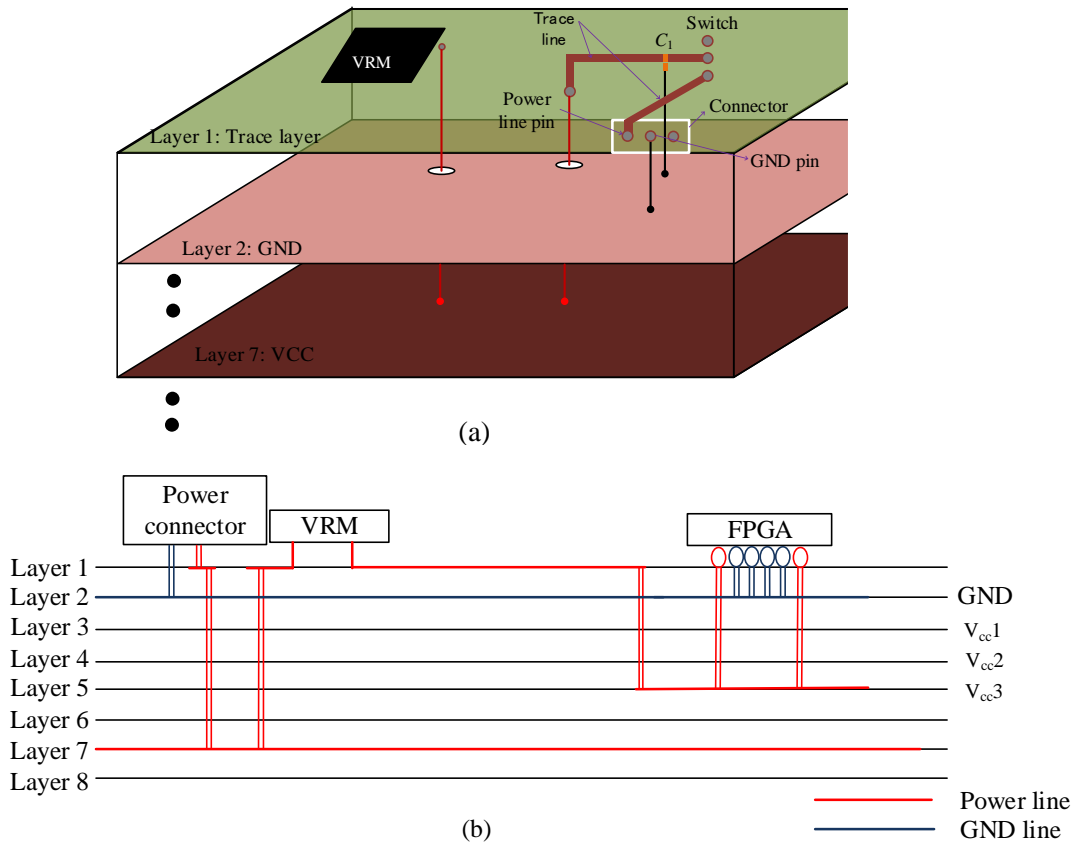


Figure 4.9 Layers of SASEBO-G board. (a) Layer view (b) Side view.

GND layer through layer 2 as shown in Fig. 4.9 (b).

4.4.2 Target Encryption Algorithm and Correlation Power Analysis (CPA)

The advanced encryption standard (AES) is used in this experiment as the targeted encryption algorithm. AES [72]. AES is a block cipher with a block length of 128 bits, and the key lengths are 128 bits and 192 bits. The number of rounds of encryption operation depends on the key length, and the larger the number of rounds, the higher the security. We choose AES-128 with a key length of 128 bits to focus only on it. AES-128 is encrypted in 10 rounds of processing as shown in Fig. 4.10. AES first takes an exclusive logical sum of the input data with the round key and initializes it before the encryption operation start. When the clock is input, the encryption process for one round is performed by the Round operation. In addition, the next clock input is the previous one. The 10 rounds AES-128 encryption process operation takes 10 clock cycles for the 10 cryptographic rounds and another additional clock cycle for data input/output. When the processing of the 10th round is completed, and the value is the final cipher.

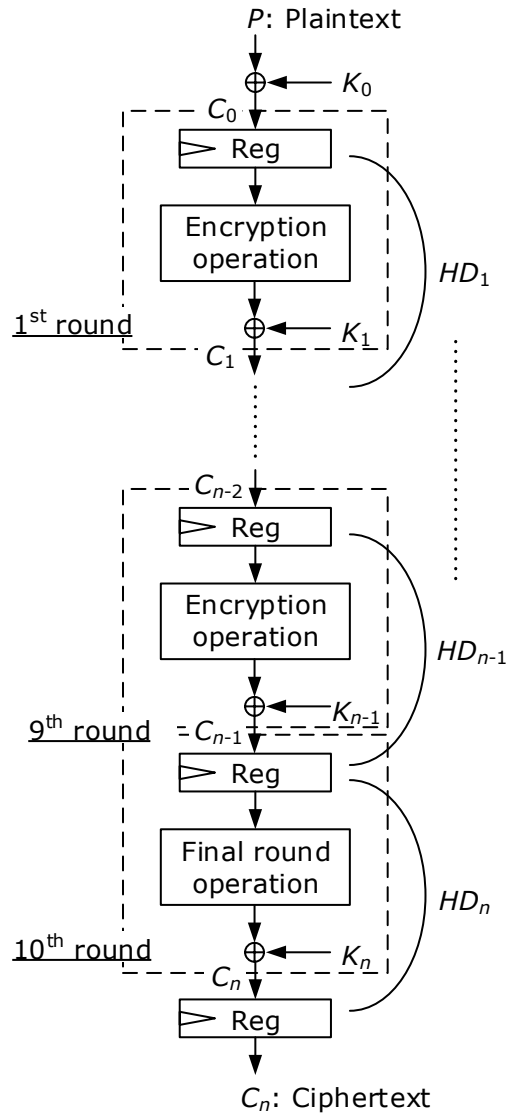


Figure 4.10 Flow of AES operation.

Side-channel analysis reveals the secret key information of the AES cryptographic algorithm implemented on the cryptographic device by focusing on the final round. The secret key information is carried outside the module via common-mode current generated due to mode conversion at the discontinuity point on the cryptographic module. Attackers observe the waveform of the common-mode current and analyze their variation in magnitude with changes in data values manipulated to obtain secret information. Attackers perform power analysis on the side-channel information with HD power model. There are many side-channel analyses method have been developed [5, 28, 74, 75]. The timing analysis [73], simple power analysis, and differential power analysis (DPA) [25] method are well known to researchers. In this experiment, we focus on the correlation power anal-

ysis (CPA) [24] method for the advanced encryption standard (AES). Another attacking method attracting the interest of many researchers is called the fault injection [76] where an excessive electrical or optical impulse is injected into the cryptographic device to cause a malfunction as does in direct power injection method [77]. However, this active method is not discussed in this experiment.

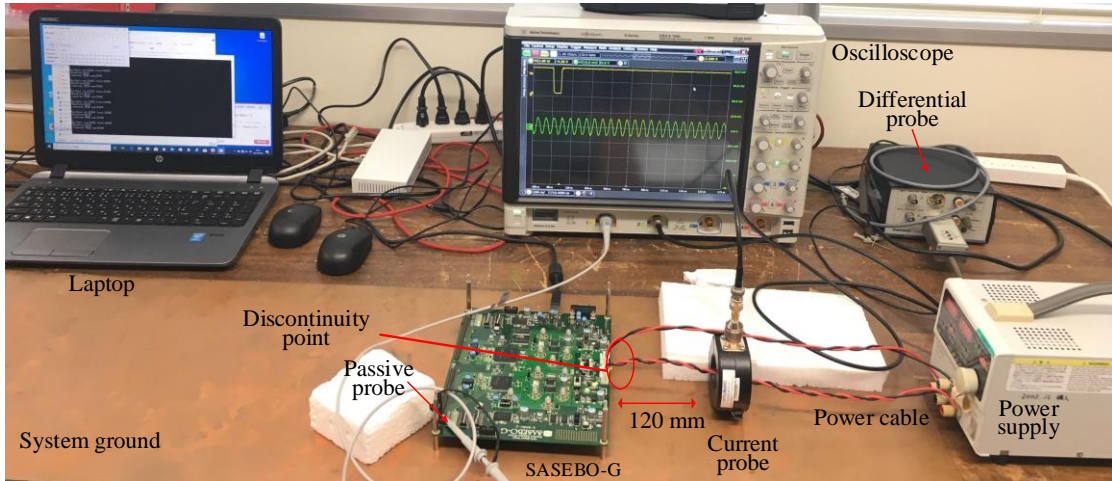


Figure 4.11 Measurement Setup.

4.4.3 Experimental Setup and Measurement Condition

Fig. 4.11 shows the measurement setup that consists of the SASEBO, a digital oscilloscope (DSO-S 104A, Keysight Technologies), DC power supply (PW16-5ADP), current probe (ETS-Lindgren/94111-1L), differential probe (P6330, Tektronix) and a laptop. In addition, for accurate measurement of the normal-mode voltage at the discontinuity point and common-mode current on the power cable, the result was taken as the average of 10 measurements. A passive probe (1161A, Agilent Technologies) was used for trigger acquisition. A laptop computer was used for controlling SASEBO-G operation and the oscilloscope. Table 4.3 summarized the common parameters for measuring the waveform of normal-mode voltage, V_n and common-mode current, I_c . The measurement equipment and measurement conditions for this experiment are also summarized in Table 4.4. The SASEBO-G with AES cryptographic algorithm is used in this experiment as the targeted cryptographic module is described in the previous section. In this experiment, the AES algorithm was processed in the cryptographic FPGA with a 128-bit key of (2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C)16.

For CPA and MTD evaluation, we used a random set of plaintext, in which all bits were changed randomly, and obtained 25000 traces. For the power model, an Hamming Distance (HD) set between the 9th and 10th rounds with respect to the secret key was used. The CPA result for the common-mode current on the power cable was obtained

around the 10th round of AES as the targeted round.

Table 4.3 Common parameters for the measurement of the waveform of V_n and I_c .

Item	Parameter
Plaintext	Random (25,000)
Encryption algorithm	AES-128
Target round	Final (10th) round
Secret key	2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C
Power model	Hamming distance (HD)
Analysis method	Correlation power analysis (CPA)
Averaging	10

Table 4.4 Measurement equipment and condition.

Oscilloscope	DSO-S 104A Keysight Technologies Sampling rate: 1.0 GSa/s Sample points: 10k
DC power supply	KENWOOD PW16-5ADP Supply voltage: 3.3 V Current limit: 0.2 A
Cryptographic devices FPGA Clock frequency	SASEBO-G Virtex-II Pro, xc2vp7 24 MHz
Probe for trigger signal	Passive probe 1161A Agilent Technologies
Probe for measurement normal-mode voltage	Differential probe P6330, Tektronix
Probe for measurement common-mode current	BCI current probe ETS-Lindgren, 94111-1L

In this experiment, clock frequency, and the supply voltage for SASEBO-G are obtained through the digital oscilloscope and dc power supply, respectively. The oscilloscope is mainly used to measure two types of time-domain waveforms: (i) normal-mode voltage at the connector, and (ii) common-mode current on an attached power cable.

Fig. 4.12 and Fig. 4.13 shows the block diagram for measuring the normal-mode voltage (V_n) and common-mode current (I_c), respectively. The labels “d” and “c” on Fig. 4.12 and Fig. 4.13 indicating the measurement point for V_n and I_c , respectively. It is observed from Fig. 4.13 that the common-mode current was detected by a current probe and recorded

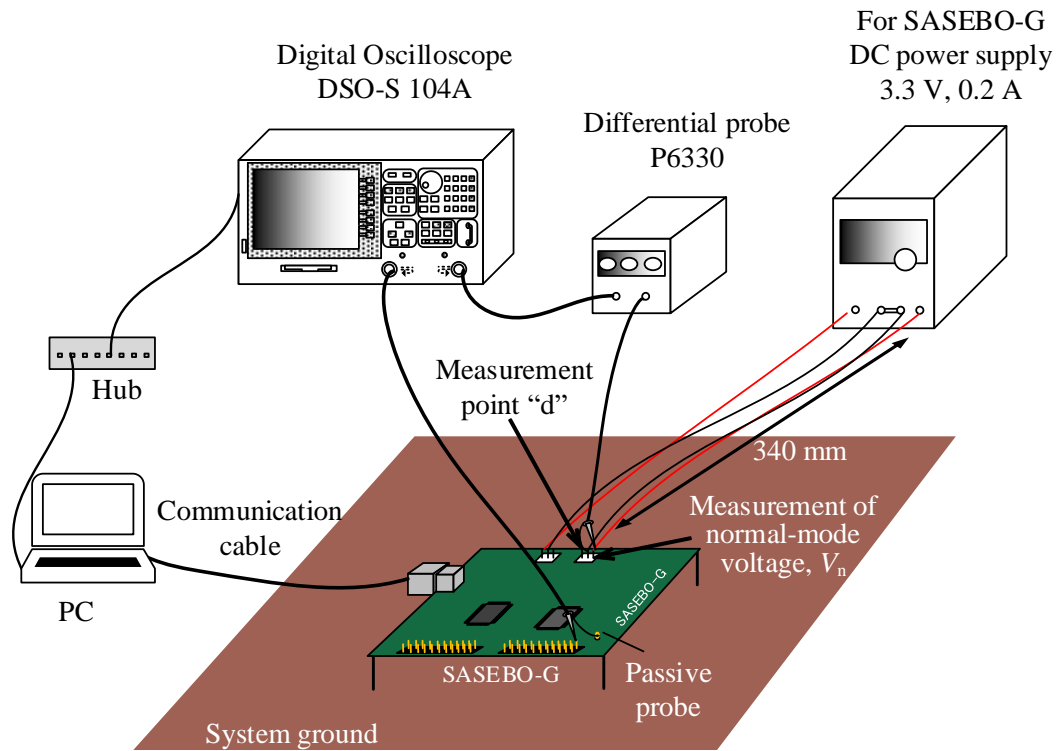


Figure 4.12 Measurement diagram for normal-mode voltage, V_n .

by the oscilloscope at sampling rate of 1.0 GSa/s and with a record length of 1 μ s. The probe was located 120 mm apart from SASEBO-G on the system ground as shown in this figure. For the normal mode voltage, the waveform of V_n is given by a voltage drop at the connector and is measured by using a differential probe and recorded by the oscilloscope in the same way as the common-mode current.

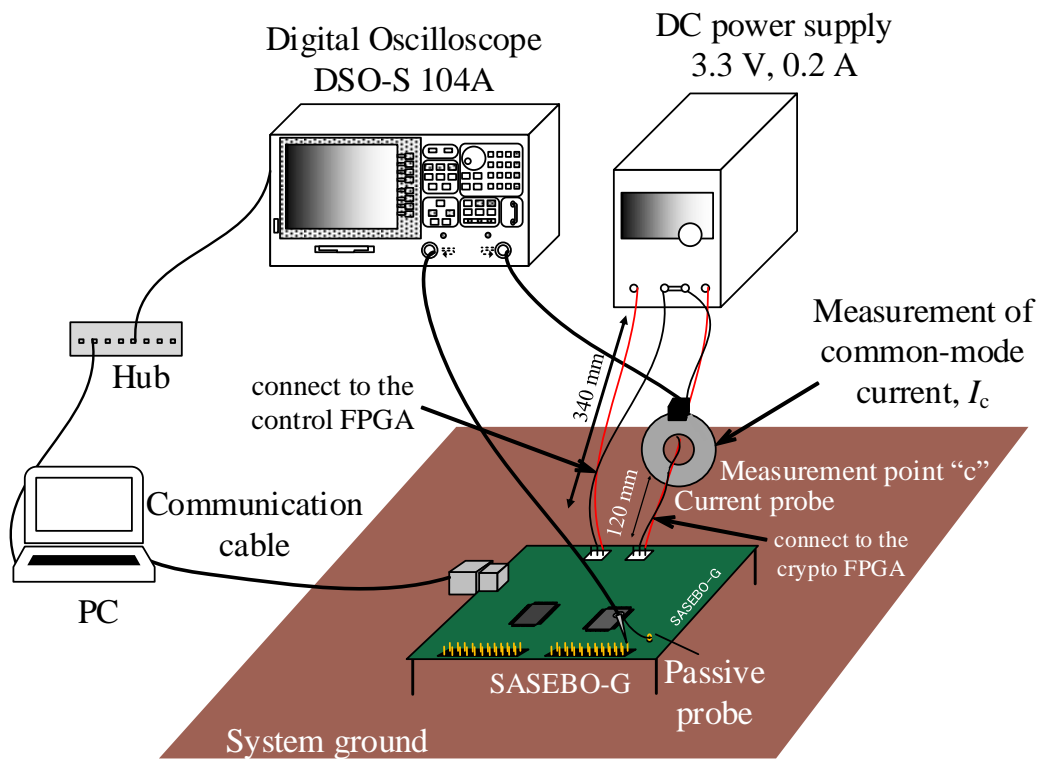


Figure 4.13 Measurement diagram for common-mode current, I_c .

4.5 Measurement Result

This section described the measurement results obtained from the evaluation system described in the previous section. At first, we measure the normal-mode voltage at the connector section and common-mode current on the power cable by using the differential probe and current probe, respectively. Then, we conduct power analysis on the acquired waveform of common-mode current to reveal the secret key. Finally, we compared 3 conditions as described in section 4.3, to evaluate the proposed countermeasure method described in Section 4.3.

4.5.1 Measurement of Normal-mode Voltage and Common-mode Current for different conditions

Fig. 4.14 shows the measured waveform of normal-mode voltage, V_n measured at the connector section between the power line and ground layer of the board for all conditions. The differential probe detected the normal-mode voltage. Similarly, Fig. 4.15 shows the output waveforms of the current probe attached to the power cable under the three conditions. The oscilloscope records both waveforms. The red, green, and blue spectra in Fig. 4.14 and Fig. 4.15 indicate the waveforms for the Reference and Conditions 2 and 1, respectively. The time origin corresponds to the start time of the encryption process.

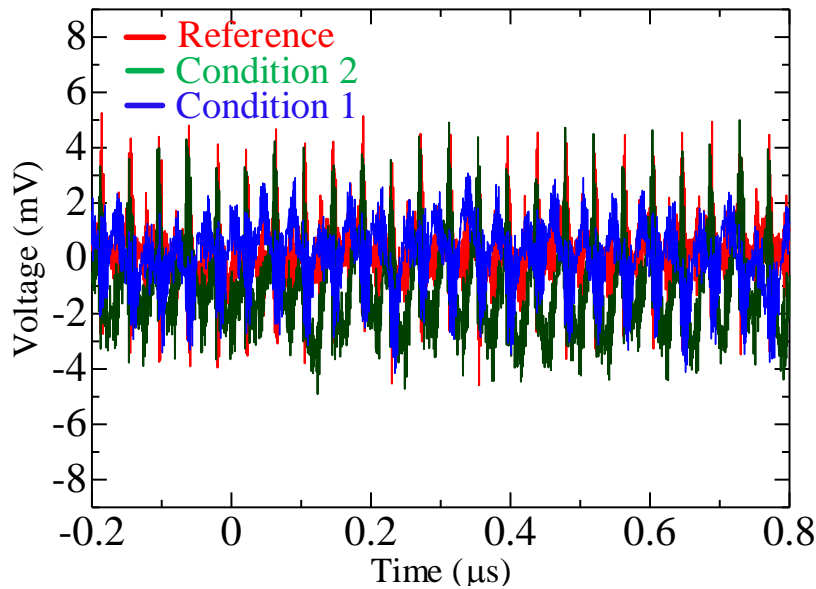


Figure 4.14 Measured Waveform of normal-mode voltage, V_n .

As shown in Fig. 7, the amplitude of V_n and I_c decreased most for Condition 1, confirming that Condition 1 results in less side-channel information leakage for the attacker to retrieve secret information and an enhancement of the SCA resistance of the

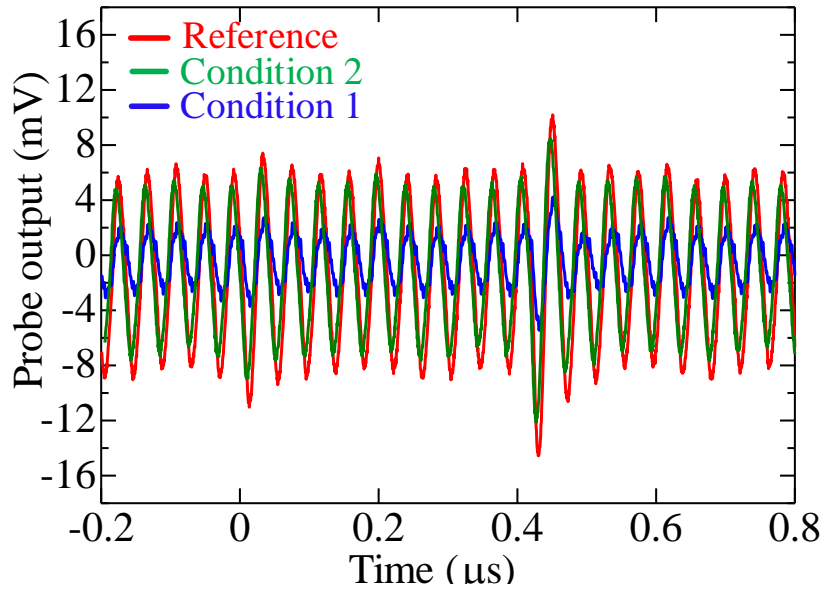


Figure 4.15 Probe output detect the measured waveform of common-mode current, I_c .

cryptographic module.

It is observed from Fig. 4.14 and Fig. 4.15 that the amplitude of normal-mode voltage and common-mode current is reduced for Condition 1, confirming that Condition 1 results in less side-channel information leakage for the attacker to retrieve secret information and an enhancement of the SCA resistance of the cryptographic module. Table 4.5 summarizes the measured normal-mode voltage, V_n and common-mode current, I_c around the 10th round. The percentages in parentheses are the reduction ratios of Conditions 1, and 2 relative to that of Reference (100%). It is found that the reduction ratios were almost the same for the common-mode current and the normal-mode voltage, and Condition 1 had the smallest reduction ratio of the three conditions. This suggests that C_x at the discontinuity point of the imbalance factor on a PDN can sufficiently reduce V_n and successfully suppress mode-conversion. As a result, the I_c flowing in the power cable also decreases, and this decrease can counter SCAs.

Table 4.5 Different measurement conditions.

	Reference	Condition 1	Condition 2
Normal-mode voltage V_n at “d” (mV)	4.8 (100 %)	1.5 (31 %)	3.1 (65 %)
Current probe output detecting I_c at “c” (mV)	11 (100 %)	3.8 (34 %)	8.7 (78 %)

4.5.2 CPA Result

Correlation Power Analysis (CPA) [24] which is one of the power major analysis method for block cipher like AES, is used for analysis the acquired waveform on common-mode current, I_c to reveal the secret information of the cryptographic module for each condition, targeting the final round of the AES-128 encryption. We use the waveform of common-mode currents flowing through the power cable as side-channel information. Also, for the comparison, we measured the waveform of common-mode currents for three different conditions as described in Section 4.3. In every condition, 25,000 waveforms were acquired and analyzed by CPA, targeting the final round of the AES-128 encryption.

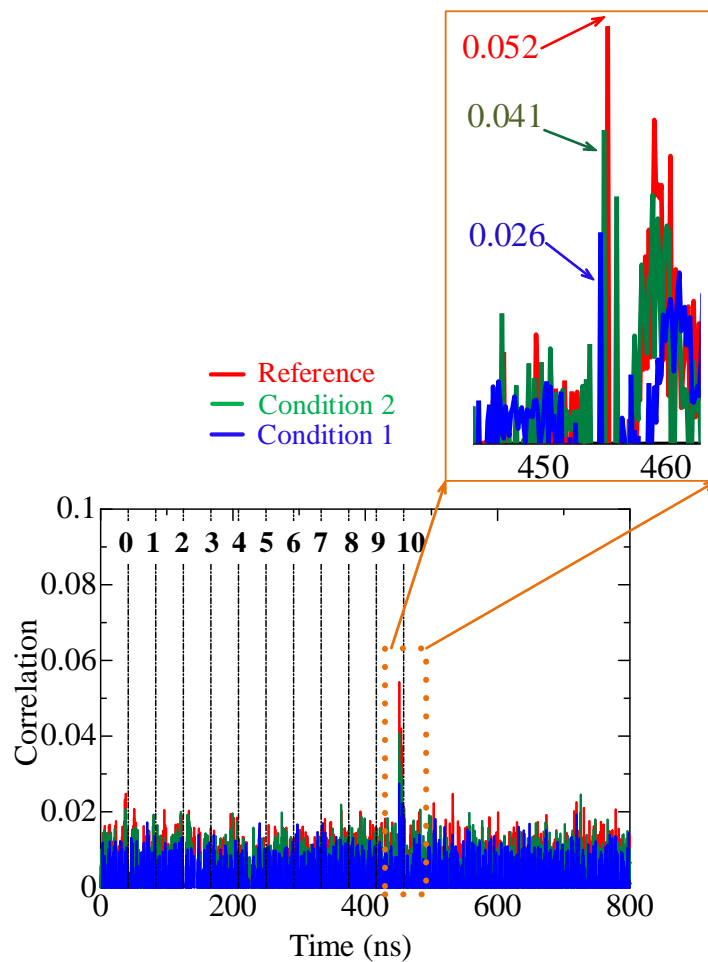


Figure 4.16 Correlation coefficient variation.

Fig. 4.16 shows the correlation coefficient variation obtained from the correlation between the common-mode current waveforms and the Hamming Distance (HD) power model based on the CPA method. The red, blue, and green lines on Fig. 4.16 and Fig. 4.17 indicate the measurement results for Reference and Conditions 1 and 2, respectively. The correlation peaks with the HD power model appears when the 10th round of AES operation finishes. As seen from Fig. 4.16, the peak correlation values are 0.052 for Reference,

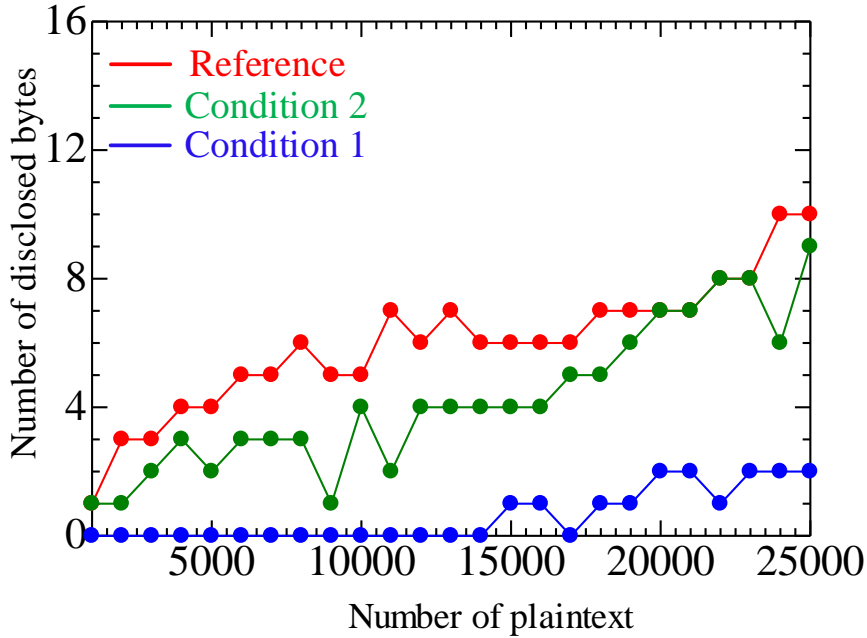


Figure 4.17 Number of disclosed bytes of secret key.

0.026 for Condition 1, and 0.041 for Condition 2. It is noticeable that the correlation for Condition 1 is minimum. It is experimentally confirmed that the filtering by mounting a capacitor on PDN is effective for counteracting SCA and mounting capacitor at the connector section is most effective for reducing common-mode current and the CPA value owing to suppressing mode conversion from normal mode to common mode.

Fig. 4.17 shows another result of CPA with respect to all the 256 key candidates for every byte (16 bytes) and indicates how many plaintexts are required to reveal secret-key byte. The horizontal axis is the number of plaintexts analyzed using the measured CM current waveforms. The vertical axis is the number of disclosed key bytes of the 10th round. It is observed in Fig. 4.17 that 10 bytes out of 16 bytes are disclosed in Reference, 9 bytes in Condition 2, and only 2 bytes in Condition 1 when analyzing all the 25,000 measured traces. This indicates that much more plaintexts are required to reveal secret-key byte by suppressing mode conversion with a capacitor placed at the connector section. Thereby, it is confirmed that the mode-conversion suppression technique improves the SCA resistance of the cryptographic module. Furthermore, the SCA resistance increases most by installing the capacitor at the discontinuity point.

4.6 Conclusion

We validated the mode-conversion suppression technique on power delivery network (PDN) to enhance the hardware security of cryptographic module because secret information leak via the common-mode current on the power cable. To reduce the common-mode current, we use the mode-conversion suppression technique on the basis of our modal-equivalent circuit model that assumes the common-mode electromotive force is proportional to the normal-mode voltage at the discontinuity point where the imbalance factor of the transmission line changes. Normal-mode voltage was reduced by placing a capacitor at the connector section on a PDN. As a result, the common-mode current decreased because of the mode-conversion suppression. Therefore, attackers have less side-channel information to reveal secret key information.

In addition, the waveforms of the common-mode current were analyzed by correlation power analysis (CPA), and it was demonstrated that CPA value and number of key bytes disclosed is decreased with decreasing the normal-mode voltage at the connector section. When information leakage occurs far from the cryptographic module via the common-mode current on the power cable, therefore, the impact of the mode-conversion suppression technique at the discontinuity point with respect to the imbalance factor is experimentally validated to enhance hardware security.

Therefore, the impact of the mode conversion suppression technique at the discontinuity point on the PDN is experimentally validated to enhance hardware security when information leakage occurs far from the cryptographic module via the common-mode current on the power cable.

Chapter 5

General Conclusion

This thesis aimed to solve the EMI issue in the signal transmission system, and enhance hardware security of the cryptographic module when information leaks via common-mode current in a power cable. The author achieved both goals by suppressing mode conversion at the interface where the cable connects with the PCB. In this thesis, the author focuses on the following two points to solve the EMI and security issues:

- (A) Mode conversion at the connector section due to imbalance difference between cable and connector section.
- (B) Secret information leakage outside the cryptographic module via the common-mode current in a power cable.

The main objective of this thesis is to achieve (A) and (B). Therefore, a concrete method was proposed for each point to realize (A) and (B).

In Chapter 2, the author explained the modal-equivalent circuit model for analysis mode conversion at the connector section that connects the cable with the PCB. The parameter, h , known as the imbalance factor, is used to explain the degree of imbalance of the transmission line, and it has an impact on mode conversion between two transmission lines. When two transmission lines with different imbalance factors are connected, mode conversion occurs at the interface. The modal-equivalent circuit model is constructed to evaluate mode conversion. The modal-equivalent circuit has the advantage of estimating mode conversion by inserting the current-controlled current source and voltage-controlled voltage source at the interface, which has the parameter of imbalance factor, h . The modal-equivalent circuit assumes that the mode conversion electromotive force is proportional to the product of the imbalance difference, Δh and the normal mode voltage, V_n . However, mode conversion can be suppressed by reducing Δh or V_n . Based on this concept, (A) is achieved in chapter 3 by reducing the value of imbalance difference, and (B) is achieved in chapter 4 by reducing the value of the normal-mode voltage.

Chapter 3 solved point (A) by suppressing mode conversion at the connector section based on imbalance matching between the cable section and the connector section. It

is observed that under balanced conditions, mode conversion between primary-common mode and secondary-common mode is dominant, and imbalance factor h_{3b} of the connector section depends on the structure of the shield that can be evaluated. We proposed an imbalance matching method at the connector section to suppress mode conversion by matching the imbalance factor of the connector section, h_{3b} with the imbalance factor of the cable section, h_{3a} . The inadequate shielding at the footprint of the female connector on the PCB surface and at the edge of both connectors causes mode conversion because of the difference in the imbalance factor between the connector section and the cable section. The footprint of the female connector on the PCB surface is improved by placing a copper layer below the female connector mounting area, and the edge of both connectors is improved by soldering and rapping with copper tape. As a result, the application of the improvement based on imbalance matching at the connector section makes the imbalance factor of the connector section closer to that of the cable section and results in the suppression of the mode conversion. It was observed from the measurement and simulation result obtained from the modal-equivalent circuit that mode conversion is suppressed by improving the footprint of the female connector on the PCB surface corresponds to Case 2. This reduction level is almost the same for the entire frequencies. Case 3 also validated the mode conversion suppression at the connector section based on imbalance matching. The experimental and estimated result also shows that the magnitude of the mode conversions between normal mode and primary-common mode, secondary-common mode is in deficient levels, and mode conversion between primary-common mode and secondary-common mode is at a high level. This result confirmed the balanced condition as mode conversion does not occur with normal mode. Under this condition, mode conversion only occurred between primary-common and secondary-common modes and achieved a good agreement with the simulation result. Therefore, the effect of the improvement based on imbalance matching at the connector section on mode-conversion suppression was experimentally and numerically validated to improve EMI issues.

Chapter 4 solved point (B) by reducing the common-mode current in a power cable that contains the secret information of the cryptographic module. The imbalance difference between the cable and the trace at the connector section on the power delivery network (PDN) gives the discontinuity of the imbalance factor. Common-mode current is generated due to mode conversion at the connector section on PDN. In order to enhance resistance against information leakage from outside the cryptographic module, it is essential to suppress mode conversion effectively. This chapter applies the mode conversion suppression technique at the connector section on PDN to enhance side-channel attack (SCA) resistance. Mode conversion is suppressed by reducing normal-mode voltage, V_n at the discontinuity point of PDN. A capacitor is mounted at the discontinuity point between the power trace and ground layer of the cryptographic module to filter high-frequency normal-mode noise. As a result, the normal mode voltage, V_n at the connector section is reduced and suppress mode conversion. Therefore, it reduces the common-mode current on the power cable and results in less side-channel information

for attackers to reveal the secret information. Waveforms of the common-mode current on the power cable were obtained under three conditions and analyzed with correlation power analysis (CPA). CPA results showed that correlation values were decreased when the capacitor was mounted at this discontinuity point. Therefore, the experimental result confirmed the improvement of the SCA resistance of the cryptographic module. The experimental result also shows that the number of secret key bytes disclosed decreases with the mode conversion suppression technique at the connector section. Hence, the mode conversion suppression technique at the discontinuity point on the PDN is expected to improve the SCA resistance of the cryptographic module effectively. Therefore, the impact of the mode conversion suppression technique was experimentally validated to enhance the hardware security when information leakage occurs far from the cryptographic module via the common-mode current in a power cable.

Appendix A

Mixed-mode S -parameter for 4-port Network

In this appendix, we investigate mode conversion for 4-port network. In Chapter 3, mode conversion was investigated by injecting outside noise through current probe. In this case, we observed the impact of imbalance matching method that proposed and validated in Chapter 3, without injecting noise. Next section explains the measurement setup for this experiment.

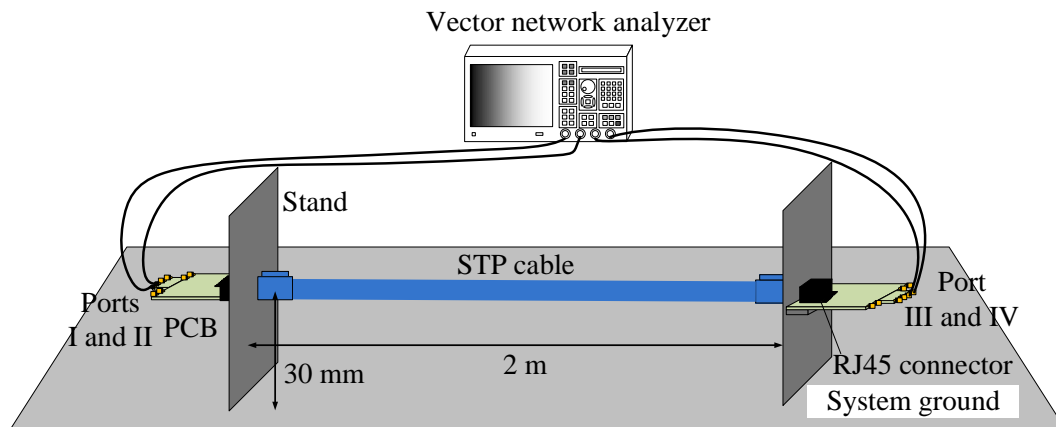


Figure A.1 Evaluation system for 4-port network.

Evaluation System

Fig. A.1 shows the evaluation system for 4-port network that is almost same as Fig. 3.12 shown in Chapter 3 except the use of current probe. It is observed that the STP cable is connected to the male connector that connect with the female connector mounted on the PCB. The measurement setup and condition for the measurement of mixed-mode S -parameter is same as described in Chapter 3, only change in the port definition. In

this case, port 3 and port 4 is connected to end of the differential transmission line on the right side PCB instead of connect them to current probe, as describe in Chapter 3. Next section explained the measurement result obtained from this evaluation system.

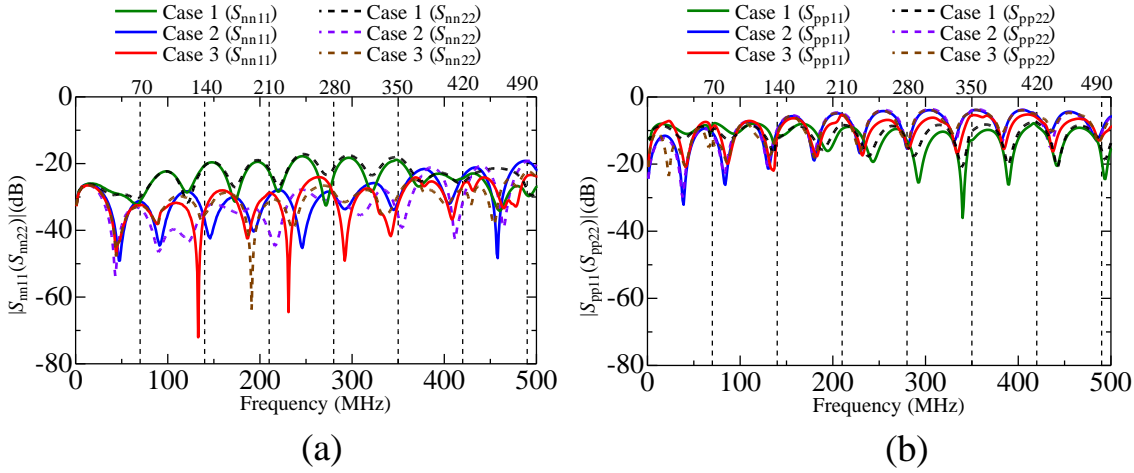


Figure A.2 Reflection characteristics of (a) Normal-mode and (b) Primary-common mode

Measurement Result

Fig. A.2 to Fig. A.5 shows the measurement result of mixed-mode S -parameter for 3 different cases as described in section 3.3. Measurement results are obtained from the measurement system shown in Fig. A.1. It is observed that the reflection characteristics and transmission characteristics of both ports in each mode are almost the same because of the symmetrical system. The vertical dashed line indicates the frequency to be $1/2$ wavelength resonance in the secondary-common mode.

It is observed from this figure that Case 1, Case 2 and Case 3 gives almost the same mode conversion amount.

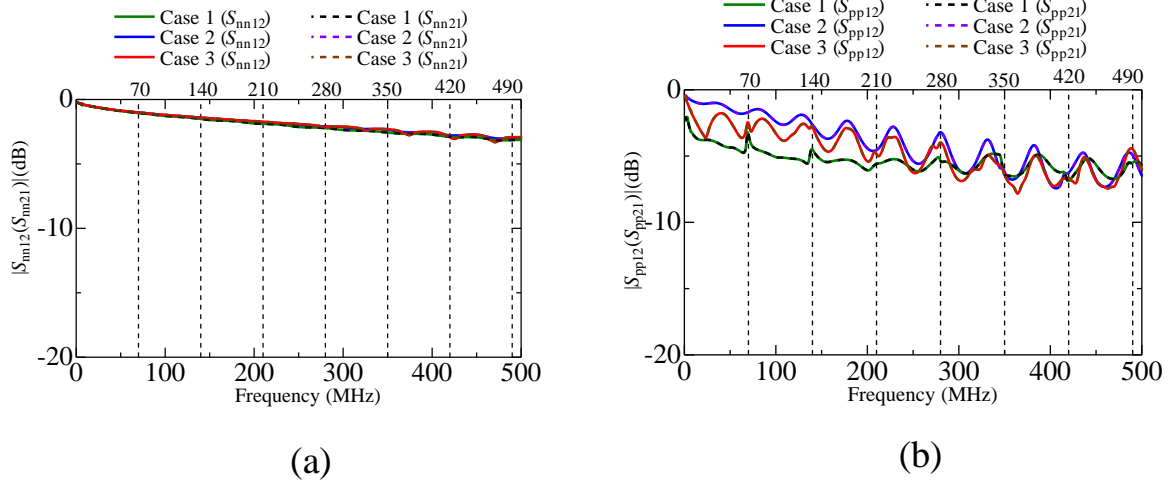


Figure A.3 Transmission characteristics of (a) Normal-mode and (b) Primary-common mode.

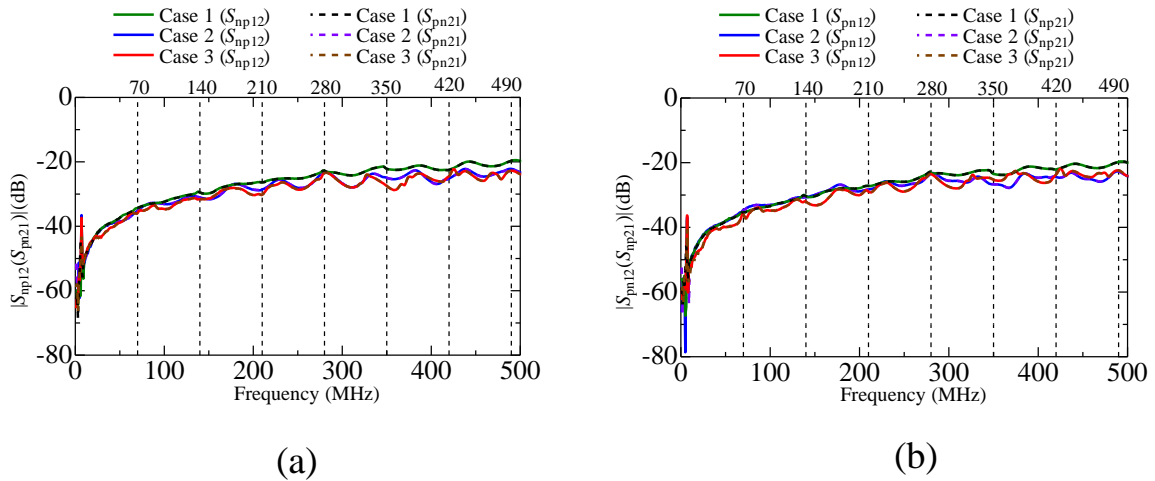


Figure A.4 Transmission characteristics of mode conversion between normal-mode and primary-common mode.

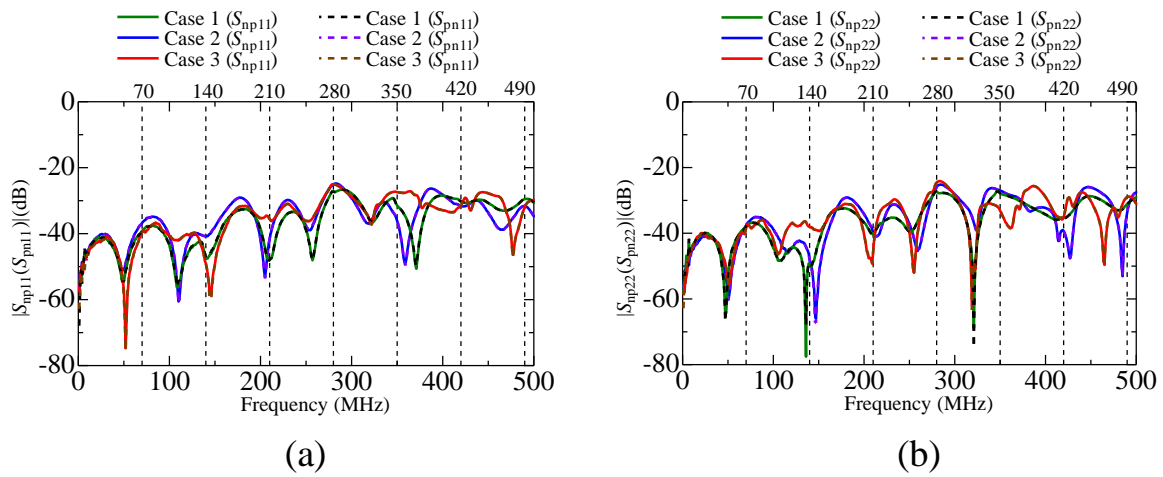


Figure A.5 Reflection characteristics of mode conversion between normal-mode and primary-common mode.

Appendix B

Mixed-mode S -parameter for Imperfect Transmission Line

In this appendix, we investigate the mode conversion for imperfect transmission line. In Chapter 3, mode conversion was investigated for perfect transmission line where both transmission lines had the same conductor definition. We observed that mode conversion was suppressed by matching imbalance factor at the interface point of a 4-conductor transmission system.

Table B.1 Different Combinations.

Transmission Line	Conditions	Cable	Connector	
			Male	Female
Imperfect transmission line	Combinations 1	STP	Shielded	Unshielded
	Combinations 2	UTP	Unshielded	Shielded
Perfect transmission line	Combinations 3	STP	Shielded	Shielded
	Combinations 4	UTP	Unshielded	Unshielded

We divided the transmission line based on the conductor definition as:

Perfect transmission line

Both transmission lines have the same conductor definition as observed in Chapter 3. Therefore, cable and connector section have the same conductor definition. In this experiment we used 4-conductor that corresponds to Combination 3, and 3-conductor transmission line that corresponds to Combination 3, as shown in Table B.1. In Combination 3, one transmission line is STP cable and another one is shielded connector. On the other hand, in Combination 4, one transmission line is UTP cable and another one is unshielded connector.

Imperfect transmission line

In imperfect transmission line, one transmission line is 3-conductor and other transmission line is 4-conductor. It is observed from Table B.1 that in Combination 1, one transmission line is STP cable and another one is unshielded connector. And in Combination 2, one transmission line is UTP cable and another one is shielded connector. In this experiment, we Investigate Combination 1. Next section explains the evaluation system.

Evaluation System

Fig. B.1 shows the evaluation system for Combination 1. It is observed that the STP cable is connected to the shielded male connector that connect with the unshielded female connector mounted on the PCB. The measurement setup and condition is same as described in Chapter 3, only change in the conductor definition. Next section explained the measurement result obtained from this evaluation system.

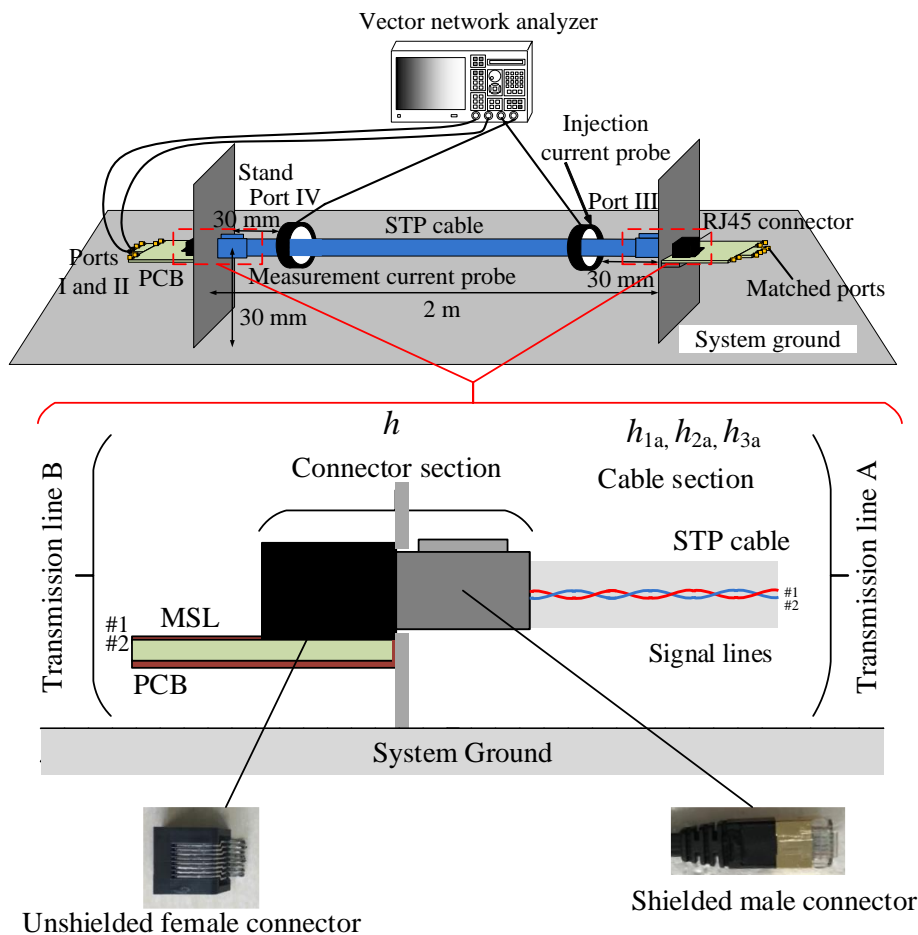


Figure B.1 Evaluation system for imperfect transmission line (Combination 1).

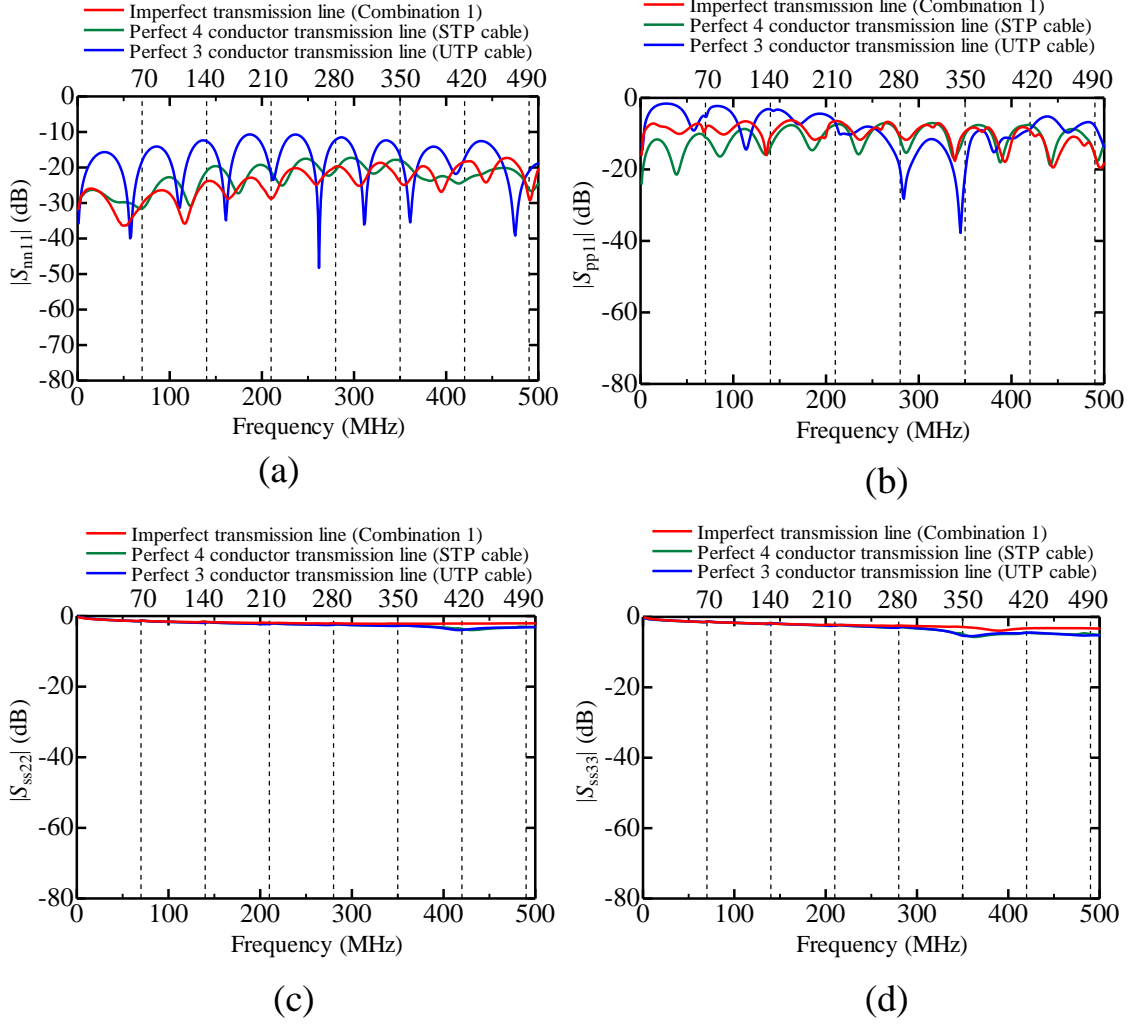


Figure B.2 Measured spectra of (a) S_{nm11} , indicates the reflection characteristics of normal-mode at Logical port 1, (b) S_{pp11} , indicates the reflection characteristics of primary-common mode at Logical port 1, (c) S_{ss22} , indicates the reflection characteristics of secondary-common mode at Logical port 2, and (d) S_{ss33} , indicates the reflection characteristics of secondary-common mode at Logical port 3.

Measurement Result

Fig. B.2 shows the spectra of mixed-mode S -parameter for reflection characteristics of each mode. Fig. B.2(a) indicate the reflection characteristics, S_{nm11} , of normal mode for Logical port 1, Fig. B.2(b) indicate the reflection characteristics, S_{pp11} , of primary-common mode for Logical port 1, Fig. B.2(c) indicate the reflection characteristics, S_{ss22} , of secondary-common mode for Logical port 2, and Fig. B.2(d) indicate the reflection characteristics, S_{ss33} , of secondary-common mode for Logical port 3.

It is observed from Fig. B.2(a) that the spectra of perfect and imperfect transmission

line are not same. Although, the measurement result of 4-conductor transmission line and imperfect transmission line are very close than the result of 3-conductor transmission line. Fig. B.2(b) showed that the measurement result of 4-conductor transmission line and imperfect transmission line are almost same.

Fig. B.2(c) and Fig. B.2(d) showed almost same spectra for perfect and imperfect transmission line.

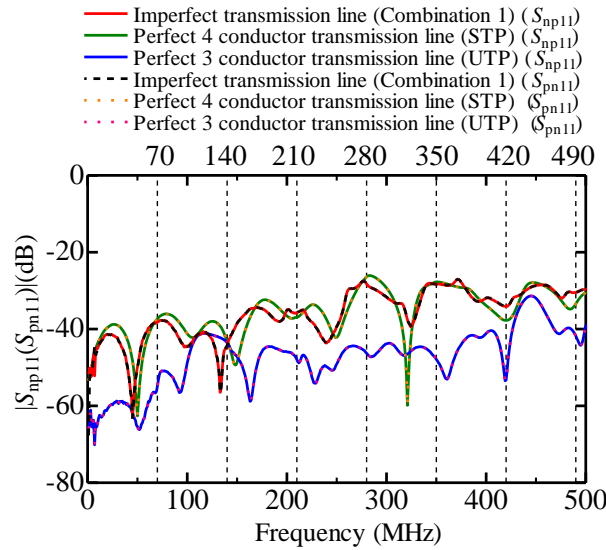


Figure B.3 Measured spectra of S_{np11} (S_{pn11}), indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and primary-common mode at Logical port 1.

Fig. B.3, Fig. B.4, Fig. B.5 and Fig. B.6 shows the spectra of mixed-mode S -parameter for transmission characteristics of each mode. Fig. B.3 shows the spectra of S_{np11} (S_{pn11}) indicates the mode conversion between normal mode and primary-common mode. It is observed from this figure that mode conversion amount between the normal-mode and primary-common mode is about -40 dB, for 4-conductor transmission line and imperfect transmission line, and is about -40 dB, for 3-conductor transmission line.

Fig. B.4(a) and Fig. B.4(b) shows the spectra of S_{ns12} (S_{sn21}) and S_{ns13} (S_{sn31}), respectively, indicating the mode conversion between normal mode and secondary-common mode. It is also observed that the mode conversion amount is at a deficient level close to the noise floor of the vector network analyzer, and it can be said that the mode conversion does not occur with normal mode. Therefore, it is confirmed from Fig. B.3, Fig. B.4(a) and Fig. B.4(b) that mode conversion does not occur with normal mode as we explained it in chapter 2.

Fig. B.5 shows the mode conversion between primary-common mode and secondary-common mode. Fig. B.5 (a) and Fig. B.5 (b) shows the spectra of S_{ps12} (S_{sp21}) and S_{ps13} (S_{sp31}), respectively, indicates the mode conversion between primary-common mode

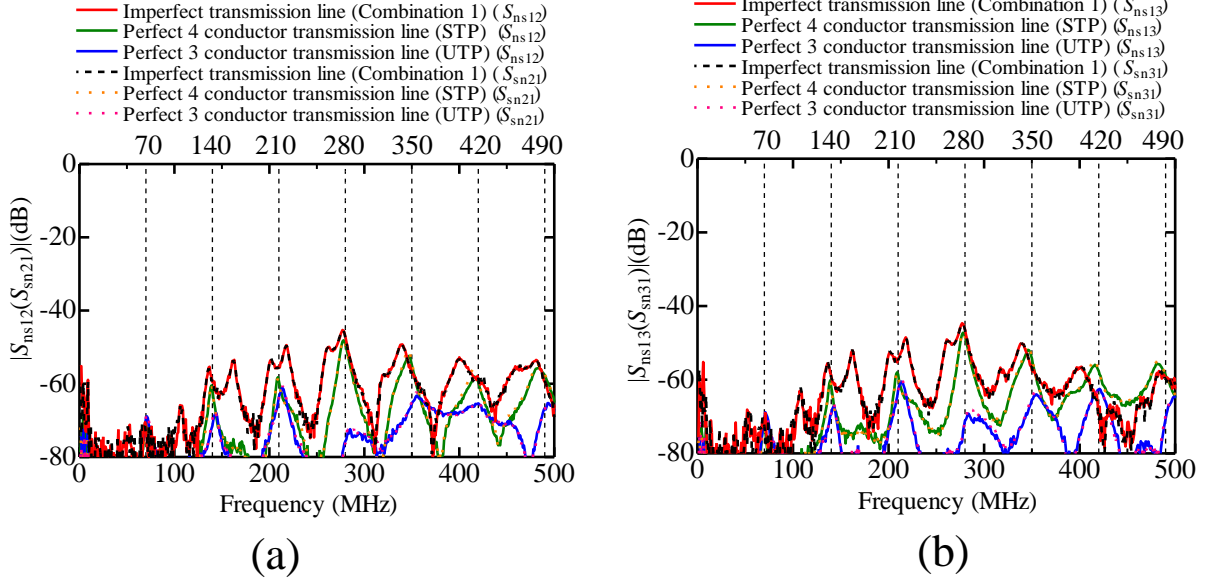


Figure B.4 Measured spectra of (a) $S_{ns12}(S_{sn21})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ns13}(S_{sn31})$, indicates the transmission characteristics of mode conversion between normal-mode at Logical port 1 and secondary-common mode at Logical port 3.

and secondary-common mode. It is observed from Fig. B.5 (a) that the spectra of the measurement result for the imperfect transmission line is almost same as perfect (3-conductor) transmission line up to 140 MHz. At 210MHz and 280 MHz, measurement result of imperfect transmission line lies between perfect (4-conductor) and perfect (3-conductor) transmission line. At 350 MHz and 420 MHz, measurement result of imperfect transmission line is almost same as perfect (4-conductor) transmission line. At high frequency, measurement result of imperfect transmission line shows better reduction of mode conversion than perfect (4-conductor) and perfect (3-conductor) transmission line. We do not know the reason for this phenomena. We need to investigate more to find the solution.

And finally, Fig. B.6 shows the spectra of $S_{ss23}(S_{ss32})$ indicates the mode conversion between secondary-common mode of Logical port 2 and secondary-common mode of Logical port 3. It is noticeable that the perfect transmission line (3-conductor and 4-conductor) shows almost the mode conversion amount. Moreover, the dotted line in the figure indicates the reciprocal value of each mixed-mode S -parameter.

It is noticeable from Fig. B.3, Fig. B.4, Fig. B.5 and Fig. B.6 that the magnitude of mode conversion amount for mixed-mode S -parameter S_{np11} and S_{pn11} , S_{ns12} and S_{sn21} , S_{ns13} and S_{sn31} , S_{ps12} and S_{sp21} , and S_{ss23} and S_{ss32} are same that also confirmed the reciprocal properties of the mixed-mode S -parameter.

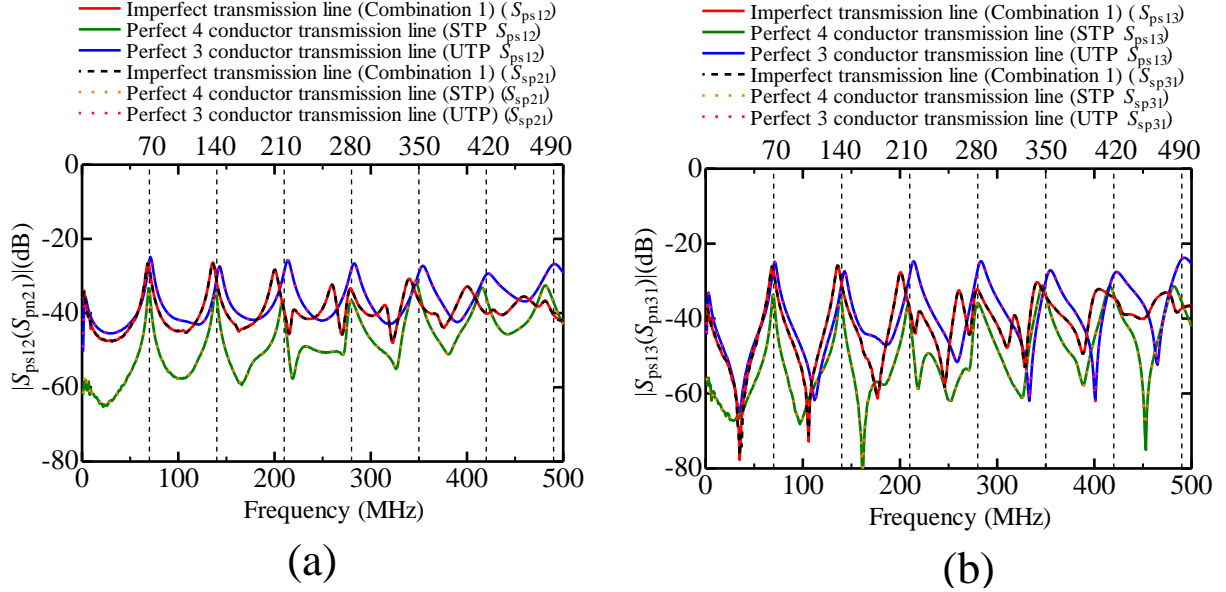


Figure B.5 Measured spectra of (a) $S_{ps12}(S_{sp21})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 2, and (b) $S_{ps13}(S_{sp31})$, indicates the transmission characteristics of mode conversion between primary-common mode Logical port 1 and secondary-common mode at Logical port 3.

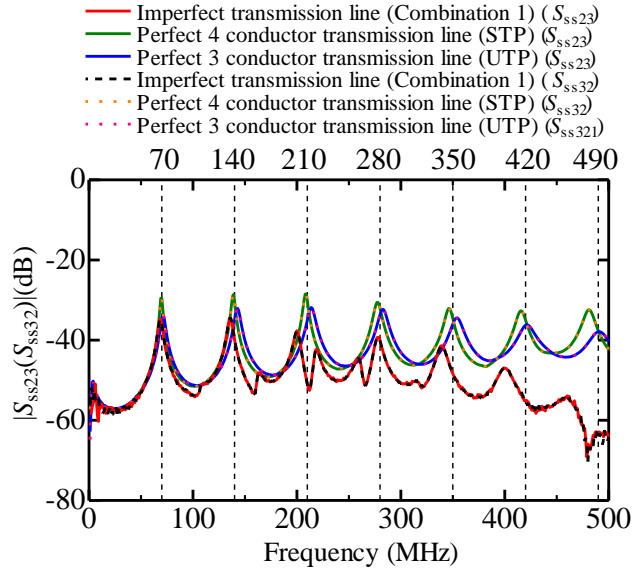


Figure B.6 Measured spectra of $S_{ss23}(S_{ss32})$ indicates the transmission characteristics of mode conversion between secondary-common mode at Logical port 2 and secondary-common mode at Logical port 3.

Bibliography

- [1] L. B. Gravelle and P. F. Wilson, "EMI/EMC in printed circuit boards-a literature review," *IEEE Trans. Electromagn. Compat.*, vol. 34, no. 2, pp. 109-116, May. 1992.
- [2] D. M. Hockanson, J. L. Drewniak, T. H. Hubing, T. P. Van Doren, F. Sha, and M. J. Wilhelm, "Investigation of fundamental EMI source mechanisms driving common-mode radiation from printed circuit boards with attached cables," *IEEE Trans. Electromagn. Compat.*, vol. 38, no. 4, pp. 557-566, Nov. 1996.
- [3] D. A. Hill, D. G. Camell, K. H. Cavcey, and G. H. Koepkel, "Radiated emissions and immunity of microstrip transmission lines: theory and reverberation chamber measurements," *IEEE Trans. Electromagn. Compat.*, vol. 38, no. 2, pp. 165-172, May. 1996.
- [4] C. R. Paul and D. R. Bush, "Radiated emission from common-mode currents," in *Proc. IEEE Int. Symp. Electromagnetic Compatibility*, Atlanta, GA, USA, pp. 197-203, Aug. 1987.
- [5] P. C. Kocher, J. M. Jaffe, and B. C. Jun, "Differential power analysis," in *Advances in Cryptology CRYPTO'99*, vol. 1666, pp. 388-397, Springer-Verlag, 1999.
- [6] Jvndb-2018-001001:, "Side channel attacks on cpu. [Online], Available: <https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-001001.html>. "
- [7] J. L. Drewniak, T. H. Hubing, and T. P. Van Doren, "Investigation of fundamental mechanisms of common-mode radiation from printed circuit boards with attached cables," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Chicago, IL, pp. 110-115, 1994.
- [8] D. M. Hockanson, J. L. Drewniak, T. H. Hubing and T. Van Doren, "Quantifying EMI resulting from finite-impedance reference planes," *IEEE Trans. Electromagn. Compat.*, vol. 39, no. 4, pp. 286-297, 1997.
- [9] J. L. Drewniak, F. Sha, T. H. Hubing, T. P. V. Doren, and J. Shaw, "Diagnosing and modeling common-mode radiation from printed circuit boards with attached cables," in *Proc. IEEE Int. Symp. Electromagn. Compat.*, Atlanta, GA, pp. 465-470, Aug. 1995.

- [10] F. B. J. Leferink and M. J. C. M. van Doorn, "Inductance of printed circuit board ground planes," in Proc. 1993 IEEE Int. Symp. Electromagn. Compat., Dallas, TX, pp. 327-329.
- [11] C. L. Holloway and E. F. Kuester, "Net and partial inductance of a microstrip ground plane," IEEE Trans. Electromagn. Compat., vol. 40, no. 1, pp. 33-46, Feb. 1998.
- [12] M. Leone, "Design expression for the trace-to-edge common-mode inductance of a printed circuit board," IEEE Trans. Electromagn. Compat., vol. 43, no. 4, pp. 667-671, Nov. 2001.
- [13] 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 Trans. Electromagn. Compat., vol. 47, no. 4, pp. 899-907, 2005.
- [14] 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," IEICE Trans. Commun., Vol. E83-B, No.3, pp. 593-599, 2000.
- [15] T. Watanabe, H. Fujihara, O. Wada, R. Koga, and Y. Kami, "A prediction method of common-mode excitation on a printed circuit board having a signal trace near the ground edge," IEICE Trans. Commun., Vol. E87-B, No.8, pp. 2327-2334, 2004.
- [16] T. Matsushima, T. Watanabe, Y. Toyota, R. Koga and O. Wada, "Increase of common-mode radiation due to guard trace voltage and determination of effective via-location," IEICE Trans. Commun., Vol. E92-B, No.6, pp. 1929-1936, 2009.
- [17] T. Matsushima, T. Watanabe, Y. Toyota, R. Koga and O. Wada "Evaluation of EMI reduction effect of guard traces based on imbalance difference method," IEICE Trans. Commun., Vol. E92-B, No.6, pp. 2193-2200, 2009.
- [18] Y. Toyota, K. Iokibe, R. Koga, and T. Watanabe, "Mode-equivalent modelling of system consisting of transmission lines with different imbalance factors," Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), pp.676-679, 2011.
- [19] K. Sejima, Y. Toyota, K. Iokibe, L. R. Koga, and T. Watanabe, "Experimental Model Validation of Mode-conversion Sources Introduced to Modal Equivalent Circuit," in Proc. 2012 IEEE Int. Symp. Electromagn. Compat., pp. 492-497, 2012.
- [20] F. Grassi, Y. Yang, X. Wu, G. Spadacini, and S. A. Pignari, "On mode conversion in geometrically unbalanced differential lines and its analogy with crosstalk," IEEE Trans. Electromagn. Compat., Vol.57, No.2, pp. 283-291, 2015.

- [21] F. Grassi, X. Wu, Y. Yang, G. Spadacini, and S. A. Pignari, "Modeling of imbalance in differential lines targeted to SPICE simulation," *Prog. Electromagn. Res. B*, Vol.62, pp. 225-239, 2015.
- [22] T. Nobunaga, Y. Toyota, K. Iokibe, L. R. Koga and T. Watanabe, "Evaluation of pigtail termination of STP cable using modal equivalent circuit of four-conductor transmission systems," 2013 International Symposium on Electromagnetic Theory, Hiroshima, pp. 222-225, 2013.
- [23] M. A. Islam, R. Irishika, K. Iokibe and Y. Toyota, "Suppression of Mode Conversion by Improved Shielding Effect of Ethernet Cable Connector Based on Imbalance Factor Matching," 2019 International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2), Rajshahi, Bangladesh, 2019.
- [24] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. Cryptographic Hardware and Embedded Systems*, pp. 16-29, 2004.
- [25] P.C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis, " " *Proc. CRYPTO*, LNCS, vol.1666, pp.388-397, Springer, 1999.
- [26] K. Iokibe, T. Amano and Y. Toyota, "On-board decoupling of cryptographic FPGA to improve tolerance to side-channel attacks, " 2011 IEEE Int. Symp. Electromagn. Compat., pp. 925-930, 2011. doi: 10.1109/ISEMC.2011.6038441.
- [27] Y. Hayashi, N. Homma, T. Mizuki, T. Sugawara, Y. Kayano, T. Aoki, S. Minegishi, A. Satoh, H. Sone and H. Inoue, "Evaluation of Information Leakage from Cryptographic Hardware via Common-Mode Current, " *IEICE Trans. on Electron.*, Vol. E95-C, No. 6, pp.1089-1097, 2012.
- [28] S. Mangard, E. Oswald, and T. Popp, "Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security), " Springer-Verlag New York, Secaucus, NJ, USA, 2007.
- [29] C.K. Koc, "Cryptographic Engineering, " Springer-Verlag New York, Secaucus, NJ, USA, 2009.
- [30] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, "The EM side-channel(s), " *CHES 2002, Lect. Notes Comput. Sci.*, vol.2523, pp.29-45, Aug. 2002.
- [31] K. Grandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results, " *CHES 2001, LNCS 2162*, pp.251-261, 2001.
- [32] O. Meynard, S. Guilley, J.-L. Danger, and L. Sauvage, "Far correlation-based EMA with a precharacterized leakage model, " *DATE 2010*, pp.1-6, March 2010.

- [33] T. Sugawara, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, and A. Satoh, "Spectrum analysis on cryptographic modules to counteract side-channel attacks," EMC '09, July 2009.
- [34] T. Plos, M. Hutter, and M. Feldhofer, "On comparing side-channel preprocessing techniques for attacking RFID devices," WISA 2009, Lect. Notes Comput. Sci., vol.5932, pp.163-177, 2009.
- [35] T. Amano, K. Iokibe and Y. Toyota, "Equivalent current source of side-channel signal for countermeasure design with analog circuit simulator," 2012 IEEE Int. Symp. Electromagn. Compat., pp. 806-811, 2012, doi: 10.1109/ISEMC.2012.6351661.
- [36] K. Iokibe, T. Amano, K. Okamoto, and Y. Toyota, "Equivalent Circuit Modeling of Cryptographic Integrated Circuit for Information Security Design," IEEE Trans. Electromagn. Compat., Vol. 55, No. 3, pp: 581-588, June 2013, doi: 10.1109/TEMC.2013.2250505
- [37] K. Iokibe, K. Maeshima, T. Watanabe and Y. Toyota, "Security simulation against side-channel attacks on Advanced Encryption Standard circuits based on equivalent circuit model," 2015 IEEE Int. Symp. Electromagn. Compat., pp. 224-229, 2015, doi: 10.1109/ISEMC.2015.7256163.
- [38] W. van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?," Computers & Security, vol.4, no.4, pp.269-286, 1985.
- [39] M.G. Kuhn, "Compromising emanations: Eavesdropping risks of computer displays," University of Cambridge Computer Laboratory, Technical Report, UCAM-CL-TR-577, 2003.
- [40] "C. R. Paul, Introduction to electromagnetic compatibility," New York: John Wiley & Sons, 1997.
- [41] Y. Hayashi, T. Sugawara, Y. Kayano, N. Homma, T. Mizuki, A. Satoh, T. Aoki, S. Minegishi, H. Sone, H. Inoue, "Information Leakage from Cryptographic Hardware via Common-Mode Current," In Proc. IEEE Symp. EMC, TUE-AM-4-3, pp. 109-114, Fort Lauderdale, USA, July 2010.
- [42] T.H. Hubing, "Printed circuit board EMI source mechanisms," In Proc. IEEE Symp. Electromagn. Compat., vol.1, pp.1-3, 2003.
- [43] Y. Kayano, M. Tanaka, and H. Inoue, "Identifying the frequency response of common-mode current on a cable attached to a pcb," IEICE Trans. Electron., vol.E87-C, no.8, pp.1268-1276, Aug. 2004.

- [44] T. Fischer, M. Leone, and M. Albach, "An analytical model for studying the electromagnetic radiation of power-bus structures," *IEEE Int. Symp. Electromagn. Compat.*, vol.221, pp.225-230, 2003.
- [45] Y. Kami, "Transmission-line circuit theory in EMC and its development," *IEICE Trans. Commun.*, vol.J-90B, no.11, pp.1070-1082, Nov. 2007 (in Japanese).
- [46] A. Sugiura, and Y. Kami, "Generation and propagation of common mode currents in a balanced two-conductor line," *IEEE Trans. Electromagn. Compat.* vol.54, no.2, pp. 466-473, Apr. 2012.
- [47] H. Uchidai, "Fundamentals of coupled lines and multi-wire antennas," Sasaki Print & Pub., Sendai, Japan, 1967.
- [48] C. R. Paul, "Analysis of Multiconductor Transmission Lines." New York: John Wiley & Sons, 1994.
- [49] Y. Toyota, T. Mikura and K. Iokibe, "Suppression of mode conversion by installing bypass capacitor to power distribution network," *IEEEJ Transactions on Fundamentals and Materials*, vol.136, Issues.1, pp.25-32, 2016 (in Japanese).
- [50] S. Baek, J. Kim and J. Kim, "Modeling and measurement of mode conversion and frequency dependent loss in high speed differential interconnection on multilayer PCB," *IEICE Trans. Electron.*, vol.E88-C, No.10, Oct. 2005.
- [51] H. Heck, S. Hall, B. Horine and T. Liang, "Modeling and mitigating AC common mode conversion in multi-Gb/s differential printed circuit boards," *Electrical Performance of electronic Packaging - 2004*, Portland, OR, USA, 2004, pp. 29-32, doi: 10.1109/EPEP.2004.1407536.
- [52] Y. Shimoshio, J. Drewniak, D. Pommerenke and T. Van Doren, "Analysis of differential to common mode conversion characteristics of connected two PCB boards," *International Symposium on EMC Sendai*, pp.25-28, June 2004.
- [53] R. Rimolo-Donadio, X. Duan, H. Bruns and C. Schuster, "Differential to common mode conversion due to asymmetric ground via configurations," *2009 IEEE Workshop on Signal Propagation on Interconnects*, Strasbourg, 2009, pp. 1-4, doi: 10.1109/SPI.2009.5089852.
- [54] A. Motohashi, F. Nakamoto, Y. Sasaki, N. Oka and H. Oh-Hashi, "A study on differential mode to common mode conversion due to asymmetric structure in differential transmission line," *IEEE CPMT Symposium Japan 2014*, Kyoto, 2014, pp. 47-50, doi: 10.1109/ICSJ.2014.7009606.

- [55] X. Wu, Y. Yang, F. Grassi, G. Spadacini, and S. A. Pignari, "Statistical characterization of line imbalance in differential lines," Proc. XXXIth General Assembly of International Union of Radio Science (URSI), Beijing, P. R. China, 2014.
- [56] F. Grassi, G. Spadacini, and S.A. Pignari, "The concept of weak imbalance and its role in the emissions and immunity of differential lines, "IEEE Trans. Electromagn. Compat., vol. 55, no. 6, pp. 1346-1349, Dec. 2013.
- [57] B. Li, D. Su, J. Wang and X. Song, "Common- and Differential-Mode Conversion Induced by Asymmetry and Dielectric Coating in a Transmission Line System," in IEEE Transactions on Electromagnetic Compatibility, vol. 59, no. 3, pp. 988-991, June 2017, doi: 10.1109/TEMPC.2016.2633360.
- [58] F. Grassi, L. Badini, G. Spadacini, and S. A. Pignari, "Crosstalk and mode conversion in adjacent differential lines," IEEE Trans. Electromagn. Compat., vol. 58, no. 3, pp. 877-886, Jun. 2016.
- [59] Y. Kayano, Y. Tsuda, and H. Inoue, "Identifying EM radiation from asymmetrical differential-paired lines with equi-distance routing," in Proc. IEEE Int. Symp. Electromagn. Compat., pp. 311-316, Aug. 2012.
- [60] L. Niu and T. H. Hubing, "Rigorous derivation of imbalance difference theory for modeling radiated emission problems," IEEE Trans. Electromagn. Compat., vol. 57, no. 5, pp. 1021-1026, Oct. 2015.
- [61] M. Liu, J. Wang and X. Wu, "Analysis of the radiation from a pigtail-terminated coaxial cable using the imbalance difference model," 2016 Progress in Electromagnetic Research Symposium (PIERS), Shanghai, pp. 2179-2183, i, 2016. doi: 10.1109/PIERS.2016.7734902.
- [62] F. Han, "Radiated emission from shielded cables by pigtail effect," IEEE Trans. Electromagn. Compat., vol. 34, no. 3, pp. 345-348, Aug. 1992, doi: 10.1109/15.155852.
- [63] F. Han, "Common mode radiation from shielded cables by pigtail effect," Fujikura Technical Journal, No. 114, pp. 32-34, 2010.
- [64] ISO/IEC 11801:2017, "Information technology -Generic cabling for customer premises," .
- [65] ISO/IEC 8877 :1992, "Information technology -Telecommunications and information exchange between systems - Interface connector and contact assignments for ISDN Basic Access Interface located at reference points S and T ,"
- [66] <https://ce8dc832c.cloudimg.io>
- [67] <https://jp.misumi-ec.com/vona2/detail/222005033557/>

- [68] <https://jp.rs-online.com/web/p/rj45-connectors/7871666/>
- [69] "IEEE Standard for Ethernet," in IEEE Std. 802.3-2018 (Revision of IEEE Std 802.3-2015) , vol., no., pp.1-5600, 31 Aug. 2018. doi: 10.1109/IEEESTD.2018.8457469.
- [70] W. R. Eisenstabt, B. Stengle, and B. M.Thompson, "Microwave Differential Circuit Design Using Mixed-mode S-parameter," Artech House Boston., pp.113-152, 2006.
- [71] Morita Tech and AIST, "Side-channel attack standard evaluation board (SASEBO)," [Online]. Available: <http://www.morita-tech.co.jp/SASEBO/en/>
- [72] "Advanced Encryption Standard (AES)," NIST FIPS publication 197, Nov. 2001.
- [73] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in Advances in Cryptology-CRYPTO, N. Koblitz, Ed., Springer-Verlag, pp. 104-113, 1996.
- [74] M. Joye, "Basics of side-channel analysis," in Cryptographic Engineering, New York, NY, USA: Springer-Verlag, no. 13, 2009.
- [75] P. Rohatgi, "Improved techniques for side-channel analysis," in Cryptographic Engineering, New York, NY, USA: Springer-Verlag, no. 14, 2009.
- [76] Y. Hayashi, N. Homma, T. Sugawara, T. Mizuki, T. Aoki, and H. Sone, "Non-invasive EMI-based fault injection attack against cryptographic modules," in Proc. IEEE Int. Symp. Electromagn. Compat., pp. 763-767, Aug. 2011.
- [77] IEC, "Integrated circuits - Measurement of electromagnetic immunity, 150 kHz to 1 GHz - Part 3: Bulk current injection (BCI) method," IEC 62132-3 ed1.0, Sep. 2007. Available: <http://webstore.iec.ch/webstore/webstore.nsf/Artnum-PK/38377>.

Research Activities

Paper

1. **Md. Ashraful Islam**, Kengo Iokibe, Yoshitaka Toyota, "Suppression of Mode Conversion at Ethernet Connector by Using Modal-Equivalent Circuit Model Based on Imbalance Matching," *IEEJ Transaction on Fundamentals and Materials (A)*, vol. 140, no. 12, pp.586-592, December 2020.

International Conferences

1. **Md. Ashraful Islam**, Ryota Irishika, Kengo Iokibe, Yoshitaka Toyota, "Suppression of Mode Conversion by Improving Shielding Around Ethernet Connector with Imbalance Matching," *2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)*, Sapporo, p. 786, Japan, Jun. 2019.
2. **Md. Ashraful Islam**, Ryota Irishika, Kengo Iokibe, Yoshitaka Toyota, "Suppression of Mode Conversion by Improved Shielding Effect of Ethernet Cable Connector Based on Imbalance Factor Matching," *Proceeding of 5th International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2-2019)*, Rajshahi, Bangladesh, July 2019.
3. **Md. Ashraful Islam**, Kengo Iokibe, Yoshitaka Toyota, "Suppression of Mode Conversion by Shielded Ethernet Connector and Improved PCB Pattern Based on Imbalance Matching," *2020 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2020)*, Sydney, Australia, May 2020.(Accepted)(Cancel due to world pandemic of COVID 2019).
4. **Md. Ashraful Islam**, Masaki Himuro, Kengo Iokibe, Yoshitaka Toyota, "Common-mode Current Reduction by Applying Mode-conversion Suppression Technique to Power Delivery Network as Side-channel Attack Countermeasure," *Submitted to 5th International Conference on Computer, Communication, Chemical, Materials and Electronic Engineering (IC4ME2-2021)*, Rajshahi, Bangladesh, December 2021.

Biography

Md. Ashrafur Islam was born in Chuadanga, Bangladesh, on January 1, 1984. received his B.Sc. and M.Sc. degrees from the Dept. of Information and Communication Engineering, University of Rajshahi, Rajshahi, Bangladesh, in 2006 and 2007. He is currently working toward a Ph.D. degree at the Dept. of Electrical and Communication Engineering, Okayama University, Okayama, Japan. His research interests include reduction of common-mode noise, EMI, and electromagnetic compatibility analysis. His current research topic is the mode analysis of a multi-conductor system by using a modal-equivalent circuit model based on imbalance matching.