A Study of Efficient Design and Evaluation Methodology of Electrical and Electronic Equipment for EMC and Hardware Security in IoT Era

March, 2019

Yusuke Yano

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

A Study of Efficient Design and Evaluation Methodology of Electrical and Electronic Equipment for EMC and Hardware Security in IoT Era

Copyright © 2019 by Yusuke Yano

All rights reserved.

Printed in Japan

Abstract

With the progress in internet of things (IoT), electromagnetic environment surrounding the electrical and electronic equipment becomes worse than ever because electromagnetic interference (EMI) caused by conducted or radiated electromagnetic noise becomes larger due to increase in the operating frequency and the power consumption of integrated circuits and power converter circuits. Along with the increase in EMI, EMI regulation levels of various electromagnetic compatibility (EMC) standards become stringent. Therefore, EMC design to control the EMI and improve noise immunity of equipment becomes increasingly important.

Besides, the risk of security attacks such as unauthorized access, communication data eavesdropping and tampering, and service interruption has increased. Especially, hardware security (HWS) attacks such as side-channel attacks (SCAs) are concerned because IoT products are used indoors and outdoors and are open and easy to access physically. SCA resistance criteria are regulated stringently by various organizations. Therefore, for equipment in IoT era, not only the EMC design but also HWS design to increase HWS attack resistance are important.

In addition, since the progress in IoT is growing rapidly, efficient EMC and HWS design is required simultaneously for adapting to the increase in production speed of IoT equipment. Generally, a product development process is driven in the order below: specification development, system and functional design, hardware and software design, trial production, and performance evaluation. However, it is rare to finish these processes at once. Actually, the performance at first evaluation often does unsatisfy the required performance, workers will often do over again from the hardware and software design process. Since this rework causes delay in product development, a repetition of the rework should be avoided.

To prevent the repetition and to design efficiently, works which required an enormous amount of man-hours and costs (i.e. the trial production and the performance evaluation) should be omitted. To improve the efficiency in product development, it is necessary two things:

(A) predicting the product performance in the design process without going through the complete trial manufacture and performance evaluation process, and

(B) optimizing the product design without trial and error.

Solving these issues, (A) and (B), with computer-aided engineering (CAE) is a current trend. CAE tools are very powerful because they can reduce trial cost in product performance prediction and design optimization, but reflecting the characteristics of the entire product to the CAE tools is unrealistic in terms of calculation cost. Therefore, a simulation method of efficient EMC and HWS performance prediction is required to reduce the calculation cost. For the efficient simulation, it is important to construct high-speed analyzable models and to narrow down the analysis dimension and range. It is preferable that the number of man-hours for constructing the model is as small as possible, and ease of model building is important. In addition, since the performance of the model depends on the condition at the time of model construction, it is necessary to properly determine the condition. Besides, even if the CAE tool is used, it is difficult to optimize a component of product composed of plural elements. If plural elements can not be simultaneously optimized, the design and simulation processes are repeated. Therefore, an optimal design method is also required. To optimize the plural elements, it is important to derive a function having the elements as a variable with respect to a criterion representing a target performance, and calculate the set of elements that satisfy the target. In deriving the function, it is practically impossible to use all the constituent elements as variables, so it is necessary to simplify the constituent elements. Since the accuracy of optimization and the application limit of optimum design depend on the simplification, appropriate simplification is important.

The objective of this thesis is establishing efficient EMC and HWS design methods realizing (A) and (B). As concrete methods to realize (A) and (B), three studies were investigated as follows:

- noise-source equivalent circuit modeling to predict conducted disturbance for realizing (A) in EMC design,
- a study of SCA resistance estimation for realizing (A) in HWS design, and
- an optimal design method of snubber circuits (a kind of filters for suppressing EMI or information leakage) for realizing (B).

The abstracts of each study are described below.

Chapter 2 described a noise-source equivalent circuit model and a model identification method for realizing (A). A simple measurement system consisting of a data logger (or an oscilloscope) and general measurement probes was used to reduce the difficulty of model construction. In addition, as an appropriate condition of model construction, the model structure, the measurement method, and the measurement accuracy were examined. As a result, it was possible to estimate conduction disturbance with an error within 6 dB which can be said to be practically sufficient accuracy.

Chapter 3 described a study of a SCA resistance estimation for realizing (A). We examined two methods: a SCA resistance evaluation method based on the signal-to-noise ratio (SNR) of the side-channel trace and a side-channel trace simulation method using the EDA (electronic design automation) tool. For the former, the signal-to-noise ratio measurement method was shown. For the latter, a simpler and faster simulation method than the conventional method was shown. As a result, it showed that it can contribute to efficiency improvement of SCA resistance prediction.

Chapter 4 described an optimal design method of RL and RC snubber circuits in a case where the snubbers are applied to a synchronous buck converter for realizing (B). For optimization, the converter circuit was simplified with considering the inpedance magnitude of components at the target frequency. It was shown that the optimum parameters can be analytically and uniquely determined by deriving the equation with the Q factor (objective function) and the snubber parameters (variables) in the simplified equivalent circuit.

Chapter 5 concludes that it is expected that the methods of Chapters 2–4 contribute to efficiency of EMC and hardware security design.

概要

IoT(Internet of Things) の進展に伴い，電気・電子機器の動作周波数や消費電力の増加により，伝導電磁ノイズによる EMI(electromagnetic interference）が大きくなり，機器周辺の電磁環境がこれまで以上に悪化している．それにより，EMC(electromagnetic conpatibility) 規格の EMI 規制値が厳しくなっている．したがって，EMI を制御し，各機器のノイズ耐性を向上させる EMC 設計がこれまで以上に重要となる．

他方で，不正アクセス，通信データの盗聴や改ざん，サービスの中断などのセキュリティ攻撃のリスクが高まっている．特に，IoT 製品は屋内外で使用され，オープンで物理的なアクセスが容易なため，SCA(side-channel attack) のような HWS(hardware security) 攻撃が懸念されている．SCA 耐性基準は，様々な組織によって厳しく規制されている．したがって，IoT 時代の機器では，EMC 設計だけでなく，HWS 設計も重要であり，効率的な HWS 設計が EMC 設計と同じ理由で同時に必要である．

さらに，IoT の進展は凄まじいため，IoT 機器の生産速度の加速に対応するために効率的な EMC/HWS 設計も同時に要求される．一般的に，製品開発のプロセスは，設計，試作，性能評価の順に実行される．しかし，これらのプロセスを一度で終えることは稀であり，評価後の性能が要求性能を満足せず，設計プロセスからやり直すことが多い．この手戻りは製品開発の遅れを引き起こすため，繰り返しは避けるべきである．

繰り返しを避け，効率的に設計するためには，膨大な工数とコスト（試作と性能評価）を必要とする作業は省略すべきである．そのため，製品開発の効率化を図るためには，以下の 2 つの実現が要求される．

(A) 製品の性能は試作および性能評価プロセスを経ることなく設計プロセスで予測すること

(B) 試行錯誤なしに製品の設計を最適化すること．

CAE(computer aided engineering) ツールを用いてこれらの問題を解決することが現代のトレンドである．CAE ツールは，製品の性能予測や設計最適化において非常に強力なツールであるものの，製品全体の特性を CAE ツールに反映させることは，計算コストの観点から現実的ではない．そのため，計算コストを削減するために，効率的な EMC と HWS 性能の予測手法が求められる．効率的なシミュレーションのためには，解析範囲を絞り込み，高速な解析モデルを構築することが必要である．モデル構築のための工数は可能な限り少ない方が好ましく，モデル構築の容易さが重要である．また，モデルの性能はモデル構築時の条件に依存するため，条件を適切に決定する必要がある．CAE ツールを用いたとしても，複数の構成要素からなる回路や PCB の特性を最適に調整することは容

易ではない．複数のパラメータを同時に最適化できなければ，設計とシミュレーションのプロセスが繰り返されてしまう．そのため，最適設計手法の確立も同時に要求される．構成要素を最適化するためには，目標の性能を表す指標に対して構成要素を変数に持つ関数を導出し，目標を満たす構成要素の組を算出することが重要である．関数の導出において，構成要素の全てを変数とすることは現実的に不可能であるため，構成要素を簡略化する必要がある．最適化の精度や最適設計の適用限界は簡略化の方法に依存するため，適切な簡略化が重要である．

本研究の目的は，上記 (A) と (B) の実現による EMC/HWS 設計の効率化である．そのための具体的な方法として，次の 3 つを検討した．

- EMC 設計において (A) を実現するための，伝導妨害を予測するノイズ源等価回路モデルおよびその構築法
- HWS 設計において (A) を実現するための，サイドチャネル攻撃耐性の予測手法
- EMC および HWS 設計において (B) を実現するための，スナバ回路を最適に設計する手法

2 章では，(A) 実現のために，ノイズ源等価回路モデルの同定法を提案した．この方法では，モデル構築工数の削減のため，データロガー (もしくはオシロスコープ) と測定プローブで構成される非常に簡便な測定系を用いた．モデル構築の適切な条件として，モデル構造，測定方法，測定精度について検討した．その結果，実用上十分な精度と言える 6 dB 以内の誤差で伝導妨害波を推定することができた．

3 章では，(A) 実現のために，サイドチャネル攻撃耐性の予測手法を検討した．サイドチャネルトレースの信号対雑音比に基づくサイドチャネル攻撃耐性評価方法と，EDA(electronic design automation) ツールを使用したサイドチャネルトレースシミュレーション方法について検討した．前者においては，信号対雑音比の測定方法を示した．後者においては，従来の方法よりも簡易かつ高速にシミュレーション可能な方法を示した．その結果，サイドチャネル攻撃耐性予測の効率化に寄与できることを示した．

4 章では，(B) 実現のために，RL および RC スナバ回路を同期降圧型コンバータに適用し，その最適設計法を提案した．最適化のために，ターゲット周波数における構成要素のインピーダンスの大きさに着目し，コンバータ回路を簡略化した．さらに，簡略化した等価回路において，Q 値を目的関数とし，スナバパラメータを変数に持つ式を導出することで，最適なパラメータを解析的かつ一意に決定できることを示した．

5 章では，本研究で得られた知見をまとめ，本論文で示した手法が IoT 時代における電気電子機器の EMC/ハードウェアセキュリティ設計手法の効率化に有用であることを述べた．

Acknowledgments

This thesis is a summary of my doctoral study in 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 who has granted me the chance to start this research and has given me innumerable advices and unrelenting encouragement. Thanks are extended to Professor Yasuyuki Nogami and Professor Eiji Hiraki who have given me much precious guidance on the course of this research. I am also deeply grateful to Assistant Professor Kengo Iokibe for his significant comments, advices, and delightful discussions which inspired many of the ideas in this thesis. I am also indebted to Dr. Tetsushi Watanabe in Industrial Technology Center of Okayama Prefecture for his impressive counsels and great insight. I am also deeply grateful to Professor Osami Wada for his significant comments, advices. My sincere thanks, going to Mr. Noriaki Kawanishi and Mr. Keiji Kino in GopherTec Inc. who supported us for precious support and helpful advice in research on side channel attacks.

I am also grateful to all present and past members of Optical and Electromagnetic Waves Laboratory, Okayama University. I particularity thank to the following members, who did much of the technical work and helped me overcome the difficulties encountered in my studies: Mr. Hiroki Geshi, Mr. Naoki Kawata, Mr. Yuhei Osaki, Mr. Yasunari Kumano, Mr. Toshiaki Teshima. I also appreciate the excellent secretarial services provided by Ms. Midori Ohnishi and Ms. Yumiko Kurooka.

Finally, I would like to dedicate this thesis to my parents, Ms. Mikiko Yano and Mr. Noboru Yano, in appreciation of their generous support and continuous encouragement.

Contents

List of Figures

List of Tables

Chapter 1

General Introduction

1.1 Background

With the progress in internet of things (IoT), various IoT devices (e.g., information terminals such as smartphone, sensors such as global positioning system and complementary metal oxide semiconductor, etc.) are developed. The IoT devices provide a wide variety of services for consumer, commercial, industrial, and infrastrucure. For example, in consumer services, automobile driving services, energy management services such as smart home, etc., are provided. In commercial applications, medical and helthcare services, transportation services, etc., are provided. For developing those services, many technical topics are vigorously researched [1]. To realize those services, it is essential to improve the performance of IoT devices. Improving the performance have been brought about by increased component density on printed circuit boards (PCBs), higher-speed switching speed of semiconductor devices, efficiency of data processing such as information-communication and cryptographic, etc..

In this situation, however, electromagnetic environment surrounding the electrical and electronic equipments becomes worse than ever because electromagnetic interference (EMI) caused by conducted or radiated electromagnetic noise becomes larger due to increase in the operating frequency and the power consumption of integrated circuits and power converter circuits. Along with the increase in EMI, EMI regulation levels of various standards, e.g., VCCI (Voluntary Control Council for Interference by Information Technology Equipment), CISPR (Comité International Spécial des Perturbations Radioélectriques), etc., become stringent. Therefore, electromagnetic compatibility (EMC) design to control the EMI and improve noise immunity of equipments becomes increasingly important.

Besides, the risk of security attacks such as unauthorized access, communication data eavesdropping and tampering, and service interruption has increased. Especially, hardware security (HWS) attacks such as side-channel attacks (SCAs) [2] are concerned because IoT products are used indoors and outdoors and are open and easy to access physically. Recently, the vulnerability of CPUs to SCA has been reported [3, 4]. SCA resistance criteria are regulated stringently by various organizations, e.g., IPA (Information-technology Promotion Agency) in Japan, NIST (National Institute of Standards and Technology) in the U.S.. Therefore, for equipment in IoT era, not only the EMC design but also HWS design to increase HWS attack resistance are important.

In addition, since the progress in IoT is growing rapidly, efficienct EMC design is required simultaneously.

1.2 Motivation

In IoT era, the quality and the efficiency of the EMC design and the HWS design are goes on important. Researches of this thesis examine methods to realize efficient EMC and HWS design. This subsection explains the motivation for the researches.

Fig. 1.1(a) shows a product development process. Generally, a product development process is driven in the order below: specification development, system and functional design, hardware and software design, trial production, and performance evaluation. However, it is rare to finish these processes at once. Actually, the performance at first evaluation often does unsatisfy the required performance, engineers will often do over again from the hardware and software design process. Since this rework causes delay in product development, a repetition of the rework should be avoided.

To prevent the repetition and to design efficiently, works which required an enormous amount of man-hours and costs (i.e. the trial production and the performance evaluation) should be ommited. To improve the efficiency in product development, it is necessary two things:

(A) predicting the product performance in the design process without going through the complete trial manufacture and performance evaluation process, and

(B) optimizing the product design without trial and error.

The main objective of this thesis is to achieve (A) and (B) in the EMC and hardware security design. If (A) and (B) are ideally achieved, the design process will be the one shown in Fig. 1.1(b). The unnecessary man-hours and costs are reduced by achieving (A), and the reworks are reduced by achieving (B).

Solving these issues, (A) and (B), with computer-aided engineering (CAE) is a current trend. Fig. 1.2 shows a product development process containing CAE analysis. CAE tools are very powerful because they can reduce trial cost in product performance prediction and design optimization, but reflecting the characteristics of the entire product to the CAE tools is unrealistic in terms of calculation cost. Therefore, a simulation method of efficient EMC and HWS performance prediction is required to reduce the calculation cost. For the efficient simulation, it is important to construct high-speed analyzable models and to narrow down the analysis dimension and range. Besides, even if the CAE tool is used, it is difficult to optimize a component of product composed of plural elements. If plural

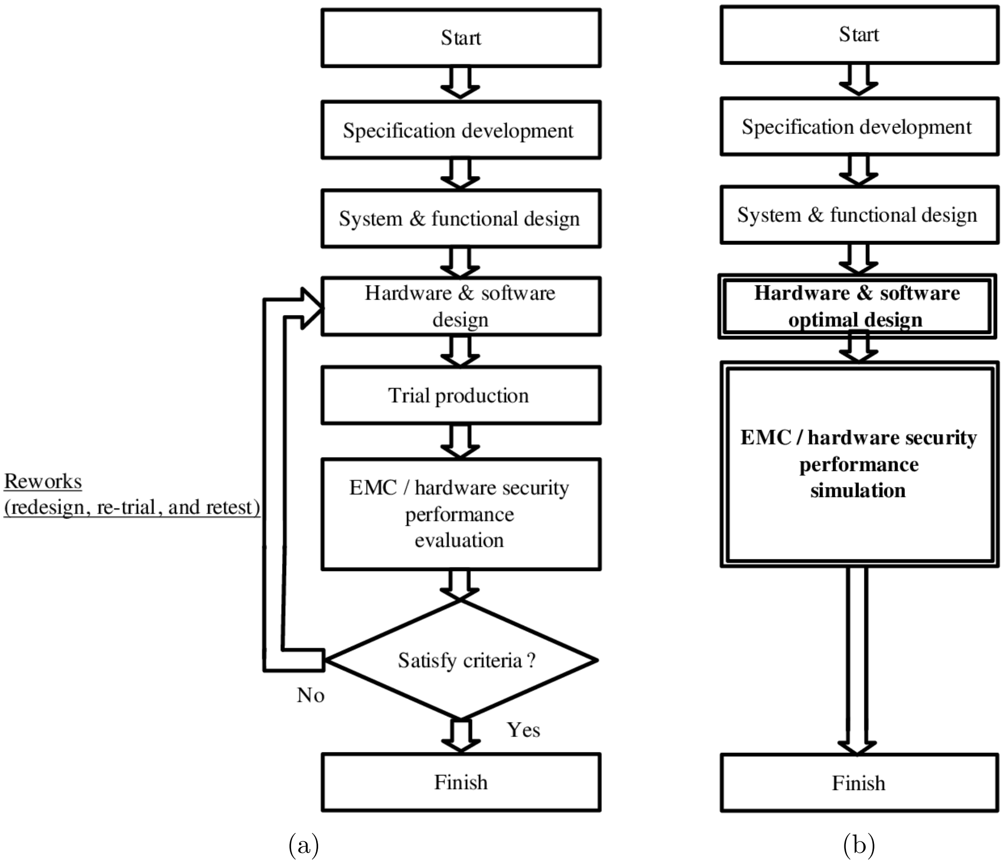

Start
Specification development
System & functional design
Hardware & software design
Trial production
EMC / hardware security performance evaluation
Satisfy criteria ?
No
Yes
Finish
Reworks
(redesign, re-trial, and retest)
(a)
Start
Specification development
System & functional design
Hardware & software optimal design
EMC / hardware security performance simulation
Finish
(b)

Figure 1.1 Development processes of products: (a) general and (b) efficient.

elements can not be simultaneously optimized, the design and simulation processes are repeated. Therefore, a optimal design method is also required. To optimize the plural elements, it is important to derive a function having the elements as a variable with respect to a criterion representing a target performance, and calculate the set of elements that satisfy the target.

The objective of this thesis is establishing efficient EMC and HWS design methods realizing (A) and (B). For realizing (A) in the EMC design, this thesis investigates noise-source equivalent circuit modeling to predict conducted disturbances (a type of EMI) caused by power convertor circuits. Power converter circuits are implemented all sorts of electronic equipments and are the cause of large EMI. The noise source equivalent circuit model is a model that can analyze noise characteristics quickly by narrowing down the analysis target to only noise. For realizing (A) in the HWS design, this thesis focuses a SCA to a field-programmable gate array (FPGA) and investigates a SCA resistance estimation method. FPGA is a highly versatile integrated circuit, and it is implemented in various equipment including cryptographic equipment. For establishing the estimation method, we examined two topics: an SCA resistance evaluation method based on the SNR of side-channel traces and an efficient side-channel trace simulation method using

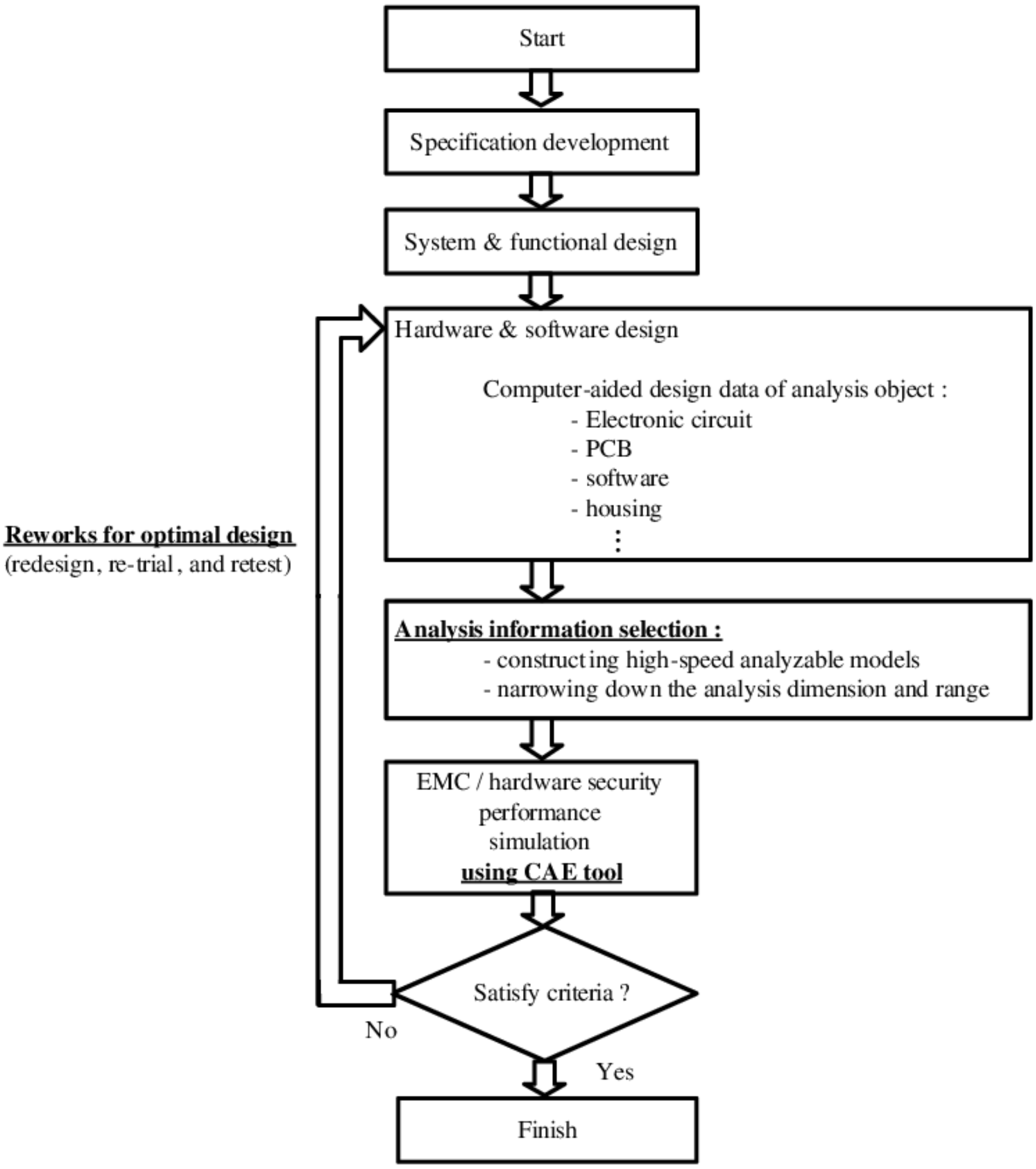

Start
Specification development
System & functional design
Hardware & software design
Computer-aided design data of analysis object :
- Electronic circuit
- PCB
- software
- housing
⋮
Analysis information selection :
- constructing high-speed analyzable models
- narrowing down the analysis dimension and range
EMC / hardware security performance simulation using CAE tool
Satisfy criteria ?
No
Yes
Finish
Reworks for optimal design
(redesign, re-trial, and retest)

Figure 1.2 Product development process with CAE analysis

an electronic design automation (EDA) tool. There is a problem that the results of the existing SCA resistance evaluation can not be fed back to the electric circuit design because the existing evaluation criteria are different from the circuit design criteria. To solve this problem, this work focus on the SNR which is applicable to both criteria of the SCA resistance evaluation and the circuit design. The simulation method used here is a method to predict the side channel trace at high-speed by narrowing down design information used in the prediction. For realizing (B), this thesis focuses snubber circuits which are widely known filter to dump resonances and investigates thier optimal design method. Since resonances occur in all sorts of electronic equipments and increase the EMI and information leakage, a optimal design method is required. Here, the snubber circuits are optimized by using the Q factor which expresses the sharpness of resonance.

As preliminary before describing details of these investigations, issues of existing methods and objectives of the investigations are explained in section 2 of each chapter.

1.3 Outline of Thesis

Figure 1.3 shows the outline of this thesis.

Chapter 2 described a noise-source equivalent circuit model and a model identification method for realizing (A). The model has two elements: equivalent sources and equivalent impedances representing respectively high-frequency current generated by switching devices and current leakage paths. The model parameters are identified only from external conducted disturbances (measured with an oscilloscope or a data logger) using circuit equations for the equivalent circuit including measurement system. The feature of this modeling method is that measurements using weak signals for modeling like the existing methods are not required. This feature make it possible to model large power equipments which were out of the application of the existing methods. Moreover, since the dedicated PCB and the advanced analysis are not used in model identification, it can be expected that the workload is reduced. The method proposed here is developed to eliminate two potential reasons for the reduced conducted disturbance simulation accuracy in previous works. The first is that part of the current was not represented in the previous model due to a balanced bridge circuit formed by the model and the measurement system. The second is that the measurement data used for parameter identification was not linearly independent because the circuit conditions were improperly changed during measurement. The model was applied to an induction heating cooker having a versatile power converter circuit, and the errors in the conducted disturbance simulation were evaluated.

Chapter 3 described a study of a SNR estimation method in side-channel analysis for realizing (A). For establishing it, this work is examined two topics: an SCA resistance evaluation method based on the SNR of side-channel traces and an efficient side-channel trace simulation method using an electronic design automation (EDA) tool. Firstly, this work has experimentally verified whether measured SNRs and correlation coefficients satisfy the analytical relationship. Since existing SCA resistance evaluation criteria are different from the circuit design criteria, there is a problem that the results of the existing evaluation can not be fed back to the electric circuit design. To solve this problem, this work focus on the SNR of side-channel traces. The SNR is commonly used as a design criterion in the circuit design, and the existing SCA resistance criteria can be predicted from the SNR. That is, if the SNR and the correlation coefficients can be accurately calculated, the SNR can be used for both the determination of countermeasure design targets and evaluation of the SCA resistance. Here, a method to measure the SNR accurately is proposed for experimental verification. The SNR was calculated using a signal component obtained from the trace when encrypting a random plaintext set and a noise component obtained from the trace when encrypting a constant plaintext set, and the correlation coefficient was calculated based on the CPA. A PCB having an FPGA implemented an AES circuit was used as an EUT, and the core power supply voltage fluctuation of the FPGA on the PCB was measured as side-channel trace. The SNR was varied by changing measurement conditions, measurement system, and EUTs, and the relationship was examined. Secondly, this work has proposed a side-channel trace simulation method using EDA tools and has investigated whether the estimated traces have the side-channel information. Here, the current consumption of a cryptographic device during encryption is calculated as the side-channel traces. The current is estimated only from the damp file, which is generated by register transfer level (RTL) simulation, using a power consumption analyzing function of an EDA tool. Since detailed design information such as propagation delay is not included in the dump file generated here, the calculation cost is reduced as compared with the conventional methods. The fluctuations of the current with respect to the random plaintext set were estimated and compared with the measured one.

Chapter 4 described an optimal design method of RL and RC snubber circuits in a case where the snubbers are applied to a synchronous buck converter for realizing (B). The method proposed here optimizes simultaneously two electronic components of the RL or RC snubber. To determine optimum snubber parameters analytically and uniquely, a contour plot drawn by a formula for the Q factor as a function of the snubber parameters derived from a simplified equivalent circuit of the resonant loop is used. The Q factor is a parameter that describes how underdamped an resonance is, and it is often used for design target in EMC design. The effects of the snubbers optimized using this method were reproduced by SPICE simulation to validate the method from the perspective of resonance damping, overshoot and power loss. The results showed that the damping effects obtained with the optimized snubbers met the Q factor design targets. They also demonstrate that the parameters are optimum in terms of suppressing overshoot and power loss. These results indicate that the method is suitable for optimizing RL and RC snubbers to damp parasitic LC resonance. The method proposed here is expected to be applied to other circuits because the contour plot can be drawn by any circuit if any objective function is just decided. This means that the proposed method is an efficient EMC and HWS design method.

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

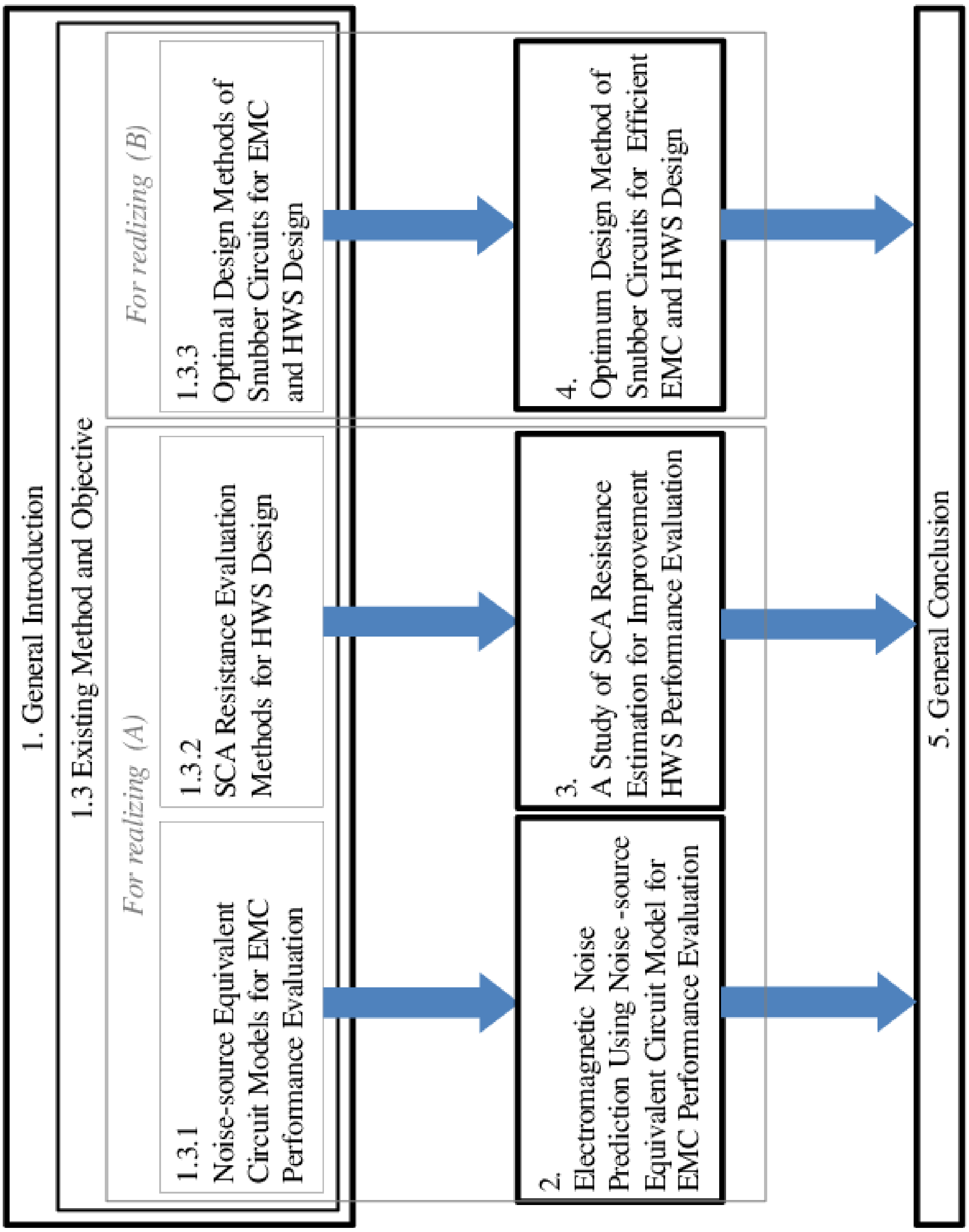

1. General Introduction
1.3 Existing Method and Objective
For realizing (A)
For realizing (B)
1.3.1
Noise-source Equivalent Circuit Models for EMC Performance Evaluation
1.3.2
SCA Resistance Evaluation Methods for HWS Design
1.3.3
Optimal Design Methods of Snubber Circuits for EMC and HWS Design
2.
Electromagnetic Noise Prediction Using Noise -source Equivalent Circuit Model for EMC Performance Evaluation
3.
A Study of SCA Resistance Estimation for Improvement HWS Performance Evaluation
4.
Optimum Design Method of Snubber Circuits for Efficient EMC and HWS Design
5. General Conclusion

Figure 1.3 Outline of this thesis

Chapter 2

Electromagnetic Noise Prediction Using Noise-source Equivalent Circuit Model for EMC Performance Evaluation

2.1 Introduction

The operating frequency of power converter circuits in electronic equipment is increasing due to the need for higher power efficiency and smaller electronic devices. Reducing electromagnetic interference (EMI) has thus become more important, and filters for suppressing EMI are required. To efficiently design such filters, a method is needed for quickly predicting EMI with high accuracy. Limits on the EMI generated in household appliances were established by CISPR 14-1 [40], and various noise source models have been developed for quickly predicting EMI [7–11].

Several noise source equivalent circuit models representing conducted disturbances caused by semiconductor device switching have been proposed [7–11]. Some of them [7–9] have equivalent current sources and equivalent linear circuit elements. The equivalent current sources represent the high-frequency current generated by the nonlinear switching operation of the semiconductor devices, and the equivalent linear circuit elements represent the impedances of the EMI leakage paths. A recently reported equivalent voltage source model consisting of voltage sources representing the voltage variations caused by device switching and of impedances [10] has a circuit structure similar to those of previously reported models [7–9]. Moreover, a model has been reported that consists of elements having functions representing the state transitions of semiconductor devices and the impedances [11]. These circuit models enable the prediction of EMI and power quality deterioration. Constructing such models (e.g., [7–11]) requires information on the impedance characteristics of the semiconductor devices, circuit components, and printed circuit boards (PCBs) of the equipment under test (EUT). However, obtaining these impedance characteristics may involve a lot of work. Models of the semiconductor devices and the electrical characteristics of the circuit components may not be available from the manufacturers, so measurements may need to be made. To obtain the electrical characteristics of the PCBs, measurement using a vector network analyzer (VNA) or simulation using an electromagnetic field analysis simulator is generally used. However, such measurement requires that the PCBs having dedicated patterns and dedicated terminals are needed to connect the measurement probes, increasing the workload. Furthermore, as PCBs become larger and more complicated, a greater amount of analysis time following simulation is needed.

A method for reducing the increase in workload has been proposed [12]. The impedance characteristics of the EUT are identified by inputting and outputting the input and output signals of a VNA into and from the EUT through current probes. With this method, changes to the system such as adding dedicated terminals are not needed for measurement, and the combined impedance of the semiconductor devices, circuit elements, and PCBs are obtained. However, if the EUT consumes a large amount of power, the noise it generates is much greater than the signal output from the VNA, making it difficult to measure the impedance characteristics with sufficient accuracy.

In this paper, we present a noise source equivalent circuit model and a model parameter identification method that are effective even in the large power consumption of the EUT. It is intended to complement the existing method. While the elements in the circuit model (equivalent power sources and equivalent impedances) are similar to those in previously proposed models [7–9], the method for identifying model parameters is different. The parameters are identified from circuit equations of the overall equivalent circuit (including a model of the EUT and the measurement system) and external conducted disturbances measured with a measuring instrument (e.g. an oscilloscope or a data logger). Since only the external measurement data are used (and not an injected signal), it is possible to identify the model parameters when the power consumption of the EUT is large although it is difficult to identify them at frequencies with low power consumption.

In previous work [13, 15], we examined a method for predicting the conducted disturbance voltage. A tabletop induction heating (IH) cooker with a general power converter circuit was used as the EUT. The method accurately predicted conducted disturbances under no-EMI-filter conditions but not under EMI-filter conditions. Subsequent work identified two potential reasons for the reduced accuracy and the method proposed here was developed to eliminate them. The first reason is that part of the current was not represented in the model used due to a balanced bridge circuit formed by the model impedance and the measurement system impedance. The second reason is that the measurement data used for model parameter identification was not linearly independent due to the way that the circuit conditions were changed during measurement was improper.

The rest of the paper is organized as follows. Section 2.2 introduces existing noise source equivalent circuit models and an objective of this research. Section 2.3 introduces the structure of the noise source equivalent circuit model and the method for identifying the model parameters. Section 2.4 describes their application in a system for measuring the conducted disturbance voltage and presents the identified parameters. Section 2.5 describes the simulation of the conducted disturbance voltage and discusses the error. Section 2.7 concludes the paper with a summary of the key points.

2.2 Existing Noise-source Equivalent Circuit Models

Reducing EMI has become more important, and carefully designed filters and PCBs for suppressing EMI are required. To efficiently design them, a method is needed for quickly predicting EMI with high accuracy because, as (A) described in Section 1.2, reflecting the characteristics of the entire product to CAE tools is unrealistic in terms of calculation cost. In [5,6], an circuit operation and an EMI are simulated by using models that faithfully express switching devices and a circuit configuration of a power conversion circuit including paracitic impedances. However, these simulation modeling is inefficient because it is necessary to model one each device and circuit pattern particularly, it is difficult and time-consuming.

Several noise source equivalent circuit models have been proposed for representing conducted disturbances caused by semiconductor device switching [7–11]. Some of them [7–9] have equivalent current sources and equivalent linear circuit elements. The equivalent current sources represent the high-frequency current generated by the nonlinear switching operation of the semiconductor devices, and the equivalent linear circuit elements represent the impedances of the EMI leakage paths. A recently reported equivalent voltage source model consisting of voltage sources representing the voltage variations caused by device switching and of impedances [10] has a circuit structure similar to those of previously reported models [7–9]. Moreover, a model has been reported that consists of elements having functions representing the state transitions of semiconductor devices and the impedances [11]. These circuit models enable the prediction of EMI and power quality deterioration. These models express only the noise generated in electric circuits and do not express the circuit operation, so that the modeling difficulty decreases because it is not necessary to know structure details of a target circuit to be modeled compared with [5,6]. This means that these models can simulate EMI even when detail information of circuit components is not available form the manufacturers. These models are models that can analyze noise characteristics quickly by narrowing down the analysis target to only noise.

Constructing such models (e.g., [7–11]) requires information on the impedance characteristics of a modeling target circuit and leakage noise. Unfortunately, obtaining these impedance characteristics may involve a lot of work. To obtain the electrical characteristics of the circuit components and the PCBs, simulation using an EM simulator or measurement using a vector network analyzer (VNA) is generally used. Table 2.1 shows features of these general methods and an existing method for reducing measurement costs [12].

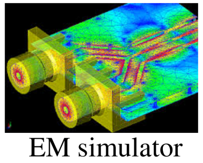
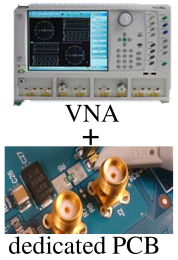
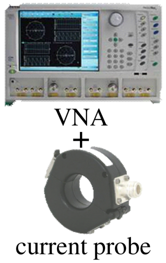
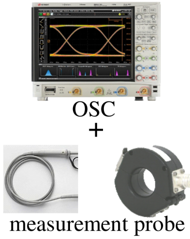
In the simulation using an EM simulator, the impedance extraction cost is extremely high. As PCBs become larger and more complicated, a greater amount of analysis time following simulation is needed. Furthermore, it is impractical to apply that to the EUT in operation. This is because an immense amount of analysis time is needed and models of all circuit components are required.

In the measurement using a VNA and dedicated PCBs, the impedance extraction cost is high. PCBs having dedicated patterns and dedicated terminals are required to connect the measurement probes of a VNA. This method has a limitation when applied to the EUT in operation. If the EUT consumes a large amount of power, the noise it generates is much greater than the signal output from the VNA, making it difficult to measure the impedance characteristics with sufficient accuracy.

A method have been proposed to reduce the impedance extraction cost in the general measurement method [12]. This method uses a VNA and current probes. Owing to contactless probing, no change in the dedicated board and the measurement system is required, thereby reducing the impedance extraction cost. However, this method is limited to small consumption EUTs for the same reason as the general measurement method.

This thesis proposed a noise source equivalent circuit model and a model parameter identification method that are effective even in large power consumption of the EUT. The model has two elements: equivalent sources and equivalent impedances representing respectively high-frequency current generated by switching devices and current leakage paths. The model parameters are identified only from external conducted disturbances (measured with an oscilloscope or a data logger) using circuit equations for the equivalent circuit including measurement system. The feature of this modeling method is that measurements using weak signals for modeling like the existing methods are not required. This feature make it possible to model large power equipments which were out of the application of the existing methods. Moreover, since the dedicated PCB and the advanced analysis are not used in model identification, it can be expected that the workload is reduced. The method proposed here is developed to eliminate two potential reasons for the reduced conducted disturbance simulation accuracy in previous works [13–15]. The first is that part of the current was not represented in the previous model due to a balanced bridge circuit formed by the model and the measurement system. The second is that the measurement data used for parameter identification was not linearly independent because the circuit conditions were improperly changed during measurement. Details of investigations are described in Chapter 2.

Table 2.1 Features of general and existing methods for obtaining electrical characteristics of circuit components and PCBs

	General methods		Existing method	Proposed method
Requirement	 Simulation using an EM simulator	 Measurement using a VNA and dedicated PCBs	 Measurement using a VNA and current probes [12]	 Measurement using a OSC and measurement probes
Impedance extraction cost	**High** (As PCBs become larger and more complicated, a greater amount of analysis time following simulation is needed.)	**High** (the PCBs having dedicated patterns and dedicated terminals are required to connect the measurement probes.)	**Low** (Owing to contactless probing, no change in the dedicated board and the measurement system is required.)	**Low** (Owing to use of measurement equipments generaly used in EMI measurement, no change in the dedicated board and the measurement system is required.)
Application to EUT in operation	**Impractical** (An immense amount of analysis time is needed. Models of all circuit components are required.)	**Limited** (If the EUT consumes a large amount of power, the noise is much greater than the signal output from the VNA, making it difficult to measure the impedance characteristics with sufficient accuracy.)		**Unlimited** (Since measurements using weak signals for modeling like the existing methods are not required, it is possible to model large power equipments.)

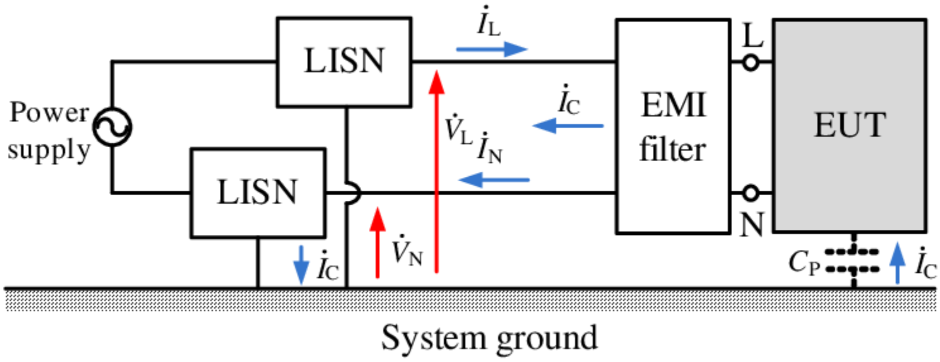


Figure 2.1 Diagrammatic illustration of system for measuring conducted disturbance voltages.

2.3 Proposed Noise Source Equivalent Circuit Model

Fig. 2.1 shows a diagrammatic illustration of the system specified in CISPR 16-2-1 [41] for measuring conducted disturbance voltages. The EUT is connected to a commercial power supply via a line impedance stabilization network (LISN). An EMI filter is mounted on the EUT. $\dot{V}_{\mathrm{L}}$ and $\dot{V}_{\mathrm{N}}$ represent the conducted disturbance voltages, which are high-frequency voltages from the L and N phases of the EUT port to the system ground, respectively. $\dot{I}_{\mathrm{L}}$ and $\dot{I}_{\mathrm{N}}$ represent normal mode currents flowing along each phase of the EUT port. C_{P} is the parasitic capacitance between the EUT and the system ground. $\dot{I}_{\mathrm{C}}$ represents a common mode current flowing through the loop consisting of C_{P}, the EUT, power cables, the LISN, and the system ground.

2.3.1 Model Structure

Previously reported models [7–11, 13, 15] have equivalent source elements representing the high-frequency currents generated by the nonlinear switching activity of the semiconductor devices and equivalent linear circuit elements representing the impedances of the EMI leakage paths. The model proposed here has the same structure.

Fig. 2.2 shows the noise source equivalent circuit model. $\dot{I}_{\mathrm{d}}$ is the equivalent current source representing the high-frequency current generated by an EUT switching device. $\dot{Z}_{\mathrm{d}}$ is the equivalent impedance for the normal mode impedance of the EUT. $\dot{Z}_{\mathrm{c}}$ is the equivalent impedance for the common mode impedance. $\dot{V}_{\mathrm{c}}$ is the equivalent voltage source representing the electromotive force that generates the common mode current. The coefficient α of $\dot{I}_{\mathrm{d}}$ and $\dot{Z}_{\mathrm{d}}$ is an unbalance factor representing the unbalance of the normal mode elements across node A.

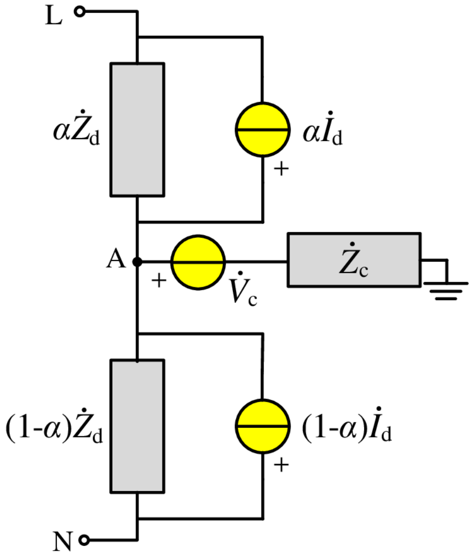


Figure 2.2 Noise source equivalent circuit model.

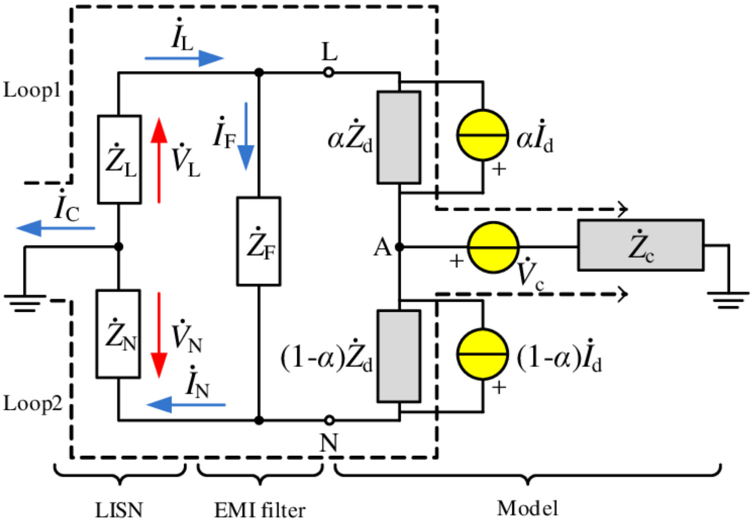


Figure 2.3 Combined equivalent circuit of measurement system and noise-source equivalent circuit model shown respectively in Fig. 2.1 and Fig. 2.2.

2.3.2 Parameter Identification Method

The parameters are identified from circuit equations of the overall equivalent circuit (including a model of the EUT and the measurement system) and external conducted disturbances measured with a measuring instrument (e.g. an oscilloscope or a data logger).

Fig. 2.3 shows the equivalent circuit for the case in which the model shown in Fig. 2.2 is applied to the EUT portion of the measurement system shown in Fig. 2.1. The right side of port L–N is the proposed noise source model and the left side is the EMI filter and the LISN. $\dot{Z}_L$ and $\dot{Z}_N$ are the equivalent impedances between the EUT side terminals and the ground terminal of the LISN. $\dot{Z}_\mathrm{F}$ is the impedance of the EMI filter. $\dot{V}_\mathrm{L}$, $\dot{V}_\mathrm{N}$, $\dot{I}_\mathrm{L}$, $\dot{I}_\mathrm{N}$ and $\dot{I}_\mathrm{C}$ correspond to those in Fig. 2.1. The model parameters are identified using these voltages and currents, which are measurable outside the EUT. $\dot{I}_\mathrm{F}$ is defined as the current flowing through $\dot{Z}_\mathrm{F}$ and is calculated using

$$\dot{I}_\mathrm{F} = (\dot{V}_\mathrm{L} - \dot{V}_\mathrm{N})/\dot{Z}_\mathrm{F}. \tag{2.1}$$

The circuit equations of the equivalent circuit shown in Fig. 2.3 are derived for model parameter identification. Application of Kirchhoff's voltage law to loops 1 and 2 (shown by the dashed lines in Fig. 2.3) gives the equations:

$$\begin{bmatrix} \dot{V}_\mathrm{L} \\ \dot{V}_\mathrm{N} \end{bmatrix} = \begin{bmatrix} -1 & \dot{I}_\mathrm{L} - \dot{I}_\mathrm{F} & 0 & 0 & 1 & -\dot{I}_\mathrm{C} \\ 0 & 0 & 1 & \dot{I}_\mathrm{F} - \dot{I}_\mathrm{N} & 1 & -\dot{I}_\mathrm{C} \end{bmatrix} \begin{bmatrix} -\alpha^2 \dot{Z}_\mathrm{d} \dot{I}_\mathrm{d} \\ \alpha \dot{Z}_\mathrm{d} \\ (1-\alpha)^2 \dot{Z}_\mathrm{d} \dot{I}_\mathrm{d} \\ (1-\alpha) \dot{Z}_\mathrm{d} \\ \dot{V}_\mathrm{c} \\ \dot{Z}_\mathrm{c} \end{bmatrix}. \tag{2.2}$$

The model parameters are determined in accordance with (2.2).

The equations (2.2) are the simultaneous quadratic equations with five unknowns ($\dot{Z}_\mathrm{d}$, $\dot{I}_\mathrm{d}$, $\dot{Z}_\mathrm{c}$, $\dot{V}_\mathrm{c}$, and α). To solve the equations, the coefficient α is determined before identifying the model parameters. When α is determined, the equations (2.2) become the simultaneous linear equations with four unknowns as shown below, and they can be easily solved.

$$\begin{bmatrix} \dot{V}_\mathrm{L} \\ \dot{V}_\mathrm{N} \end{bmatrix} = \begin{bmatrix} -\alpha^2 & \alpha(\dot{I}_\mathrm{L} - \dot{I}_\mathrm{F}) & 1 & -\dot{I}_\mathrm{C} \\ (1-\alpha)^2 & (1-\alpha)(\dot{I}_\mathrm{F} - \dot{I}_\mathrm{N}) & 1 & -\dot{I}_\mathrm{C} \end{bmatrix} \begin{bmatrix} \dot{Z}_\mathrm{d} \dot{I}_\mathrm{d} \\ \dot{Z}_\mathrm{d} \\ \dot{V}_\mathrm{c} \\ \dot{Z}_\mathrm{c} \end{bmatrix}. \tag{2.3}$$

The coefficient α must be carefully determined because the value of α affects the accuracy of model parameter identification. In our previous work [15], we assumed that the common mode current flowing through the EUT flows equally to terminals L and N. We thus set α to 0.5 to make the two normal mode impedances ($\alpha \dot{Z}_\mathrm{d}$ and $(1-\alpha)\dot{Z}_\mathrm{d}$) equal. However, setting α to 0.5 creates a problem: a state in which part of the current generated by $\dot{V}_\mathrm{c}$ flows through $\dot{Z}_\mathrm{F}$ cannot be represented. This is because $\dot{Z}_\mathrm{L}$ and $\dot{Z}_\mathrm{N}$ are generally equal, and $\alpha \dot{Z}_\mathrm{d}$ and $(1-\alpha)\dot{Z}_\mathrm{d}$ are also generally equal. This means that the circuit on the left side of node A (Fig. 2.3) becomes a balanced bridge circuit. If the actual EUT has unbalanced common mode current paths, a contradiction arises between the $\dot{I}_\mathrm{F}$ of the measurement and the $\dot{I}_\mathrm{F}$ of the equivalent circuit. This contradiction may cause an error in model parameter identification. Therefore, α should be set to a value other than 0.5. The determination of α will be explained in the next section.

Solving the simultaneous linear equations requires that the measurement data set be acquired multiple times. In general, a solution is unobtainable unless the number of unknowns is equal to the number of equations. Therefore, n measurements are needed to obtain a sufficient number of linear equations. The minimum number of measurements $n_{\rm min}$ required is the smallest positive integer satisfying $n_{\rm min} \geq$ (number of parameters) / (number of circuit equations). Here, since the number of unknowns is four ($\dot{Z}_{\rm d}$, $\dot{I}_{\rm d}$, $\dot{Z}_{\rm c}$, and $\dot{V}_{\rm c}$) and the number of equations is two, $n_{\rm min}$ is two.

The linear equations obtained from the multiple measurements must be linearly independent, so a circuit condition is changed for each measurement to obtain measurement data unique to each measurement. The circuit condition is changed by using a different electrostatic capacitance for the EMI filter. The characteristics of the EMI filters used in this work are described in the next section. This method for changing the circuit condition differs from that used in our previous work [15]. In that work, a resistor simulating the input impedance of the measurement equipment was connected to the LISN measurement port, and the resistance was varied between 5 and 500 Ω. However, the input impedance of the LISN seen by the EUT was not changed at a frequency lower than 300 kHz, that is, the circuit condition was not changed, and linearly independent measurement data were not obtained. The input impedance of the LISN side seen by the EUT can be changed at a lower frequency by varying the impedance of the EMI filter.

To identify the model parameters from the measurement data, it is necessary to measure not only the magnitude but also the phase. Therefore, an oscilloscope or data logger is used to measure the data. Data having different phases are obtained by changing the circuit conditions for each measurement. To align the phases of the data, it is also necessary to measure a trigger signal (e.g. the gate drive signal of the switching device) for each measurement.

2.4 Parameter Identification

2.4.1 EUT and Measurement System

The model parameter identification method was applied to a system for measuring conducted disturbance voltages. The system configuration is shown in Fig.2.4, and the equipment specifications are listed in Table 2.2.

In Fig.2.4, $\dot{V}_{\rm L}$ and $\dot{V}_{\rm N}$ are the conducted disturbance voltages, $\dot{I}_{\rm L}$ and $\dot{I}_{\rm N}$ are the normal mode currents, and $\dot{I}_{\rm C}$ is the common mode current. The system ground is a ground reference plane in a shield room. The EUT was connected to the LISN through a 400-mm power cable positioned 50 mm above the system ground. Although this measurement system was basically constructed in accordance with CISPR16-2-1 [41] in that the EUT was placed directly on the system ground, it differed from the CISPR standard. To evaluate the model in the presence of both normal mode current and common mode current, we increased parasitic capacitance $C_{\rm P}$ between the ground plane of the EUT PCB and the system ground, thereby increasing the common mode current. As the EUT, we used a tabletop IH cooker (Panasonic, KZ-PH32) containing a general power

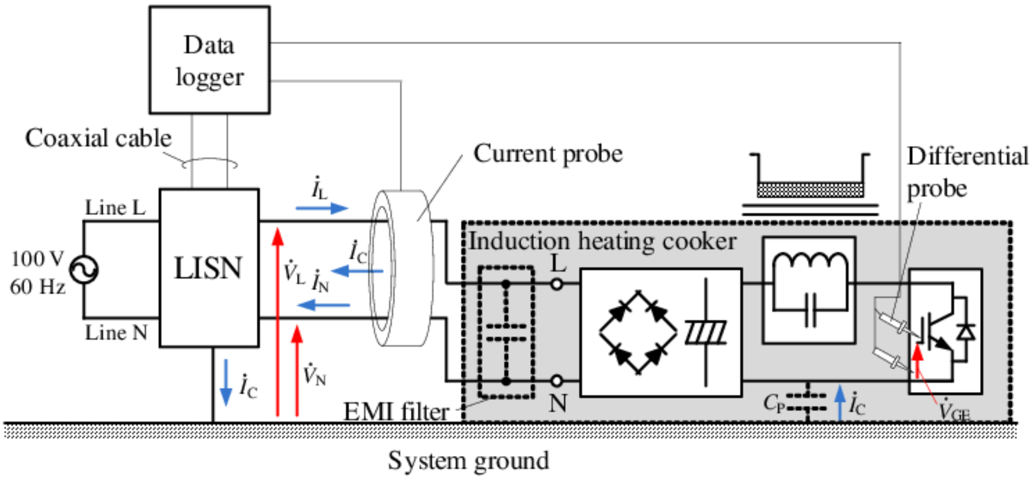


Figure 2.4 Configuration of system for measuring conducted disturbance voltages.

Table 2.2 Specifications of System for Measuring Conducted Disturbance Voltages.

Component	Specifications
Induction heating cooker	KZ-PH32, Panasonic
Power level setting	1400 W
LISN	Custom made
Electrical characteristics	Described elsewhere [42].
Data logger	DL850, Yokogawa
Module	720210
Sampling rate	20 MS/s
Frequency band	DC – 20 MHz
Current probe	94111-1L, ETS-Lindgren
Frequency band	20 Hz – 1 GHz
Differential probe	P5200A, Tektronix
Frequency band	DC – 50 MHz

converter circuit. As the LISN, we used one prepared by our research group [42], which has impedance characteristics conformed to CISPR16-1-2 [43].

We applied the model shown in Fig. 2.2 to the whole circuit of the EUT, hence the model does not correspond exactly to the circuit configuration of the EUT. The model equivalently express the noise occurring in the EUT and its leakage.

At the same time that we measured the voltage and current data ($\dot{V}_{\mathrm{L}}$, $\dot{V}_{\mathrm{N}}$, $\dot{I}_{\mathrm{L}}$, $\dot{I}_{\mathrm{N}}$, and $\dot{I}_{\mathrm{C}}$) for use in identifying the model parameters, we also measured the gate-emitter voltage $\dot{V}_{\mathrm{GE}}$ of an insulated-gate bipolar transistor (IGBT) mounted on the EUT PCB for use in aligning the phases of the data. We used a data logger (Yokogawa, DL850) to make the measurements. $\dot{V}_{\mathrm{L}}$, $\dot{V}_{\mathrm{N}}$, $\dot{I}_{\mathrm{L}}$, and $\dot{I}_{\mathrm{N}}$ were measured indirectly; instead, they were calculated from the measured voltages at the LISN measurement ports ($\dot{V}_{\mathrm{A}}$ and $\dot{V}_{\mathrm{B}}$)

and the known LISN impedance [42]. The input impedance of the LISN looking from the EUT port $\dot{Z}_{\mathrm{in}}$ is calculated by

$$\dot{Z}_{\mathrm{in}} = \dot{Z}_{11} - \frac{\dot{Z}_{12}}{\dot{Z}_{21}}\dot{Z}_{\mathrm{mp}}, \tag{2.4}$$

where, $\dot{Z}_{\mathrm{mp}}$ is the LISN measurement port impedance, $\dot{Z}_{11}$, $\dot{Z}_{12}$, $\dot{Z}_{21}$, and $\dot{Z}_{22}$ are Z-parameters of the LISN. $\dot{V}_{\mathrm{L}}$ and $\dot{V}_{\mathrm{N}}$ are calculated by

$$\dot{V}_{\mathrm{L,N}} = \frac{\dot{Z}_{\mathrm{in}}}{\dot{Z}_{21}}(1 + \frac{\dot{Z}_{22}}{\dot{Z}_{\mathrm{mp}}})\dot{V}_{\mathrm{A,B}}, \tag{2.5}$$

$\dot{I}_{\mathrm{L}}$ and $\dot{I}_{\mathrm{N}}$ are calculated by

$$\dot{I}_{\mathrm{L,N}} = \frac{\dot{V}_{\mathrm{L,N}}}{\dot{Z}_{\mathrm{in}}}. \tag{2.6}$$

The data logger was connected to the LISN measurement ports by coaxial cables. The ports were terminated with 50-Ω resistors because the input impedance of the data logger was fixed at 1 MΩ. That is, $\dot{Z}_{\mathrm{mp}}$ is 50-Ω. $\dot{I}_{\mathrm{C}}$ was measured on the power cable between the LISN and EUT using a current probe (ETS-Lindgren, 94111-1L) and a 50-Ω termination resistor. $\dot{V}_{\mathrm{GE}}$ was measured using a differential probe (Tektronix, P5200A). Besides, line voltage (60 Hz, 100 V) was measured using a coaxial cable as a trigger signal.

Fig. 2.5 shows time domain waveform of the conducted disturbances ($\dot{V}_{\mathrm{A}}$, $\dot{V}_{\mathrm{B}}$, and $\dot{I}_{\mathrm{C}}$) and trigger signals ($\dot{V}_{\mathrm{GE}}$ and line voltage). $\dot{V}_{\mathrm{A}}$ and $\dot{V}_{\mathrm{B}}$ vary with the line voltage in top side of Fig. 2.5. $\dot{V}_{\mathrm{A}}$ and $\dot{V}_{\mathrm{B}}$ also vary with $\dot{V}_{\mathrm{GE}}$ in bottom side of Fig. 2.5. Therefore, $\dot{V}_{\mathrm{A}}$ and $\dot{V}_{\mathrm{B}}$ should be obtained synchronized with both the line voltage and $\dot{V}_{\mathrm{GE}}$. $\dot{V}_{\mathrm{A}}$ and $\dot{V}_{\mathrm{B}}$ were obtained using two level triggers as shown in bottom side of Fig. 2.5. Besides, they were acquired at the sampling rate of 20 MHz during the period of 1 ms. Data used in the model identification $\dot{V}_{\mathrm{L}}$, $\dot{V}_{\mathrm{N}}$, $\dot{I}_{\mathrm{L}}$, and $\dot{I}_{\mathrm{N}}$ were calculated by 2.5 and 2.6.

Fig. 2.6 shows the spectral envelopes of the measured voltage or current without the EMI filter. Since the fundamental switching frequency of the IGBT was 27 kHz, its harmonic components are plotted. Fig. 2.6(a) shows the conduction disturbance voltage, where $\dot{V}_{\mathrm{L}}$ is shown as white circles, $\dot{V}_{\mathrm{N}}$ is shown as black circles, and the noise floor is shown as a gray line. $\dot{V}_{\mathrm{L}}$ and $\dot{V}_{\mathrm{N}}$ were 10 dB or more greater than the noise floor up to 3 MHz, so we evaluated the proposed model in the frequency band up to 3 MHz. Fig. 2.6(b) shows the normal mode current, where $\dot{I}_{\mathrm{L}}$ is shown as white circles, $\dot{I}_{\mathrm{N}}$ is shown as black circles, and the noise floor is shown as a gray line. At the fundamental switching frequency having the highest current level, the magnitudes of the normal mode currents were 110 dBμA. When applying the method of Tarateeraseth et al. [12], in which the impedance characteristics are obtained by injecting the signal into a measurement system from a VNA, a current of 120 dBμA or more must be injected. This makes experimentation difficult because such large current is not available to output with commercial VNAs.

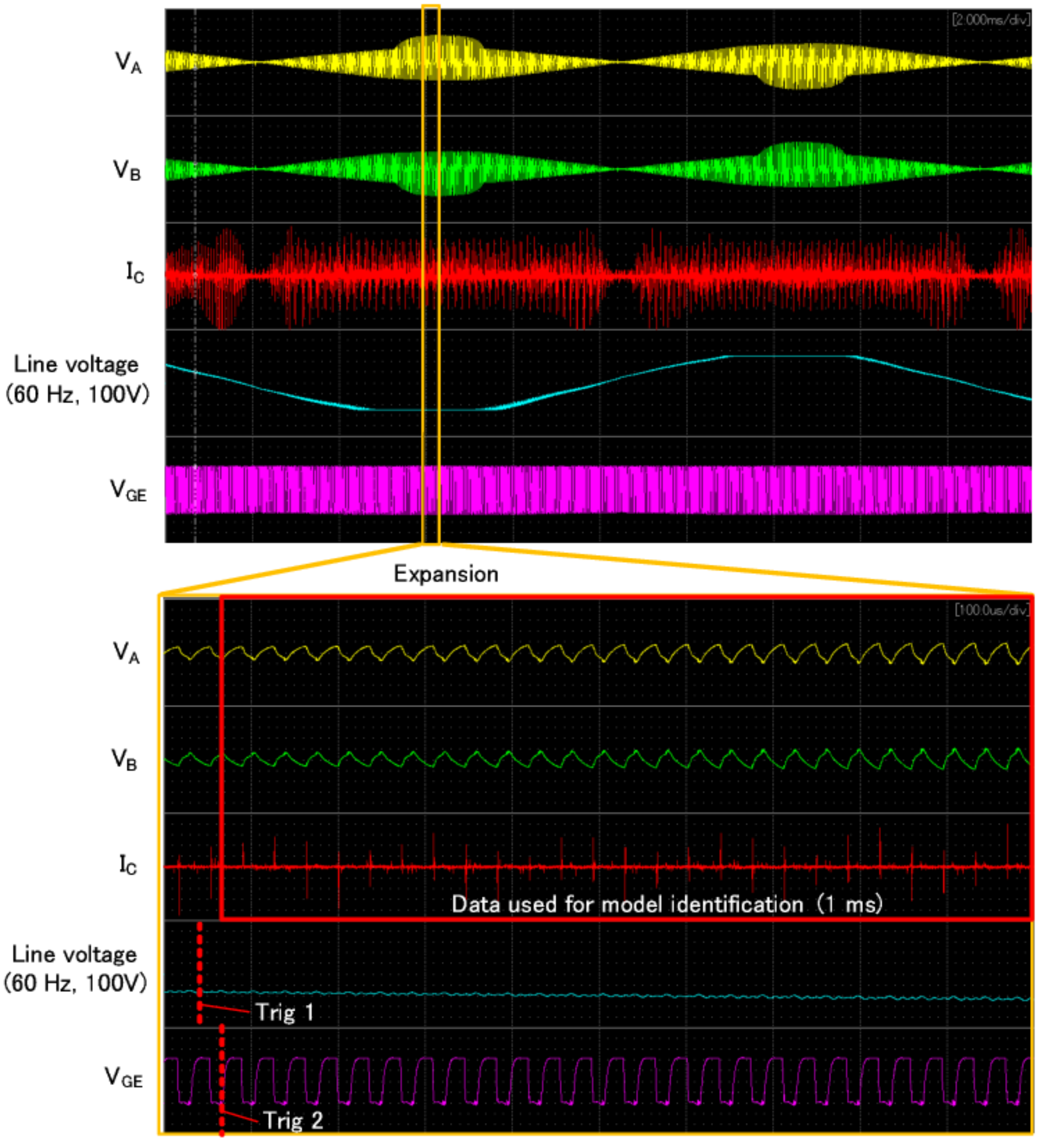
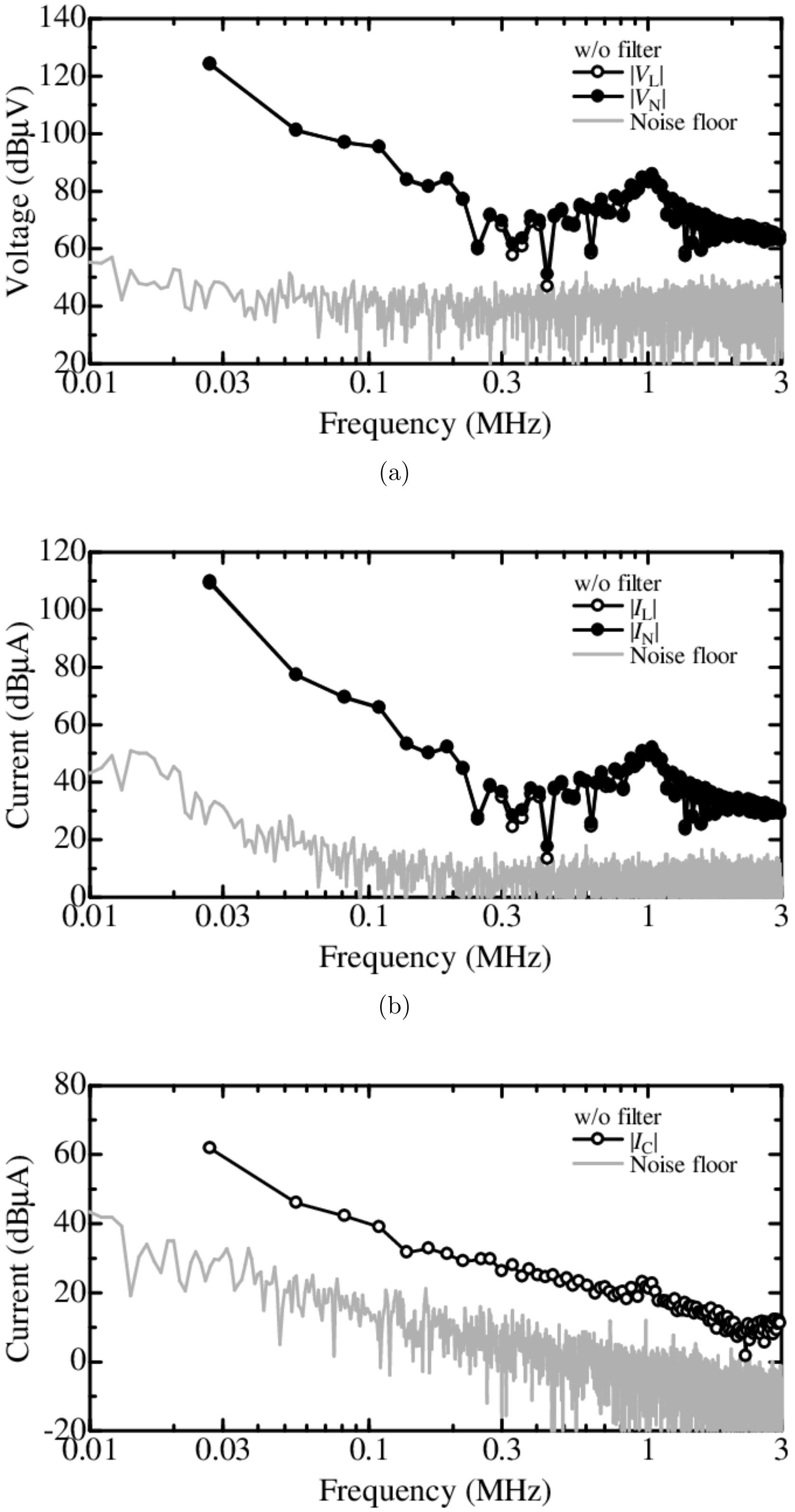


Figure 2.5 Time domain waveform of measured conducted disturbances and trigger signals.



(a)

(b)

(c)

Figure 2.6 Spectral envelopes of measured voltage or current without EMI filter: (a) $\dot{V}_L$ and $\dot{V}_N$, (b) $\dot{I}_L$ and $\dot{I}_N$, and (c) $\dot{I}_C$.

Table 2.3 EMI filter conditions and characteristics of leaded ceramic capacitors used as EMI filter.

	EMI filter characteristics		
Condition	Capacitance (μF)	ESL (nH)	ESR (mΩ)
w/o filter for modeling	open	-	-
w/ filterA for modeling	0.041	20	10
w/ filterB for evaluation	4.4	20	9

Fig. 2.6(c) shows the common mode current, where $\dot{I}_{\mathrm{C}}$ is shown by a white circle and the noise floor is shown by a gray line. The magnitude of $\dot{I}_{\mathrm{C}}$ was about 20 to 40 dB smaller than that of $\dot{I}_{\mathrm{L}}$ and $\dot{I}_{\mathrm{N}}$. This means that $\dot{I}_{\mathrm{L}}$ and $\dot{I}_{\mathrm{N}}$ contributed more to the conducted disturbance voltages ($\dot{V}_{\mathrm{L}}$ and $\dot{V}_{\mathrm{N}}$) than $\dot{I}_{\mathrm{C}}$. Therefore, we used a normal mode filter as the EMI filter in our evaluation.

2.4.2 Identified Model Parameters

The coefficients of the normal mode model parameters were changed from $\alpha = 0.5$ in the previous study to $\alpha = 1$ for two reasons. The first one was to prevent a circuit from becoming a balanced bridge circuit, as described in Section 2.3. The second was so that the model structure would approximate the actual structure of the EUT. The EUT has only one switching device; moreover, the power supply layer of the terminal N-side is located on the system ground side of the EUT PCB, and the parasitic capacitance C_{P} between the EUT and the system ground is assumed to be on the terminal N-side. Parameters $\dot{V}_{\mathrm{c}}$ and $\dot{Z}_{\mathrm{c}}$, representing the equivalent common mode source, should be connected to the terminal N-side node to express the common mode current and path.

To identify the four model parameters, we measured the voltage and current data under two circuit conditions. Table 2.3 shows the characteristics of the two leaded ceramic capacitors used as an EMI filter. The conditions without the filter and with filter A were used for two measurements. The condition with filter B, the capacitor originally mounted on the EUT, was used for evaluation.

It was necessary to set the capacitance of filter A to an appropriate value. If it was too small, the measured data with filter A would not differ from those without the filter, and it would not be possible to solve the simultaneous equations. Conversely, if the capacitance was too large, the measured data would approach the noise floor, and it would not be possible to measure the data with sufficient accuracy. We set the capacitance of filter A to 0.041 μF, which we felt was an appropriate value.

It is expected that different data is obtained for different $\dot{Z}_{\mathrm{IN-LISN}}$, where $\dot{Z}_{\mathrm{IN-LISN}}$ is the normal mode input impedance looking leftward from terminal pair L–N in Fig. 2.4.

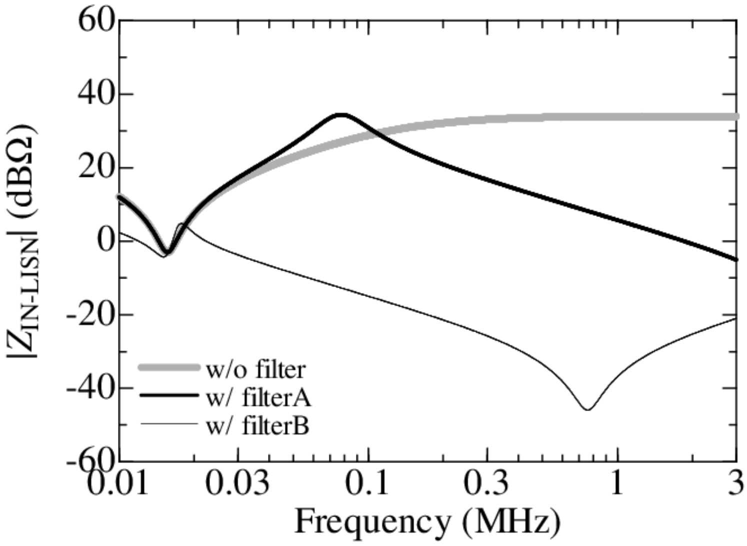


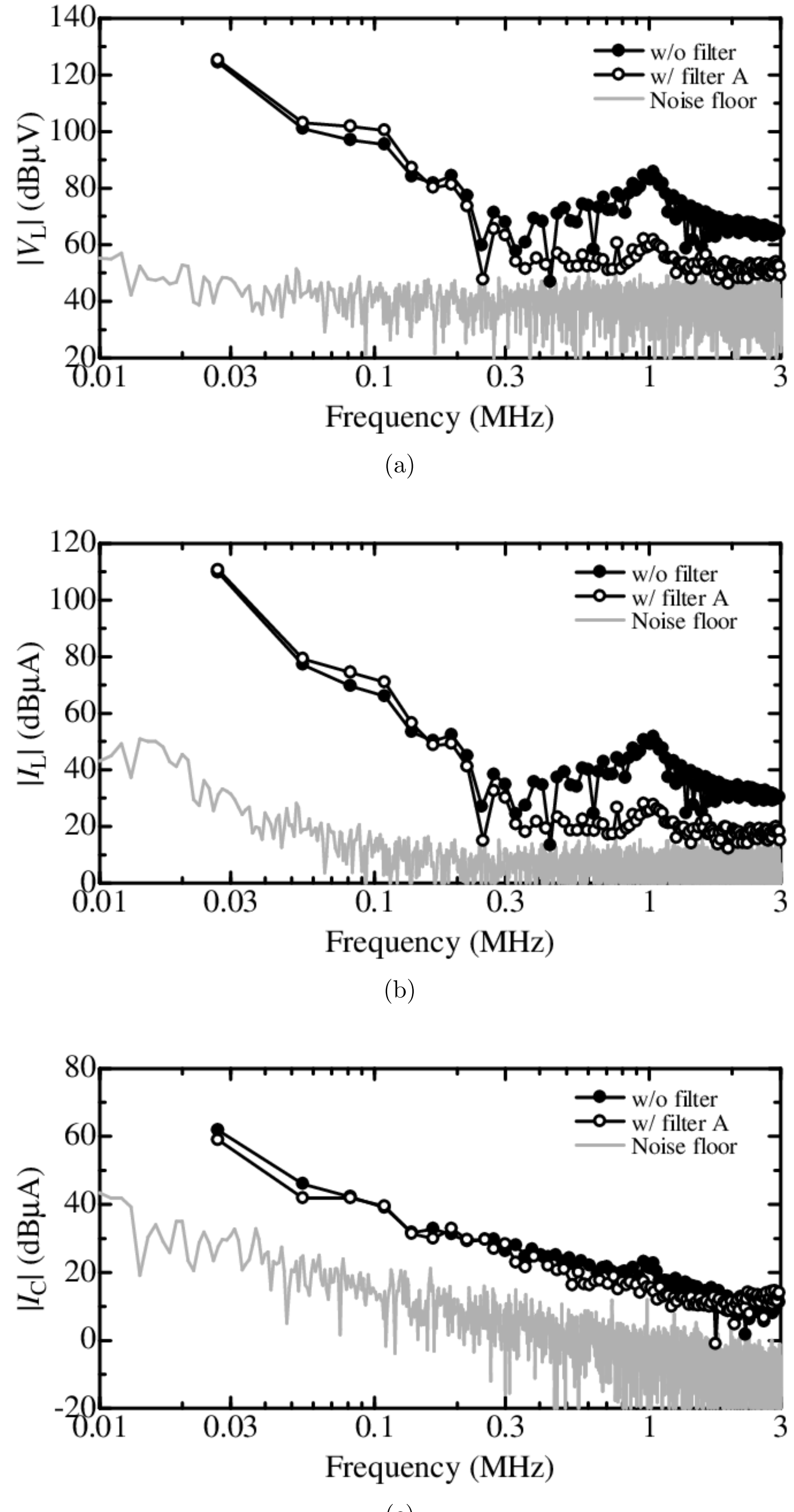
Figure 2.7 Normal mode input impedance $\dot{Z}_{\text{IN}-\text{LISN}}$ looking leftward from terminal pair L–N in Fig. 2.4.

Fig. 2.7 shows $\dot{Z}_{\text{IN}-\text{LISN}}$ under three filter conditions, where the thick gray line represents the condition without the filter, the thick black line represents the condition with filter A, and the thin black line represents the condition with filter B. The input impedance differed between the fundamental switching frequency of 27 kHz and higher switching frequencies under all filter conditions.

We checked that different data can be obtained under the two conditions (without and with filter A). Fig. 2.8(a), Fig. 2.8(b), and Fig. 2.8(c) show respectively $\dot{V}_{\text{L}}$, $\dot{I}_{\text{L}}$, $\dot{I}_{\text{C}}$. The black and white circles represent respectively the values measured without and with filter A. The gray solid line represents the noise floor. In Fig. 2.8(a), at frequencies below 0.25 MHz, the reduction in $\dot{V}_{\text{L}}$ corresponded to the reduction in $\dot{Z}_{\text{IN}-\text{LISN}}$ with filter A. For example, the reduction in $\dot{Z}_{\text{IN}-\text{LISN}}$ at 0.08 MHz was − 6 dB. Similarly, the reduction in $\dot{V}_{\text{L}}$ was − 6 dB. These consistent reductions indicate that there is a proportional relationship between $\dot{V}_{\text{L}}$ and $\dot{Z}_{\text{IN}-\text{LISN}}$. At frequencies above 0.25 MHz with filter A, $\dot{V}_{\text{L}}$ and the noise floor were equivalent at most frequencies, and the proportional relationship was not found due to the insufficient measured level. In Fig. 2.8(b), these features were also observed for $\dot{I}_{\text{L}}$. In Fig. 2.8(c), $\dot{I}_{\text{C}}$ were almost unchanged under two conditions.

Fig. 2.9 shows the four model parameters ($\dot{Z}_{\text{d}}$, $\dot{I}_{\text{d}}$, $\dot{Z}_{\text{c}}$, and $\dot{V}_{\text{c}}$) identified by using two sets of data measured under two conditions (without and with filter A). The solid lines represent the magnitudes, and the broken lines represent the phases. The upward triangles represent the parameters calculated using $\alpha = 1$, and the downward triangles represent the parameters calculated using the previously used $\alpha = 0.5$ [15].

The normal mode parameters were equivalent regardless of α even though there was a change in $\dot{Z}_{\text{d}}$. In the model, the open circuit voltage between terminal pair L–N $\dot{V}_{\text{LN}}$ is $\dot{V}_{\text{LN}} = -[\alpha^2 + (1-\alpha)^2]\dot{Z}_{\text{d}}\dot{I}_{\text{d}}$. The magnitude of $\dot{Z}_{\text{d}}$ with $\alpha = 0.5$ was 6 dB smaller than



(a)

(b)

(c)

Figure 2.8 Spectral envelopes of measured voltage or current under two conditions (without and with filterA): (a) $\dot{V}_{\mathrm{L}}$, (b) $\dot{I}_{\mathrm{L}}$, and (c) $\dot{I}_{\mathrm{C}}$.

the one with $\alpha = 1$ and the phases were equal. Therefore, $\dot{V}_{\text{LN}}$ was $-0.5\dot{Z}_{\text{d}}\dot{I}_{\text{d}}$ regardless of α.

The common mode parameters differed depending on α. The cause for these differences is presumed to be that $\dot{I}_{\text{F}}$ was represented in the equivalent circuit due to changing α. The differences in the simulated conducted disturbance voltages discussed in the next section were due to the difference in the common mode parameters.

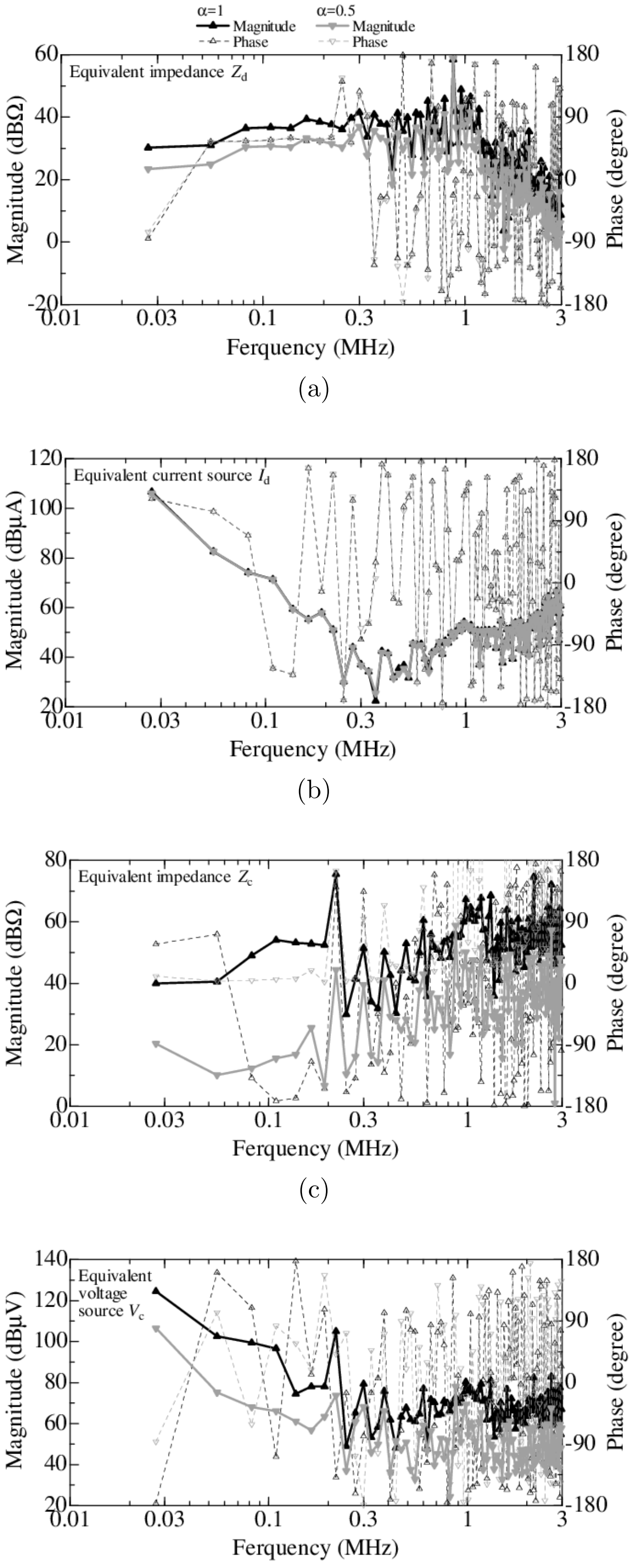
The equivalent normal mode impedance $\dot{Z}_{\text{d}}$ shown in Fig. 2.9(a) exceeded the range of $-$ 90 degrees to 90 degrees at frequencies higher than 0.25 MHz and did not exhibit a typical impedance characteristic. This was apparently due is attributed to the model structure not completely matching the actual structure of the EUT. That is, $\dot{Z}_{\text{d}}$ equivalently (not physically) represents the normal mode impedance of the EUT. The same applies to the equivalent common mode impedance $\dot{Z}_{\text{c}}$ shown in Fig. 2.9(c). Moreover, the spectrum gradients of the normal mode equivalent current source $\dot{I}_{\text{d}}$ and the common mode equivalent voltage source $\dot{V}_{\text{c}}$ were about $-$ 60 dB/decade, which differ from the gradient of a typical trapezoidal current wave. We speculate that this was due to $\dot{I}_{\text{d}}$ and $\dot{V}_{\text{c}}$ equivalently representing the switching current generated in the EUT.

2.5 Conducted Disturbance Voltage Simulation

2.5.1 Evaluation of Errors

We simulated the conducted disturbance voltage $\dot{V}_{\text{L}}$ using filter B (Table 2.3), the identified model parameters (Fig. 2.9), and the circuit shown in Fig. 2.3. Fig. 2.10 shows the spectral envelopes of the measured and simulated values. The black and white circles represent respectively the measured values without a filter and with filter B. The upward and downward triangles represent respectively the values simulated using $\alpha = 1$ and $\alpha = 0.5$. The gray solid line represents the measured noise floor. Using filter B reduced the measured value of $\dot{V}_{\text{L}}$ in accordance with the impedance characteristics plotted in Fig. 2.7. For $\alpha = 1$, the simulated $\dot{V}_{\text{L}}$ predicted the decrease in the measured one with filter B. For $\alpha = 0.5$, the simulated $\dot{V}_{\text{L}}$ approximately predicted the decrease in the measured one with filter B, but the accuracy was less than that for $\alpha = 1$. Fig. 2.11 shows the errors between the measured and simulated values. For $\alpha = 1$, the errors at most of frequencies below 1 MHz were less than 6 dB while those at frequencies above 1 MHz were larger than 6 dB. For $\alpha = 0.5$, the errors at most of frequencies below 1 MHz were less than 10 dB while those at frequencies above 1 MHz were larger than 10 dB. Same features were also observed for $\dot{V}_{\text{N}}$.

We concluded that the smaller errors for $\alpha = 1$ were because the asymmetric normal mode parameters made it possible to represent the part of the common mode current flowing through the EMI filter ($\dot{I}_{\text{F}}$). In Fig. 2.7, normal mode input impedance $\dot{Z}_{\text{IN-LISN}}$ with filter B was 20 dB or more lower than other filter conditions at most frequencies. It is reasonable that normal mode current $\dot{I}_{\text{L}}$ decreases as with $\dot{Z}_{\text{IN-LISN}}$. Therefore, when



(a)

(b)

(c)

(d)

Figure 2.9 Identified model parameters using $\alpha = 0.5$ and $\alpha = 1$: (a) $\dot{Z}_\text{d}$, (b) $\dot{I}_\text{d}$, (c) $\dot{Z}_\text{c}$, and (d) $\dot{V}_\text{c}$.

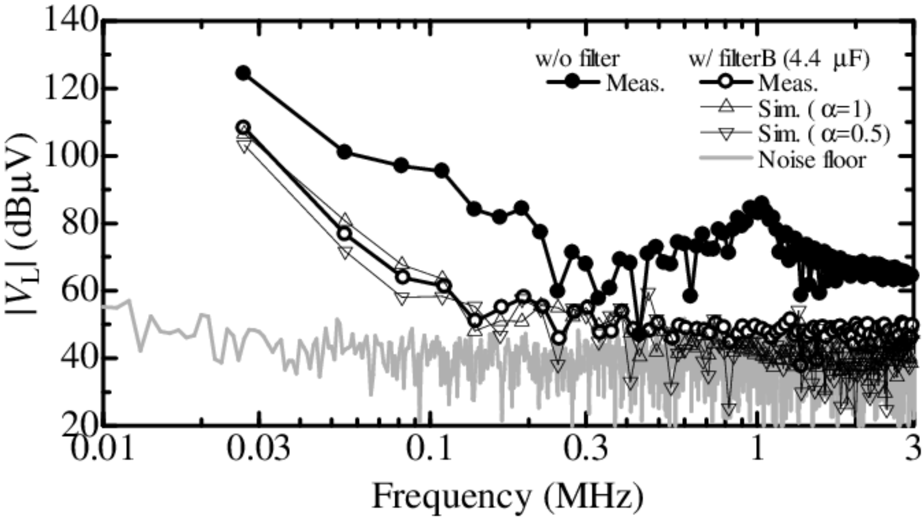


Figure 2.10 Spectral envelopes of measured conducted disturbance voltage $\dot{V}_L$ without filter and measured and simulated $\dot{V}_L$ with EMI filter B (4.4 μF).

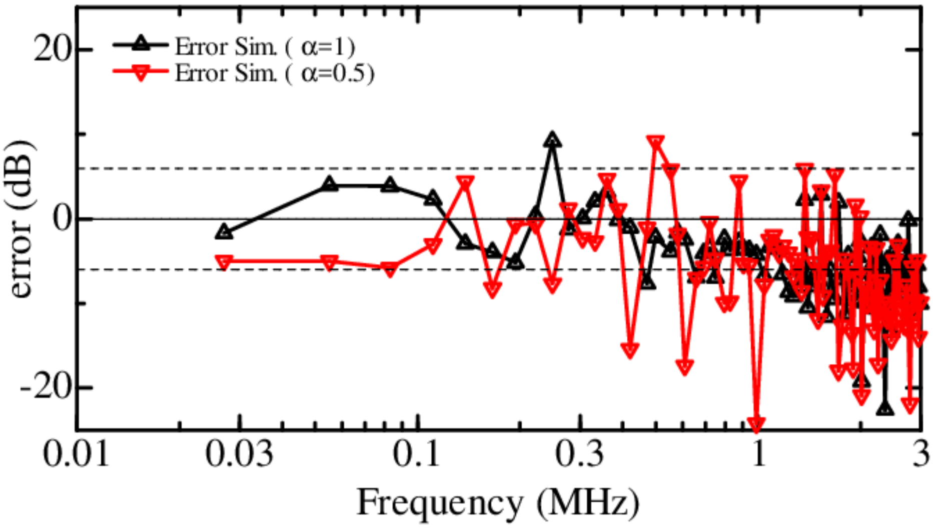


Figure 2.11 The errors between measured and simulated conducted disturbance voltages.

filter B was mounted, common mode current dominantly affected $\dot{V}_L$. Therefore, from Fig. 2.6(b) and Fig. 2.6(c), we deduce that $\dot{I}_L$ is equal to common mode current $\dot{I}_C$ at 54 kHz. This means that the identification accuracy of the common mode parameters also contribute to accuracy and that the contribution increases with the frequency. Since the common mode parameter identification accuracy for $\alpha = 1$, which can represent $\dot{I}_F$, is apparently better than that for $\alpha = 0.5$, the error for $\alpha = 1$ is considered to be smaller than that for $\alpha = 0.5$. Altogether, the results shown in Fig. 2.10 suggest that the model structure should be free of particular structures such as a balanced bridge circuit.

We tested two values of α in Fig. 2.10 and obtained different simulation results. This suggests that the prediction accuracy of $\dot{V}_{\mathrm{L}}$ depends on α, and besides, there is a possibility that another value of α that produces a more accurate prediction than $\alpha = 1$. To examine this, α of 0, 0.1, 0.3, 0.7, and 0.9 were used. The obtained model parameters are shown in Fig. 2.12. As mentioned above, since $\dot{V}_{\mathrm{LN}}$ is constant at $-0.5\dot{Z}_{\mathrm{d}}\dot{I}_{\mathrm{d}}$ regardless of the value of α, no difference was seen in $\dot{Z}_{\mathrm{d}}$ and $\dot{I}_{\mathrm{d}}$. On the other hand, since the expression accuracy of $\dot{I}_{\mathrm{F}}$ changes with α, the differences were seen in $\dot{Z}_{\mathrm{c}}$ and $\dot{V}_{\mathrm{c}}$. In $\dot{Z}_{\mathrm{c}}$ and $\dot{V}_{\mathrm{c}}$, the difference between $\alpha = 0.1$ and $\alpha = 0.3$ is larger than that between $\alpha = 0$ and $\alpha = 0.1$. That is, the closer the condition which $\dot{I}_{\mathrm{F}}$ is not expressed is set, the larger the parameters change. The prediction results of $\dot{V}_{\mathrm{L}}$ are shown in Fig. 2.13. Except for $\alpha = 0.5$, the whole $\dot{V}_{\mathrm{L}}$ were predicted with same accuracy. This result suggests that the same prediction accuracy can be obtained if particular structures such as a balanced bridge circuit are avoided.

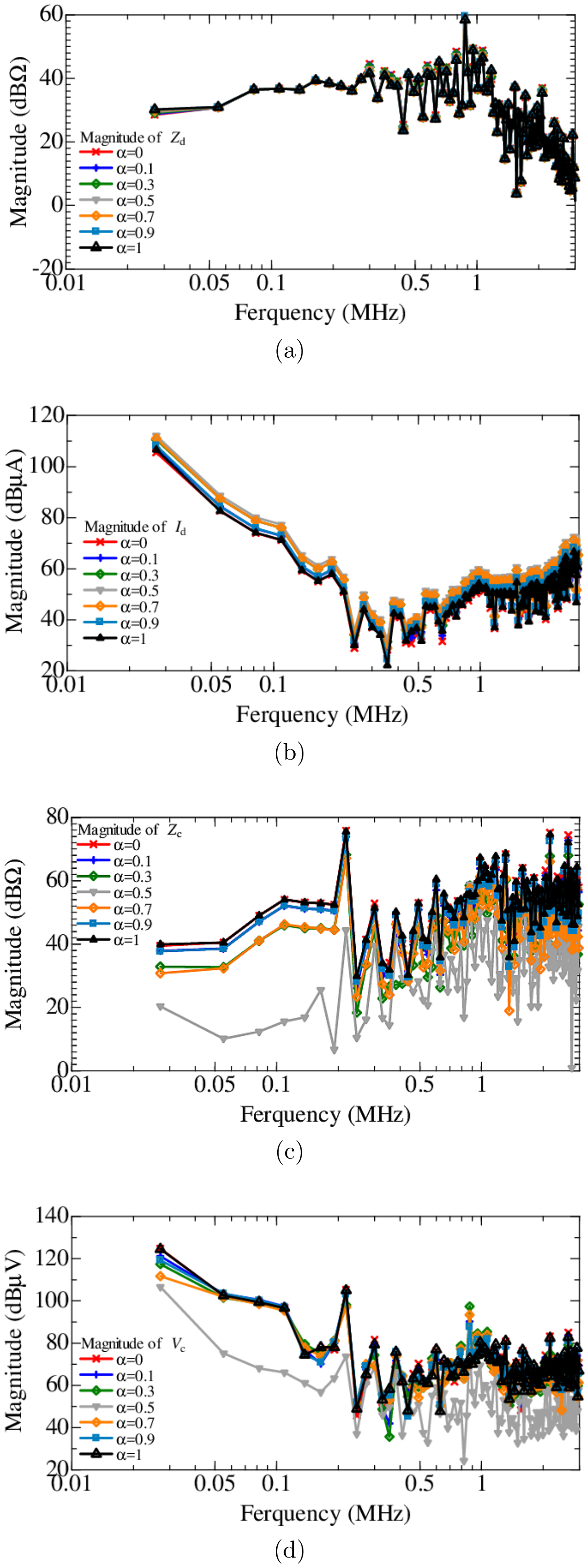
In Fig. 2.10, at frequencies above 1 MHz, errors exceeding 10 dB were observed for both values of α, and the prediction accuracy tended to decrease with the frequency. We next consider the cause of this decrease in accuracy.

2.5.2 Consideration of Prediction Accuracy Decrease at High Frequencies

The decrease in prediction accuracy was due to decrease in measurement accuracy for modeling. As shown in Fig. 2.8(b), $\dot{I}_{\mathrm{L}}$ was 20 dBμA at 1 MHz with filter A. Since $\dot{I}_{\mathrm{C}}$ is almost as much as $\dot{I}_{\mathrm{L}}$ at 1 MHz or more with filter A, as shown in Fig. 2.8(b) and Fig. 2.8(c), a voltage drop due to $\dot{I}_{\mathrm{C}}$ should be seen in $\dot{V}_{\mathrm{L}}$. However, $\dot{I}_{\mathrm{C}}$ was also small, so only the noise floor was observed. That is, measurement accuracy for $\dot{V}_{\mathrm{L}}$ was low. The frequencies with low measurement accuracy corresponded to those with low simulation accuracy. We thus concluded that the decrease in prediction accuracy at high frequencies was due to the decrease in measurement accuracy for modeling.

The decrease in measurement accuracy causes inconsistency between the measured voltage and the impedance of the measurement system. As mentioned in the previous section, the proportional relationship between $\dot{V}_{\mathrm{L}}$ and $\dot{Z}_{\mathrm{IN-LISN}}$ was not evident at frequencies above 1 MHz. This caused a contradiction in the simultaneous equations used for model parameter identification, resulting in errors in the model parameters. If the inconsistency is included in the measurement data used for identifying the model parameters, the condition number of simultaneous equations is large, which can result in inaccurate model parameters. This is why the prediction accuracy of $\dot{V}_{\mathrm{L}}$ was lower at higher frequencies.

From Fig. 2.8, we identified the measurement accuracy required to obtain sufficient prediction accuracy. In Fig. 2.8(a), at frequencies below 1 MHz, $\dot{V}_{\mathrm{L}}$ was greater than the



(a)

(b)

(c)

(d)

Figure 2.12 Identified model parameters using $\alpha = 0, 0.1, 0.3, 0.5, 0.7, 0.9, and 1$: (a) $\dot{Z}_{\rm d}$, (b) $\dot{I}_{\rm d}$, (c) $\dot{Z}_{\rm c}$, and (d) $\dot{V}_{\rm c}$.

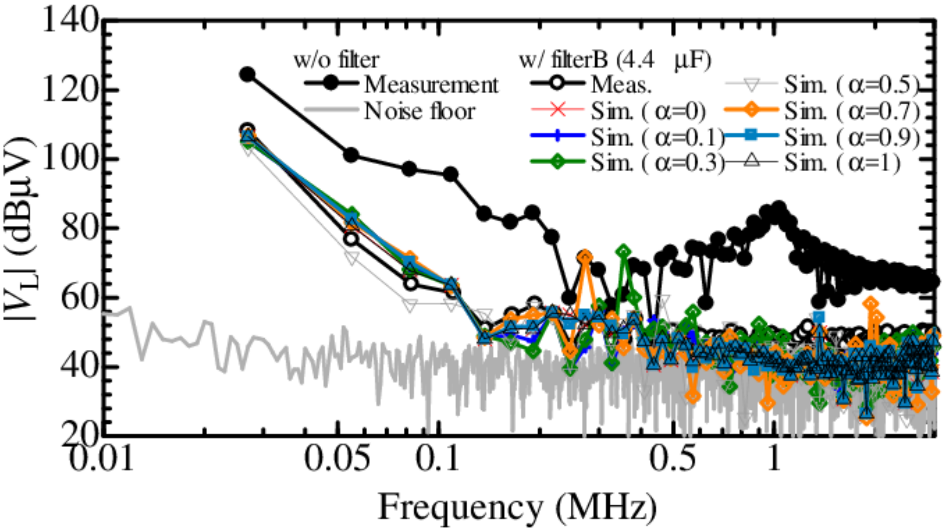


Figure 2.13 Spectral envelopes of measured and simulated $\dot{V}_{\mathrm{L}}$ for the different α.

noise floor by more than 10 dB for both filter conditions. At frequencies above 1 MHz without the filter, it was 20 dB or more than the noise floor at most frequencies. By contrast, at frequencies above 1 MHz with filter A, it and the noise floor were equivalent at most frequencies. In Fig. 2.8(b), these features were also observed for $\dot{I}_{\mathrm{L}}$. In Fig. 2.8(c), at frequencies below 1 MHz, $\dot{I}_{\mathrm{C}}$ was greater than the noise floor by about 20 dB for both filter conditions. At frequencies above 1 MHz, $\dot{I}_{\mathrm{C}}$ was greater than the noise floor by about 10 dB at most frequencies.

These results show that application of our noise source equivalent circuit model and our model parameter identification method requires that all measured voltages and current levels be larger than the noise floor by 10 dB or more. When changing the circuit conditions, care should be taken to ensure that the measured voltages and currents do not become too small under all circuit conditions. In the case of sufficiently measurement, the noise source equivalent circuit model and the identification method are effective for predicting conduction disturbance voltages. They are sufficiently accurate only when the original voltage and current levels are large compared to noise floor. Therefore, at a frequency with a low noise level, it is necessary to use them only as complements to another method, e.g. Tarateeraseth *et al.* [12].

2.6 Another Application

To demonstrate the applicability of this model to a wide variety of products, a DC-DC converter was modeled by the proposed method as another application example [44–46].

In the modeling shown here, the scope of circuits in which a model was applied differs from that shown in Section 2.3 to 2.5. In the modeling of the power converter circuit mentioned above, the scope of modeling was apploximately the circuit of the whole EUT.

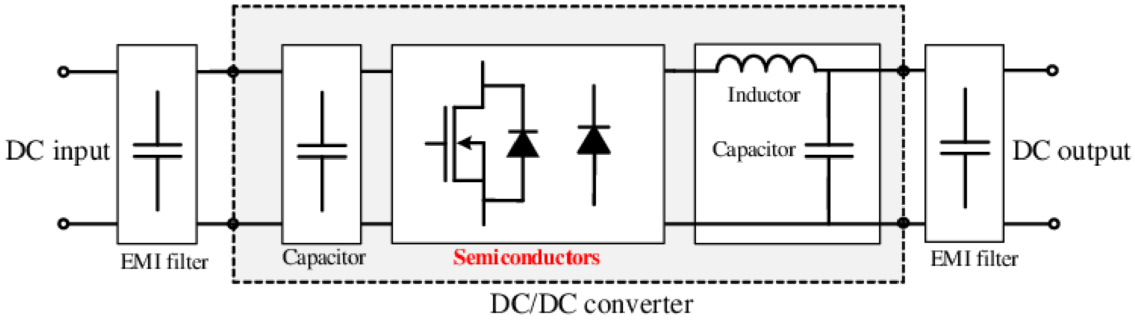


Figure 2.14 Diagrammatic illustration of DC-DC converter.

The reason for this is that the circuit size of the power conversion circuit is large, which is the major part of the EUT. The conversion from the normal-mode noise generated in the power converter circuit to the common-mode noise was sufficiently considered because the circuit is large, thus, the model representing both normal- and common-mode was constructed.

On the other hand, in a modeling of a DC-DC converter shown here, the scope of modeling is only the converter, and a model only represents the normal-mode noise. The reason for this is that the circuit size of the converter is small because that is used for low power products, and the conversion from normal-mode to common-mode in the converter is hardly occurs. That is, assuming that the conversion occurs at a place different from the converter, a model representing only the normal-mode noise generated in the converter can be constructed. Complex phenomena such as the conversion from normal-mode noise to common-mode noise and radiation of common-mode noise can be separated from the model and the model can be simplified. In addition, since it is possible to separately consider a noise source and leakage paths, noise countermeasures can be designed particularly and appropriatly. Besides, since circuits other than a linearly operating circuit are not modeled, it is expected that a preproduction cost is lowered and efficient design is realized.

2.6.1 Model Structure and Parameter Identification Method

Fig. 2.14 is a diagrammatic illustration of a DC-DC converter. Here, a circuit for realizing the basic function of the DC-DC, a switching device and a voltage stabilizing circuits provided on the input and output side, were targeted for modeling.

A model used here have also equivalent source elements representing the high-frequency currents generated by the nonlinear switching activity of the semiconductor devices and equivalent linear circuit elements representing the impedances of the EMI leakage paths as similar sa the previously reported models [7–11,13,15]. Fig. 2.15 shows the noise source equivalent circuit model. $\dot{I}_{s1}$ and $\dot{I}_{s3}$ are the equivalent current sources representing the high-frequency current generated by an EUT semiconductor devices. $\dot{Z}_1$, $\dot{Z}_2$, $\dot{Z}_3$ are the

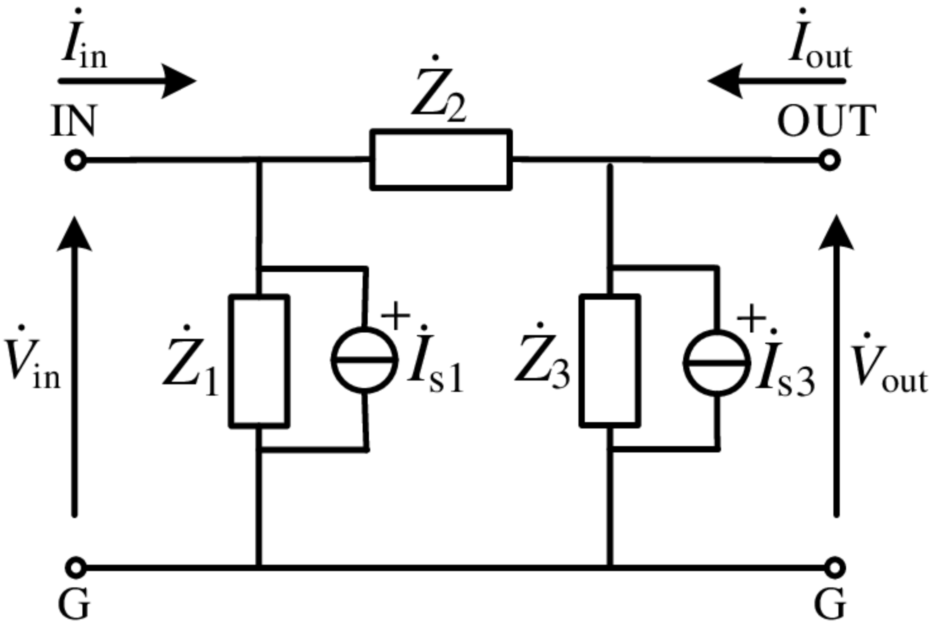


Figure 2.15 Two-port noise source equivalent circuit model for DC-DC converter.

equivalent impedance for the normal mode impedance of the EUT. To predict leakage of conducted disturbance to the input and output ports of DC-DC converter, this model has two ports. This model consists of three equivalent impedances and two equivalent current sources. In [47, 48], the minimum number of elements of the equivalent circuit model having n terminals is demonstrated as

$$n_{\mathrm{Z}} = \frac{n(n-1)}{2} \tag{2.7}$$

and

$$n_{\mathrm{Is}} = n - 1. \tag{2.8}$$

where, n_{Z} is the minimum number of equivalent impedance and n_{Is} is the minimum number of equivalent current source. For 3-terminal circuits, n is 3, that is, n_{Z} and n_{Is} are 3 and 2, respectively.

The model parameters are identified from circuit equations. When the input current $\dot{I}_{\mathrm{inin}}$, output current $\dot{I}_{\mathrm{outout}}$, input voltage $\dot{V}_{\mathrm{in}}$ and output voltage $\dot{V}_{\mathrm{out}}$ are defined in the direction of Fig. 2.15, the circuit equations are given by

$$\begin{bmatrix} \dot{I}_{\mathrm{inin}} \\ \dot{I}_{\mathrm{outout}} \end{bmatrix} = \begin{bmatrix} \dot{V}_{\mathrm{in}} & \dot{V}_{\mathrm{in}} - \dot{V}_{\mathrm{out}} & 0 & -1 & 0 \\ 0 & \dot{V}_{\mathrm{out}} - \dot{V}_{\mathrm{in}} & \dot{V}_{\mathrm{out}} & 0 & -1 \end{bmatrix} \begin{bmatrix} \dot{Z}_1^{-1} \\ \dot{Z}_2^{-1} \\ \dot{Z}_3^{-1} \\ \dot{I}_{\mathrm{s1}} \\ \dot{I}_{\mathrm{s3}} \end{bmatrix}. \tag{2.9}$$

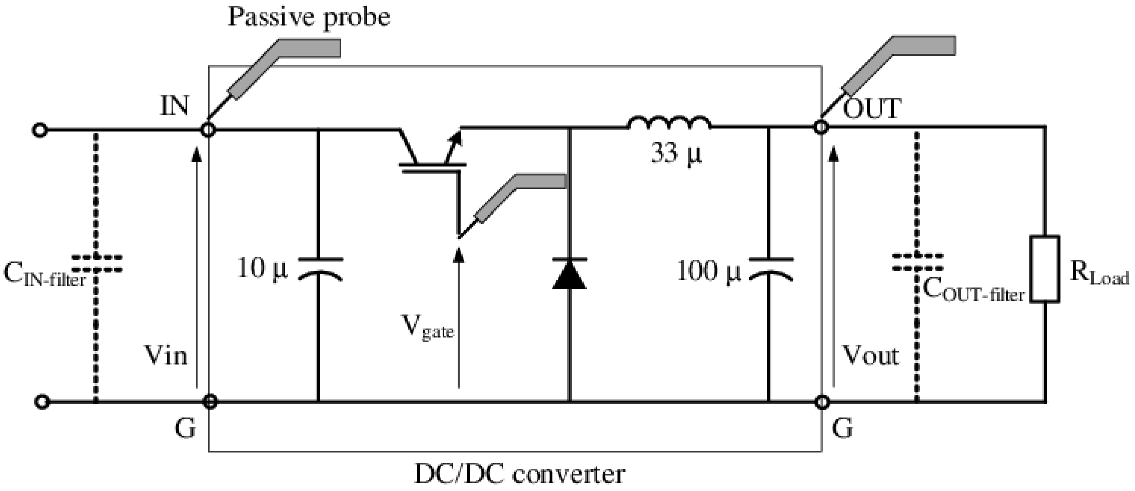


Figure 2.16 DC-DC converter evaluation board and measurement points of conducted disturbance.

As mentioned in Section 2.3, the minimum number of measurements $n_{\min}$ required is the smallest positive integer satisfying $n_{\min} \geq$ (number of parameters) / (number of circuit equations). Here, since the number of unknowns is five ($\dot{Z}_1$, $\dot{Z}_2$, $\dot{Z}_3$, $\dot{I}_{s1}$ and $\dot{I}_{s3}$) and the number of equations is two, $n_{\min}$ is three.

The linear equations obtained from the multiple measurements must be linearly independent, so a circuit condition is changed for each measurement to obtain measurement data unique to each measurement. In addition, it is not preferable to change circuit operation such as duty ratio and switching frequency in the multiple measurements. Therefore, in this study, the circuit condition was changed by using capacitance of EMI filters provided for input and output of the converter. In [44,45], the circuit condition was changed by using the road resistor R_{Load}; however, since the duty ratio varied due to R_{Load}, the method for changing the circuit condition was changed from the load resistor to the input and output EMI filters.

2.6.2 Parameter Identification

An evaluation board (BD9G341EFJ-EVK-101, ROHM) was used as EUT. Fig. 2.16 shows a circuit of the evaluation board. This board have a DC-DC converter with step-down from 12–76 V to 5 V by pulse width modulation (PWM). The converter operates at 200 kHz. In this study, the load resistance R_{Load} of 10 Ω was used. $C_{\text{IN-filter}}$ and $C_{\text{OUT-filter}}$ are EMI filters. Measurement points of conducted disturbance ($\dot{V}_{\text{in}}$ and $\dot{V}_{\text{out}}$) and a trigger signal (V_{gate}) are shown in Fig. 2.16 V_{gate} was used for averaging and data processing.

The DC-DC converter used as an EUT and specifications of system for measuring conducted disturbance are shown in Table 2.4. The configuration of system for measuring

Table 2.4 Specifications of System for Measuring Conducted Disturbance.

Component	Specifications
DC-DC converter	BD9G341EFJ-EVK-101, ROHM
Input voltage	12–76 V
Output voltage	5 V
Clock	200 kHz
Oscilloscope	DSO-S 104A, Agilent Technologies
Sampling rate	1 GS/s
Frequency band	1 GHz
Averaging	1024
DC power supply	PW18-1.8AQ, TEXIO
Output voltage	12 V
Impedance stabilization network	Custom made Described in Appendix A.
Passive probe	1160A, Keysight Technologies
Frequency band	500 MHz

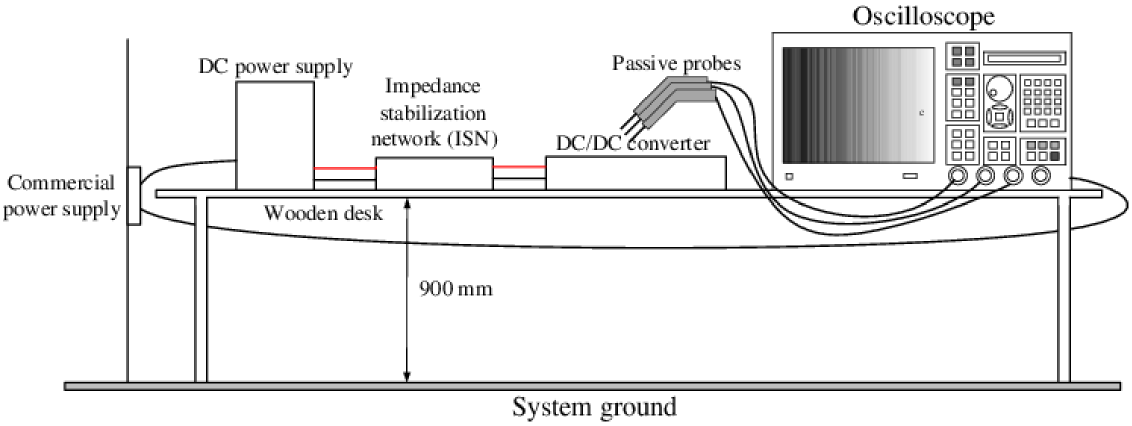


Figure 2.17 Configuration of system for measuring conducted disturbance.

conducted disturbance is shown in Fig. 2.17. To minimize the common-mode coupling, the height between the EUT and the system ground was set to 900 mm. The power supply to the DC-DC was supplied from a DC power supply (PW18-1.8AQ, TEXIO) via an Impedance stabilization network (ISN). The ISN was made to keep that the input impedance looking leftward from the DC-DC converter is constant. The details of the ISN are shown in A. The conducted disturbance voltages ($\dot{V}_{\text{in}}$ and $\dot{V}_{\text{out}}$) were measured by the oscilloscope (DSO-S 104A, Agilent Technologies) at the measurement points shown in Fig. 2.16. The conducted disturbance currents ($\dot{I}_{\text{inin}}$ and $\dot{I}_{\text{outout}}$) were calculated using

Table 2.5 Measurement Conditions and EMI filter Characteristics.

	Capacitor characteristics	
Condition	$C_{\mathrm{IN-filter}}$ (μF)	$C_{\mathrm{OUT-filter}}$ (nH)
w/o filters for modeling	N/A	N/A
w/ filters C for modeling	20	20
w/ filters D for modeling	40	40
w/ filters E for evaluation	10	10

the input impedance of the ISN $\dot{Z}_{\mathrm{IN\_ISN}}$ and the load resistance R_{Load}, respectively.

$$\dot{I}_{\mathrm{inin}} = -\frac{\dot{V}_{\mathrm{in}}}{\dot{Z}_{\mathrm{IN\_ISN}}} \tag{2.10}$$

$$\dot{I}_{\mathrm{outout}} = -\frac{\dot{V}_{\mathrm{out}}}{R_{\mathrm{Load}}} \tag{2.11}$$

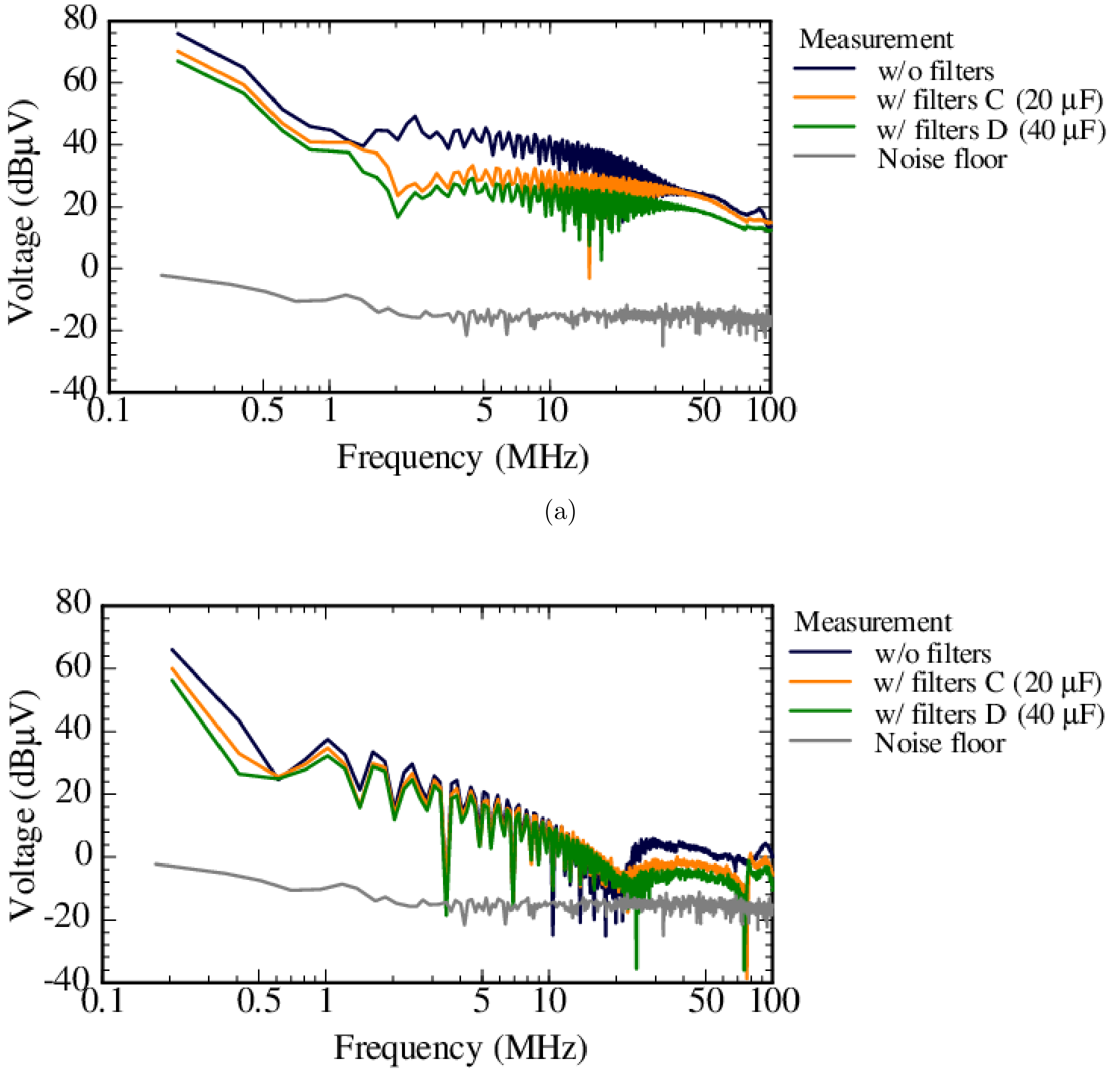
The number of averaging was set to 1024 for accurately measuring the conducted disturbance and modeling.

For increasing the circuit equations, the circuit condition was changed by using capacitance of EMI filters provided for input and output of the converter shown in Fig. 2.16. The used capacitance are shown in Table 2.5. For identifing model parameters, three conditions were used: without filters, with filters C of 20 μF, and with filters D of 40 μF. Each capacitance was chosen to change the voltage due to capacitance change. For evaluating model, one condition was used: with filters E of10 μF. The measured $\dot{V}_{\mathrm{in}}$ and $\dot{V}_{\mathrm{out}}$ are shown in Fig. 2.18. Both the voltages differed depending on the circuit conditions. The model parameters were identified from the measured conducted disturbance and the circuit equations.

2.6.3 Conducted Disturbance Voltage Simulation

The conducted disturbance voltages with filters E were simulated by a circuit simulater (Microwave office, AWR) and compared with the measured that. The simulation circuit contained the ISN, the identified model, and the load resistor. The simulated voltages ($\dot{V}_{\mathrm{in}}$ and $\dot{V}_{\mathrm{out}}$) are shown in Fig. 2.19.

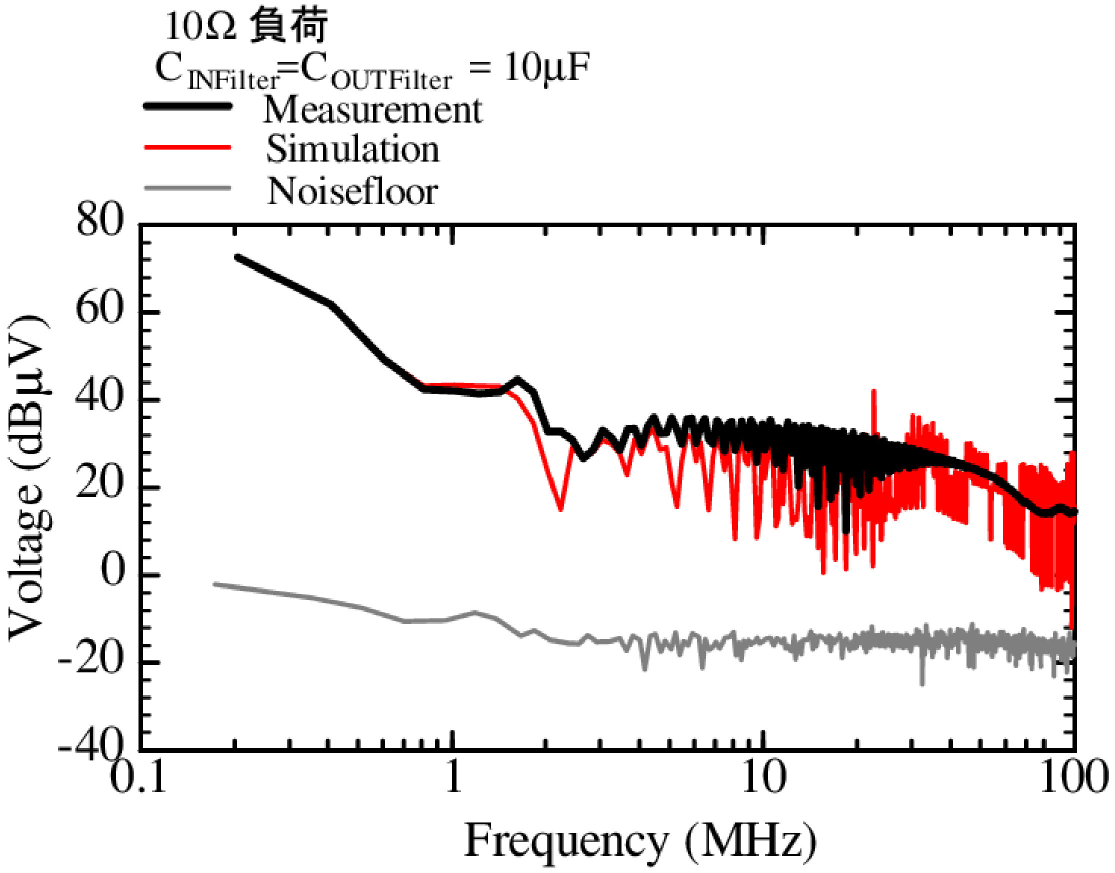
In Fig. 2.19(a), $\dot{V}_{\mathrm{in}}$ was predicted with high accuracy at frequiencies up to 10 MHz. The prediction accuracy deteriorated from 10 MHz to 100 MHz, but $\dot{V}_{\mathrm{in}}$ was predicted with an error within 20 dB. In Fig. 2.18(a), at frequencies up to 100 MHz, the difference between the noise floor and the voltage levels under the three conditions exceeded 30



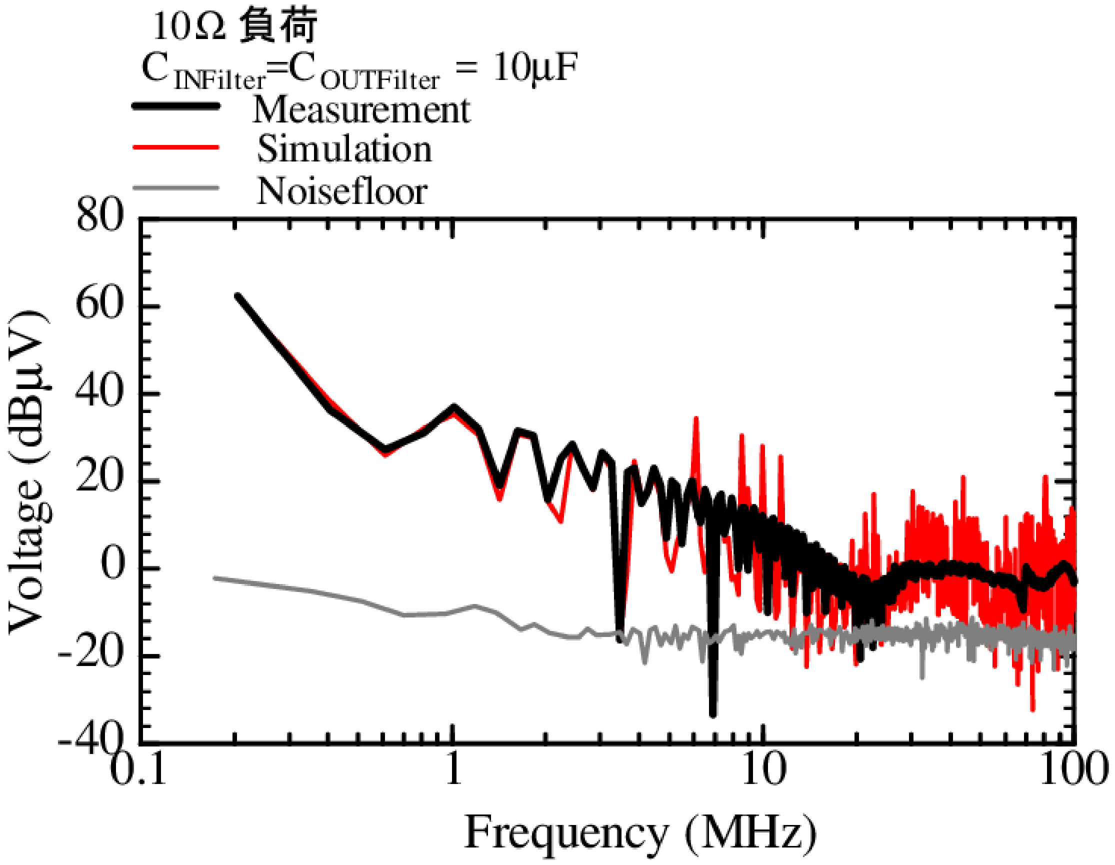
(a)

(b)

Figure 2.18 Spectral envelopes of measured voltage under three conditions (without filters, with filters C, and with filters D): (a) $\dot{V}_{\text{in}}$ and (b) $\dot{V}_{\text{out}}$.



(a)



(b)

Figure 2.19: Spectral envelopes of simulated voltages with filter E. (a) $\dot{V}$ and (b) $\dot{V}$

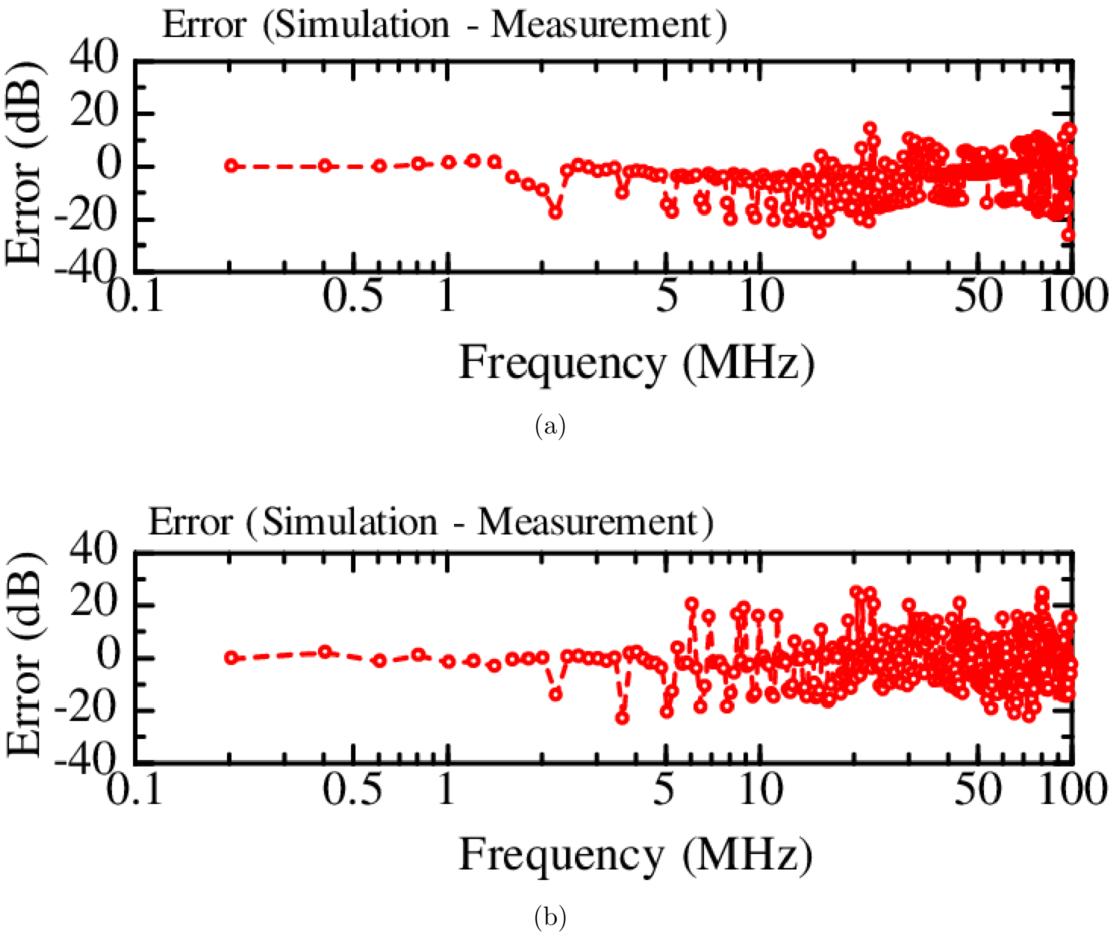


Figure 2.20 Errors of spectral envelopes with filters E: (a) $\dot{V}_{\text{in}}$ and (b) $\dot{V}_{\text{out}}$.

dB at most frequencies. The previous section concluded that the measurement accuracy required for modeling is approximately 10 dB. We thus inferred that the high prediction accuracy of $\dot{V}_{\text{in}}$ was due to good measurement accuracy.

In Fig. 2.19(b), $\dot{V}_{\text{out}}$ was predicted with high accuracy at frequencies from 200 kHz to 10 MHz. However, the prediction accuracy decreased at frequencies over 10 MHz, and an error within 30 dB was observed. In Fig. 2.18(b), the difference between the noise floor and the voltage levels under three conditions were less than 10 dB at frequencies over 10 MHz. The frequency at which the prediction accuracy deteriorated and the frequency at which the measurement accuracy decreased below 10 dB were consistent. Following the previous section conclusion, it is inferred that the prediction accuracy deterioration at frequencies over 10 MHz was due to insufficient measurement accuracy.

Altogether, the conduction disturbance was accurately predicted by our model. The two results mentioned in this chapter suggest the effectiveness of our noise source equivalent circuit modeling and the applicability to other circuits.

2.7 Conclusion

We have presented a noise source equivalent circuit model for predicting conducted disturbances to enable efficient design of EMI filters. The model has two basic elements: equivalent sources and equivalent impedances representing respectively high-frequency currents generated by switching devices and current leakage paths. We have also presented a model parameter identification method that uses only the measured voltage and current to avoid the workload required to perform measurements using a vector network analyzer or simulation using an electromagnetic field analysis simulator. Our model parameter identification method overcomes two problems: 1) the measurement data used for model parameter identification is not linearly independent and 2) part of the current is not represented due to a balanced bridge circuit formed by the model impedance and the measurement system impedance.

We applied the noise source equivalent circuit model to a tabletop IH cooker containing a general power converter circuit and evaluated the errors in the conducted disturbance voltages by using simulation. Although the magnitude of the errors depended on the accuracy of the measured voltage and current, the conducted disturbance voltage was predicted with an error of 6 dB or less when the measured voltage and current levels were more than 10 dB above the noise floor. Besides, we applied the model to a general DC-DC converter and evaluated the errors in the conducted disturbance voltages. As a result, the conducted disturbance was also predicted accurately. These suggest that conducted disturbance voltages can be predicted with practical accuracy using the proposed model and method, meaning that they are useful for designing EMI filters.

Chapter 3

Side-channel Attack Resistance Estimation for Improvement of HWS Performance Evaluation

3.1 Introduction

SCAs that illegally decipher secret information from cryptographic equipment by exploiting EM radiation/emanation are a realistic threat . These attacks are based on information gained from the implementation of a cryptgraphic system, rather than from mathematical weaknesses in the implemented algorithm itself. Some SCAs require technical knowledge of the cryptographic system, although others such as DPA [2] are especially effective as black-box attacks. Although SCAs are a powerful, if a cryptographic device is protected by countermeasures, it can induce a high attack cost, so designing such countermeasures is very important. Efficient design of countermeasures requires a method to predict SCA resistance at an early stage of the design process.

For establishing efficient SCA resistance estimation, this chapter proposed two methods: a SNR measurement method for realizing an SCA resistance evaluation method based on the SNR of side-channel traces and a side-channel trace simulation method using an EDA tool. These methods are the prior examinations for establishing a SNR simulation method. There is a problem that the results of the existing SCA resistance evaluation can not be fed back to the electric circuit design because the existing evaluation criteria are different from the circuit design criteria. To solve this problem, this work focus on the SNR which is applicable to both criteria of the SCA resistance evaluation and the circuit design. The simulation method used here is a method to predict the side channel trace at high-speed by narrowing down design information used in the prediction. If the SNR-based evaluation is possible and the SNR and existing evaluation criteria are calculated by side-channel simulation, the SCA resistance prediction and countermeasure design target determination are possible at the initial design process. The backgrounds of each study are described as follows.

Firstly, the SCA resistance evaluation is described. An efficient SCA resistance evaluation method is required for designing countermeasures because the typical evaluation methods have several issues. In the measurement to disclosure (MTD) [16] which analyzes a number of side-channel traces required for the key decryption and correlation power analysis (CPA) [17] which determines the correct secret-key for all the possible key hypothesis, the cost of SCA resistance evaluation increases due to an improvement in vulnerability by countermeasures. Besides, since the outputs of MTD and CPA are not a value generally used for electric circuit design, it is difficult to provide feedback to the countermeasure design. In Welch's t-test established in ISO/IEC17825 [18] which determines the possibility of information leakage by statistical processing, the cost of evaluation does not increase with countermeasures; however, it is difficult to provide the feedback for the same reason as MTD.

A purpose of this work is providing a SCA resistance evaluation method that can associate the evaluation result with design criteria of countermeasure circuits. This method uses a signal-to-noise ratio (SNR) of side-channel traces as a criterion because of two reasons. The first one is that the correlation coefficient and the number of trace needed for key decryption which are commonly used as SCA resistance criteria can be predicted from the SNR. The second one is that the SNR is commonly used as a design criterion in electric circuit design. That is, if the SNR and the correlation coefficients can be accurately calculated, the SNR can be used for both the determination of countermeasure design targets and evaluation of the SCA resistance. The relationship between the SNR and the correlation coefficients was analytically derived [20]. Moreover, the relationship between the number of traces needed for key decryption and the correlation coefficient was derived using a hypothesis test [21, 49]. These mean that, if the SNR and the correlation coefficients can be accurately calculated, the SNR can be used as SCA resistance design targets.

This work has experimentally verified whether measured SNRs and correlation coefficients satisfy the analytical relationship [20]. Here, a method to measure the SNR accurately is proposed for experimental verification. The SNR was calculated using a signal component obtained from the trace when encrypting a random plaintext set and a noise component obtained from the trace when encrypting a constant plaintext set, and the correlation coefficient was calculated based on the CPA. A PCB having an FPGA implemented an AES circuit was used as an EUT, and the core power supply voltage fluctuation of the FPGA on the PCB was measured as side-channel trace. The SNR was varied by changing measurement conditions, measurement system, and EUTs, and the relationship was examined.

Secondly, the side-channel trace simulation is described. SCA resistance can be estimated by simulating side-channel traces such as power supply voltage fluctuations while a device operates. Several side-channle trace simulation methods have been proposed [22–27, 30]. The traces are estimated from a device's internal dynamic current and the characteristics of its power distribution network (PDN). These methods [22–27, 30] simulate the dynamic current only from hardware design information. While the dynamic current can also be obtained through on-die measurements [28,29], such current measurement is impractical in most designs, so this thesis does not describe that approach in more detail.

Physical device level simulation methods using SPICE have also been proposed [22, 23,30]. In these simulations, the dynamic current during encryption is calculated via side-channel traces by using a dump file, along with the CMOS circuits inside the cryptographic device or their equivalent circuit models. The dump file is obtained by recording all data transitions of circuits in the device, such as resistors and flip-flops at a certain moment, in their entirety. Because these simulations can represent the physical characteristics of a device (e.g., wiring delays due to circuit placement and routing, unbalanced circuits caused by wiring is coupling, etc.), they can simulate current fluctuations including the effects of physical phenomena. This approch requires technical knowledge of the cryptographic device in terms of the CMOS circuits and circuit models. General-purpose devices, such as field programmable gate arrays (FPGAs) and microcontrollers, have become popular as cryptographic devices. Unfortunately, engineers can not generally obtain physical information about these devices, which is confidential information held by the device vendors. That is, these simulation methods are limited to use with dedicated devices such as application specific integrated circuits (ASICs).

Hence, for estimating side-channel traces generated by general-purpose devices, a gate level simulation method has been investigated [27]. Moreover, in the field of EMC, several gate level simulation methods have been proposed [24–26]. In all of these approaches, the dynamic current is calculated using a device's electrical characteristics and a dump file generated by the power consumption analyzer of an electronic design automation (EDA) tool. The device characteristics are already known by the EDA tool, and the dump file is genarated by the timing analyzer. In other words, engineers do not have to be aware of the device characteristics, and analysis tools other than the EDA tool are unnecessary for dynamic current simulation. This is an advantage over physical device-level simulation methods. The calculation costs of those methods are high, however, and they are not suitable for use in the early design process. In addition, to generate the dump file, those methods also require a configuration file obtained by logic synthesis from a hardware description language (HDL) file. Because the configuration file includes detailed design information such as propagation delays, it is possible to simulate current accurately, but the cost increases further.

To decrease the simulation cost, we focus on register-transfer level (RTL) simulation. In this type of simulation, the dynamic current may not be predicted as precisely as with gate-level simulation, because an HDL file before logic synthesis, which includes no detailed design information, is input into the analyzer. The reason for using the HDL file is that detailed design information such as propagation delays may be unnecessary for estimating SCA resistance at the early stage of the design process, and high-speed SCA resistance simulation is expected to be achievable by RTL simulation, in which such information is not considered. In [31, 32], it was reported that the frequency spectrum around the clock frequency and below contains a large amount of side-channel information. Therefore, it is inferred that analysis at high frequencies is not required. This suggests that most of the side-channel information can be predicted with a time resolution the same as the clock period, meaning that detailed design information may be unnecessary.

In this paper, we examine dynamic current prediction based on RTL simulation and show that the predicted dynamic current contains side-channel information equivalent to that of measured dynamic current. A printed circuit board (PCB) with an FPGA implementing an advanced encryption standard (AES) circuit was used as the equipment under test (EUT). Although the dynamic current inside the FPGA can be predicted, it cannot be measured directly. Therefore, we converted the measured core power supply voltage fluctuation to the dynamic current of the FPGA by using the impedance characteristics of the PCB including the FPGA [50, 51]. To evaluate this simulation method, we compared the predicted current with the measured and calculated current. The paper assumes an SCA attack scenario of correlation power analysis (CPA) [17], in which the hamming distance (HD) model in terms of all 16 bytes of two intermediate values in the AES encryption process was used as a side-channel information leakage model, and we thus compared CPA results. In addition, for evaluation from another point of view, we compared measurement to disclosure (MTD) [16] results.

This work has proposed a side-channel trace simulation method using EDA tools and has investigated whether the estimated traces have the side-channel information. Here, the current consumption of a cryptographic device during encryption is calculated as the side-channel traces. The current is estimated only from the damp file, which is generated by register transfer level (RTL) simulation, using a power consumption analyzing function of an EDA tool. Since detailed design information such as propagation delay is not included in the dump file generated here, the calculation cost is reduced as compared with the existing methods [22–27]. The fluctuations of the current with respect to the random plaintext set were estimated and compared with the measured one.

The rest of this chapter is organized as follows. Section 3.2 introduces existing SCA resistance estimation methods and an objective of this research. Section 3.3 introduces the SNR in side-channel analysis. Here, the definition of SNR, the relationships between the SNR and the common SCA resistance criteria, and the SNR measurement method are described. Section 3.4 shows experimental verification of the analytical relationship between the SNR and correlation coefficients. Section 3.5 introduces the side-channel trace estimation based on RTL simulation and the method for converting from measured side-channel traces to dynamic current. Section 3.6 evaluates the dynamic current simulated via side-channel traces by comparing it with the converted current obtained from measured traces. The simulated current is also evaluated in terms of CPA and MTD. Finally, Section 3.7 concludes this chapter with a summary of the key points.

3.2 Existing SCA Resistance Estimation Methods

Side-channel attacks (SCAs) that illegally deciphers secret information of cryptographic equipment exploiting electromagnetic (EM) radiation/emanation has been a realistic threat. SCAs are attacks based on information gained from the implementation of a cryptgraphic system, rather than mathematical weaknesses in the implemented algorithm itself. Some SCAs require technical knowledge of the cryptographic system, although others such as differential power analysis (DPA) [2] are especially effective as black-box attacks. Though SCAs are a powerful, if the cryptographic devices are protected by countermeasures, SCAs can require attackers a lot of attack cost, thus, designing countermeasures are highly important.

In HWS design in IoT era, it is required that not only superior countermeasures but also efficient countermeasure design methods. The efficient design achieving (A) described in Section 1.2 is provided by a signal-to-noise ratio (SNR) of side-channel trace (a general term for a trace including confidential information such as voltage, current, EMI, etc. during cryptographic processing) simulation method. Therefore, the ultimate objective of this work is establishing the SNR simulation method. As preparation stages for achieving the objective, there are two tasks:

- establishing an SCA resistance evaluation method using signal-to-noise ratio (SNR) and
- establishing an efficient side-channel trace simulation method.

The reason why the above two tasks are necessary is explained below.

There is a problem that the results of the existing SCA resistance evaluation can not be fed back to the electric circuit design because the existing evaluation criteria are different from the circuit design criteria. To solve this problem, this work focus on the SNR which is applicable to both criteria of the SCA resistance evaluation and the circuit design. The simulation method used here is a method to predict the side channel trace at high-speed by narrowing down design information used in the prediction. If the SNR-based evaluation is possible and the SNR and existing evaluation criteria are calculated by side-channel simulation, the SCA resistance prediction and countermeasure design target determination are possible at the initial design process. The details of issues for exsisting study are described as follows. Details of the investigation is described in Chapter 3.

Firstly, issues of the existing evaluation methods for SCA resistance evaluation are explained. Features of existing methods are shown in Table 3.1. The SCA resistance evaluation are divided into two types: actual attack evaluation and non-attack evaluation.

In the actual attack evaluation, the attack cost and the ease of attack are calculated by continuing attacks equivalent to ones used by actual attackers until the confidential information (i.e. plaintext and secret-key) is analyzed [16, 17]. The outputs of this evaluation are the number oftraces needed for secret-key disclosure which representing the attack cost and the correlation coefficient which representing the ease of attack. These outputs are important for evaluating SCA resistance performance because the resistance is estimated quantitatively and directly by them. This evaluation is widely used due to high reliability of the outputs, however, there are two issues in this evaluation. The first one is that the evaluation cost increases with the SCA countermeasure level. The second one is that feeding back the evaluation result to the countermeasure design is difficult because the outputs can not be used for designing electric circuits and ICs.

For preventing the increase in the evaluation cost in the actual attack evaluation, two non-attack evaluation methods are proposed. A method using t-test is the one of them. This method evaluates the SCA resistance by checking whether side-channel trace changes depending on the confidential information by statistical hypothesis testing based on Welch's t-test, and is established in ISO/IEC17825 [18]. The evaluation cost is kept down because the confidential information analysis is unnecessary and the number of traces needed for t-testing does not depend on SCA countermeasure level. However, this method has two issues. The first one is that the SCA resistance performance is estimated indirectly because it is only judged whether the confidential information is leak or not. whether the confidential information is leak or not. The second one is that feeding back the evaluation result to the contermeasure design is difficult as same reason as the second one of the actual attack evaluation.

Another non-attack evaluation method using signal-to-noise ratio (SNR) [19, 20] has been examined to solve the above issues. This method evaluates the SCA resistance by calculating SNR of side-channel traces. It is assumed that obtaining the SNR by separating the traces into a signal component containing the confidential information and a noise component containing no confidential information. The SNR represents amount of the information leakage quantitatively, moreover, the SNR is compatible with the outputs of the actual attack evaluation. Therefore, the SCA resistance performance is estimated quantitatively and directly. Besides, the evaluation cost is kept down because the confidential information analysis is unnecessary and the number of traces needed for calculating the SNR does not depend on SCA countermeasure level. It is notable that the SNR is widely used as a design criterion of electric circuits and ICs. This means that feeding back a result of the SNR evaluation to the countermeasure design is easy.

In previous studies on the SNR evaluation [21], the relationships between the SNR and the number of traces needed for secret-key disclosure or the correlation coefficient is analytically derived. However, a method for extracting the SNR from side-channel traces has not been established. One of tasks for the objective of this work is that establishing a method for extracting the SNR from side-channel traces. The definition of SNR of side-channel traces, the relationships between the SNR and the actual attack evaluation criteria, a measurement method of SNR we proposed, and an experimental examination are described in Section 3.3 and 3.4.

Table 3.1 Features of existing methods for SCA resistance evaluation

	Actual attacks	Non-attacks	
		t-test [18]	Signal-to-noise ratio [19, 20]
Evaluation approch	Calculating the attack cost and the ease of attack by continuing attacks equivalent to ones actually used by attackers until the confidential information (i.e. plaintext and secret-key) is analyzed.	Checking whether side-channel trace changes depending on the confidential information by statistical hypothesis testing.	Calculating signal-to-noise ratio of side-channel traces by separating the traces into a signal component containing confidential information and a noise component containing no confidential information.
Output	The number of traces needed for secret-key disclosure, the correlation coefficient	Presence or absence of the information leakage	Amount of the information leakage
Reliability of output	**High** (SCA resistance performance is estimated quantitatively and directly.)	**Low** (The output of this method is incompatible with the one of actual attack evaluation. SCA resistance performance is estimated indirectly.)	**High** (The SNR is compatible with the outputs of actual attack evaluation [21], thus, the outputs are calculated from SNR. Therefore, the SCA resistance performance is estimated quantitatively and directly.)
Evaluation cost	**High** (The evaluation cost increases with the SCA countermeasure level.)	**Low** (The number of traces needed for t-testing does not increase with the SCA countermeasure level because the confidential information analysis is unnecessary.)	
Feedback to design	**Difficult** (The outputs can not be used for designing electric circuits and ICs.)		**Easy** (SNR is widely used as a design criterion of electric circuits and ICs.)

Secondly, issues of the existing side-channel trace simulation methods are explained. Several simulation methods for simulating power supply voltage fluctuations of ICs in operation have been proposed [22–27]. All of the methods shown here are methods for simulating the fluctuation of device internal dynamic current only from the HW design information by electronic design automation (EDA) tools. While the dynamic current can also be found through on-die measurements [28, 29], measuring current is impractical in most designs, thus, in this thesis does not described them in more details. Features of existing methods are shown in Table 3.2.

The physical device level simulation methods using SPICE has been proposed [22, 23, 30]. In these simulations, the current consumption during encryption is calculated using a dump file, which is all data transitions of circuits in a device such as resisters and flip-flops at a certain moment are recorded in its entirety, and CMOS circuits inside a cryptographic device or circuit models equivalent to the CMOS circuits. These simulations can represent the physical characteristics of a device (e.g. wiring delay in the whole cryptographic circuit occurring at the time of circuit placement and routing, unbalance of the circuit when the wiring is coupled, etc.), thus, analyzing the current fluctuation including the physical phenomenon is possible. However, these require technical knowledge of cryptographic devices because engineers can not obtain the physical information in general, while the dump file is generated by an EDA tool. Recently, general-purpose devices (such as FPGA and microcontroller) have become popular as cryptographic devices instead of dedicated devices (such as application specific integrated circuits (ASICs)). Unfortunately, the internal information of these devices is confidential of device vendors. In other words, these simulation methods are limited to application to dedicated devices, and a method for general-purpose devices is required.

In the field of EMC, several logic level simulation methods are proposed for calculating the current consumption of general-purpose devices [24–26]. For estimating side-channel traces, simulation methods have been investigated [27]. The current consumption is calculated using the device electrical characteristics and the toggle rate by a power consumption analyzing function of an EDA tool. The device characteristics are owned by the EDA tool, and the toggle rate is determined by the EDA tool based on the dump file. In other words, engineers do not have to be aware of the device characteristics, and analysis tools other than the EDA tool are unnecessary in the current consumption simulation. Since this point is superior to the physical device level simulation methods, this thesis focuses on the logic level simulation using an EDA tool.

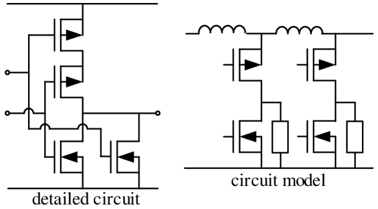
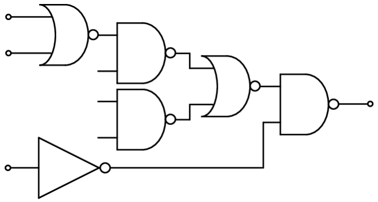
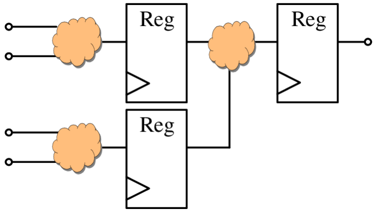
In [24–27], a power supply noise is simulated accurately for EMI or side-channel trace prediction. However, thier calculation costs are high. A configuration file obtained by logic synthesis from the HDL file is input to a timing simulator. Since the configuration file includes the detailed design information such as propagation delay, it is possible to simulate traces accurately, but the cost increases.

Therefore, for increasing in speed of simulation, this thesis proposes a side-channel trase simulation method which executes the RTL simulation by inputting the HDL file before logic synthesis. The reason of using the HDL file is that the detailed design information such as propagation delay may be unnecessary and high-speed side-channel simulation is expected by the RTL simulation in which the information is not taken into account. In [31, 32], it has been reported that frequency spectrum around the clock frequency have large side-channel information. Therefore, It is inferred that in the side-channel trace simulation, analysis at high frequency is not required as much as EMI prediction. This suggests that most of the side-channel information can be simulated with the time resolution as much as the clock period, that is, the detailed design information may be unnecessary.

Even though the current consumption is accurately calculated, it is unclarified whether the calculated current has the side-channel information. Therefore, this work investigated whether the calculated current has the side-channel trace information.

Another one of tasks for the purpose of this thesis is that investigating whether the calculated current has the side-channel trace information. Details of this investigation are described in Section 3.5 and 3.6.

Table 3.2 Features of existing methods for side-channel trace simulation

	Physical device level [22, 23, 30]	Gate level [24–27]	RTL level (Used in proposed method)
			
Procedure	**I**. Create a dump file by an EDA tool. **II**. Create a device level simulation circuit from the physical characteristics of a cryptographic device. **III**. Calculate current consumption by SPICE.	**I**. Create a dump file including the detailed design information by an EDA tool. **II**. Calculate dynamic current by a power analyzing function of EDA tool.	**I**. Create a dump file excluding the detailed information by an EDA tool. **II**. Calculate dynamic current by a power analyzing function of EDA tool.
Difficulty	**Difficult** (In procedure **II**, CMOS circuits inside a cryptographic device or circuit models are needed.)	**Easy** (Files other than the dump file are unnecessary. The device characteristics are also unnecessary.)	
Simulation Accuracy	**High** (Procedure **III** analyzes the current fluctuation including the physical phenomenon.)	**Enough** (A power supply noise is simulated accurately for side-channel trace prediction.)	
Simulation cost	**Very High** (Generally, a huge amount of calculation cost is necessary.)	**High** (Since the simulation performed based on the detailed design information, calculating cost is high.)	**Low** ((Since the simulation performed based on the simple design information, calculating cost is low.)

3.3 SCA Resistance Prediction Based on SNR of Side-channel Traces

This section describes a SNR of side-channel trace measurement method. As a preliminary explanation, the definition of the SNR and the relationships between the SNR and existing evaluation criteria are described. Then, measurement method we proposed is described.

3.3.1 Definition of SNR of Side-channel Traces

The definition of SNR is described with an example using the power supply voltage of a cryptgraphic device as a side-channel trace. The voltage fluctuates with input data, operations in encryption/decryption process in the cryptographic circuit, and random noise superimposed on the measurement. The side-channel trace has three components: signal component V_{data} correlated with the power model and depending on the input data, noise component V_{op} uncorrelated with the power model and depending on the cryptographic operations, and random noise components V_{noise} independent on the data and the cryptographic operations. Considering AES-128 which processes all the 16 bytes of the data block simultaneously, V_{data} and V_{op} are depends on data and cryptographic operations in all the bytes. Since CPA is taken for the SCA scenario in this work, we here focus on voltage fluctuations of V_{data} and V_{noise} at an interesting moment with respect to plaintexts, input data for the cryptographic circuit. The SNR is defined as a ratio of variances of the signal and noise components at the interesting time. V_{op} has a constant value at the interesting time regardless change in data for all the measurements. The variance $\mathrm{Var}(V_{\mathrm{op}})$ can, therefore, be regarded to be zero. The SNR is, then, represented with the variance of V_{data} and V_{noise} as,

$$\mathrm{SNR} = \frac{\mathrm{Var}(V_{\mathrm{data}})}{\mathrm{Var}(V_{\mathrm{noise}})} \tag{3.1}$$

3.3.2 Prediction of Evaluation Criteria in Actual Attacks

The relationships between the SNR defined above and the two existing evaluation criteria, the correlation coefficient and the number of traces needed for secret-key disclosure, are analytically derived in []. In CPA, a correlation coefficient is calculated from a power model for a key-hypothesis and a set of measured side-channel traces. A relationship between the SNR and the correlation coefficient ρ is represented as,

$$\rho(V_{\mathrm{total}}, H_{\mathrm{i}}) = \frac{\rho(V_{\mathrm{data}}, H_{\mathrm{i}})}{\sqrt{1 + \frac{1}{\mathrm{SNR}}}} \tag{3.2}$$

where, H_{i} is the power model such as hamming distance (HD) or Hamming weight (HW) model, and V_{total} is the sum of V_{data} and V_{noise}. $\rho(V_{\mathrm{total}}, H_{\mathrm{i}})$ means a correlation coefficient between commonly measured traces and a power model, and $\rho(V_{\mathrm{data}}, H_{\mathrm{i}})$ means a correlation coefficient between the signal component extracted by a particular method and a power model. When a pair of ρ_1 and SNR_1 are obtained from the measured traces, ρ_2 for arbitrary SNR_2 at same time can be calculated by

$$\rho_2 = \rho_1 \frac{\sqrt{1 + \frac{1}{\mathrm{SNR}_1}}}{\sqrt{1 + \frac{1}{\mathrm{SNR}_2}}} \tag{3.3}$$

Correlation coefficients are also calculated with other power models for all the possible key hypothesis to declare the most-likely key hypothesis the secret key. The correct secret key is determined according to the correlation coefficients based on the nature that the correlation coefficient for the correct key hypothesis becomes significantly greater than those for wrong hypotheses. If a key hypothesis is wrong, the power model and the side-channel traces are uncorrelated, that is, the mean of the correlation coefficients is zero. By contrast, if a key hypothesis is correct, the mean of correlation coefficients ρ_{c} is $0 < |\rho_{\mathrm{c}}|1$. The number of traces needed for secret-key disclosure n_{r}, represents the number of traces necessary for determining a significant difference between zero and ρ_{c}, and is calculated by

$$n_{\mathrm{r}} = 3 + 8 \frac{z_{1-\alpha}^2}{\ln^2 \frac{1+\rho_{\mathrm{c}}}{1-\rho_{\mathrm{c}}}} \tag{3.4}$$

where, α is a confidence level and $z_{1-\alpha}$ is a value obtained from a percentage point of the normal distribution. It is expected that ρ and n_{r} are predicted for arbitrary SNR using (3.3) and (3.4).

All that remains is to establish a method to correctly acquire the SNR from side-channel traces for realizing the SCA resistance evaluation by SNR.

3.3.3 Proposed SNR Measurement Method

The traces measured with common way is composed of V_{data} and V_{noise}, and these two components are generally impossible to measure separately. To separate them, two plaintext configurations are used here:

- a constant plaintext and
- a varied plaintext set.

With the constant plaintext, $\mathrm{Var}(V_{\mathrm{data}})$ is zero because the variation with respect to the plaintexts does not occur, thus $\mathrm{Var}(V_{\mathrm{noise}})$ is extracted. With the varied plaintext set, $\mathrm{Var}(V_{\mathrm{data}} + V_{\mathrm{noise}})$ is observed.

Generally, it can be considered that V_{noise} is independent and identically distributed irrespective of data and encryption operations. Therefore, in side-channel trace acquisition, $\mathrm{Var}(V_{\mathrm{noise}})$ decreases with the number of averaging N_{avg} based on the law of large numbers. Altogether, $\mathrm{Var}(V_{\mathrm{data}})$ can be extracted from the measurement used the varied plaintext set with an enough N_{avg}.

In [], $\mathrm{Var}(V_{\mathrm{data}})$ was extracted with N_{avg} set to 50. However, excessive averaging which approximates $\mathrm{Var}(V_{\mathrm{noise}})$ to zero causes inefficiency of the evaluation. In this study, for reducing N_{avg}, $\mathrm{Var}(V_{\mathrm{data}})$ is extracted using the reproductive property of distribution. Here, $\mathrm{Var}(V_{\mathrm{data}})$ is calculated by

$$\mathrm{Var}(V_{\mathrm{data}}) = \mathrm{Var}(V_{\mathrm{data}} + V_{\mathrm{noise}}) - \mathrm{Var}(V_{\mathrm{data}}) \tag{3.5}$$

As a precondition for using (3.5), both traces ($V_{\mathrm{data}} + V_{\mathrm{noise}}$ and V_{noise}) have to be followed the normal distribution. Regarding that, it has been conformed that the traces measured with the enough N_{avg} are satisfied with the precondition.

3.4 Experimental Evaluation of Resistance Prediction Based on SNR

3.4.1 Application and Measurement System

For examining validity of the proposed SNR measurement method and the SCA resistance evaluation based on the SNR, this research used two PCBs as EUTs. The reason for using two EUTs is to check whether the examination results are depend on the EUTs. The features of the EUTs are shown in Table 3.3.

Table 3.3 EUTs used for examining validity of proposed SNR measurement method and SCA resistance evaluation based on SNR.

Component	Specifications	
	EUT-A	EUT-B
Cryptographic module	SENPU, AIST	SASEBO-G, AIST
FPGA	Cyclone V (5ECFA5F23), ALTERA	Virtex-II Pro (xc2vp7), Xilinx, for encryption Virtex-II Pro (xc2vp30), Xilinx, for control
Clock freq.	48 MHz	24 MHz
Implemented AES	Lookup-table based AES-128	Composite based AES-128

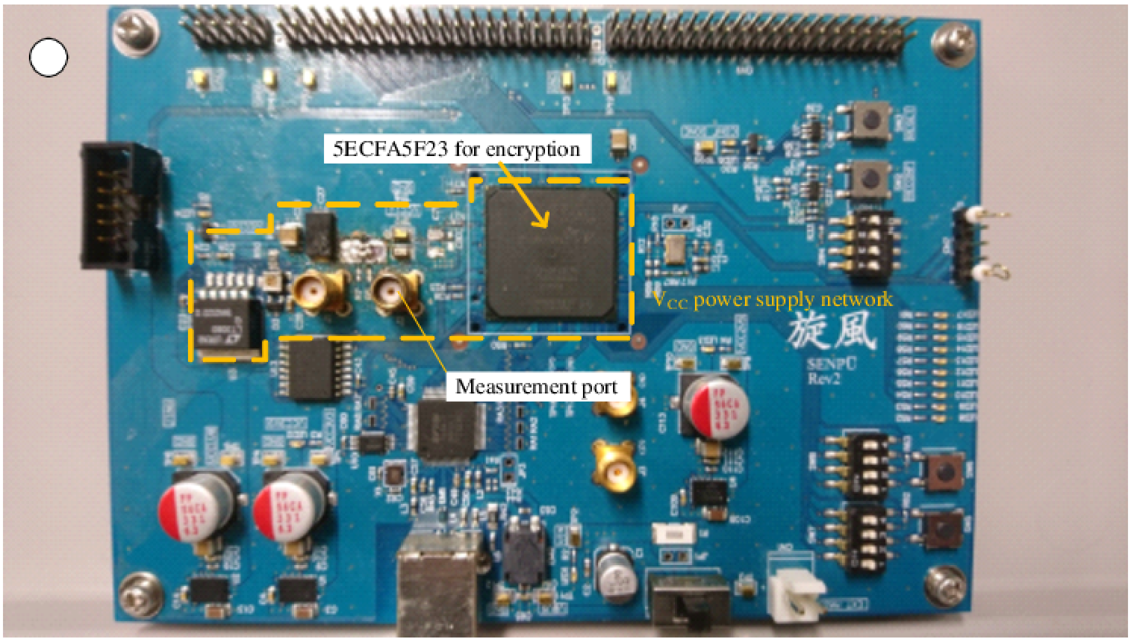
The PCB of EUT-A is SENPU which is one of the side-channel standard evaluation boards produced by National Institute of Advanced Industrial Science and Technology (AIST). An FPGA (Cyclone V, 5CEFA5F23, ALTERA) is implemented on SENPU for encryption. Fig. 3.1 shows the appearance of SENPU. The part indicated by the broken lines in Fig. 3.1(a) and Fig. 3.1(b) are the V_{cc} power supply network (PDN) including the FPGA. For measuring side-channel traces and measuring characteristics of the PCB, a SMA connector is mounted in the PDN. Although several decoupling capacitors are usually mounted on the back side fo the FPGA, in this research, they are unmounted for measuring V_{cc} accurately. A lookup-table based AES-128 circuit is implemented on the FPGA of EUT-A as an encryption circuit. This AES circuit was generated from Verilog-HDL files written in RTL level by a logic synthesis tool (Quartus Prime Lite Edition 15.1, Intel). For simulating and measuring side-channel traces accurately, this AES circuit is designed not to process other functions during encryption. Besides, this circuit operates with a clock of 48 MHz.

The PCB of EUT-B is SASEBO-G [] which is one of the side-channel standard evaluation boards produced by AIST and Tohoku University. SASEBO-G has two FPGAs: Virtex-II Pro (xc2vp7), Xilinx for encryption and Virtex-II Pro (xc2vp30), Xilinx for communication and control. Fig. 3.2 shows the appearance of SASEBO-G. The two FPGAs have independent dedicated GND and V_{cc} wiring and are designed so that each power consumption does not influence as much as possible. The part indicated by the broken lines in Fig. 3.2(a) and Fig. 3.2(b) are the V_{cc} power supply network including the encryption FPGA. As the same to EUT-A, though several decoupling capacitors are usually mounted on the back side fo the encryption FPGA, in this research, they are unmounted for measuring V_{cc} accurately. Furthermore, the 100 μF electrolytic capacitor mounted on the PDN was also removed. A composite based AES-128 circuit is implemented on the encryption FPGA of EUT-B as an encryption circuit. This AES circuit was generated from Verilog-HDL files written in 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.

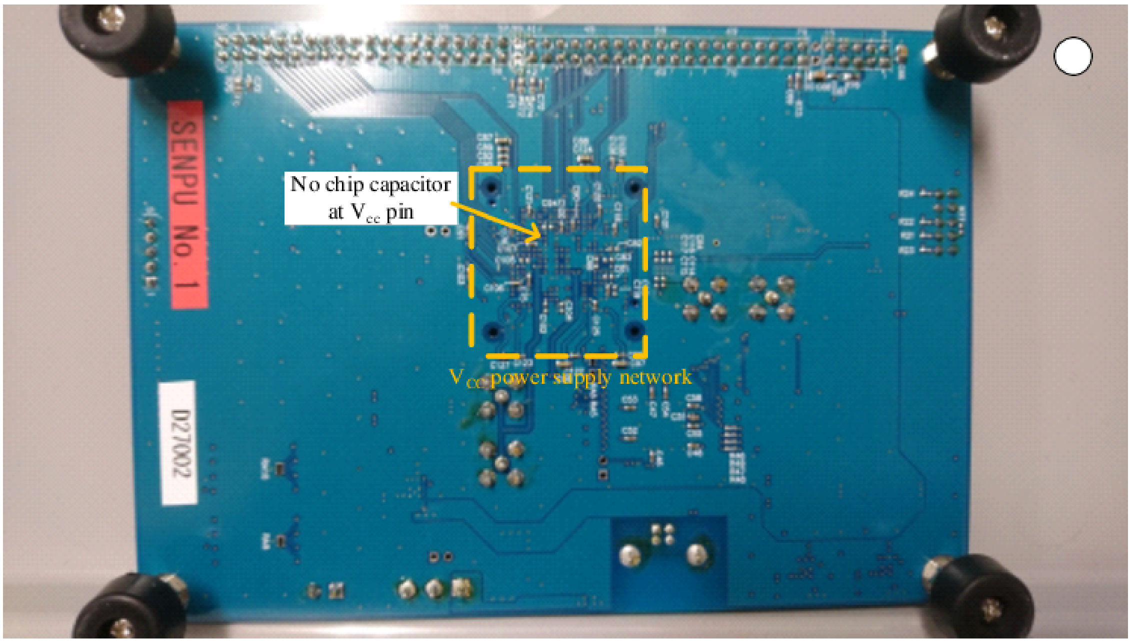
Then, the measurement system for each EUT is explained. The specifications of system for measuring SNR on EUT-A are shown in Table 3.4. V_{cc} fluctuation was measured by an oscilloscope (DSO-S 104A, KEYSIGHT Technologies) with two probes, power rail probe (N7020, KEYSIGHT Technologies) and a coaxial cable, at the SMA measurement port shown in Fig. 3.1(a). The reason why two probes were used is to observe the effect of measurement conditions. Simultaneously, several N_{avg} were used for changing the SNR and the correlation coefficient in each probe condition. The N_{avg} conditions are listed in Table 3.4.

The specifications of system for measuring SNR on EUT-B are shown in Table 3.5. V_{cc} fluctuation was measured by an oscilloscope (54845A, Agilent Technologies) with a passive probe (1161A, Agilent Technologies) at the measurement point shown in Fig. 3.2(a). Several N_{avg} were used for changing the SNR and the correlation coefficient. The N_{avg} conditions are listed in Table 3.5.

In both SNR measurement, common plaintext sets and secret-key were used. The common parameters are shown in Table. 3.6. For measuring $V_{\mathrm{data}} + V_{\mathrm{noise}}$, the varied plaintext set, all of the bits are changed to random, was used. For measuring V_{noise}, the constant plaintext, all of the bits are zero, was used. A secret-key (2B 7E 15 16 28 AE D2 A6 AB F7 15 88 09 CF 4F 3C)$_{16}$ was used. For both plaintext sets, 10000 traces were obtained.

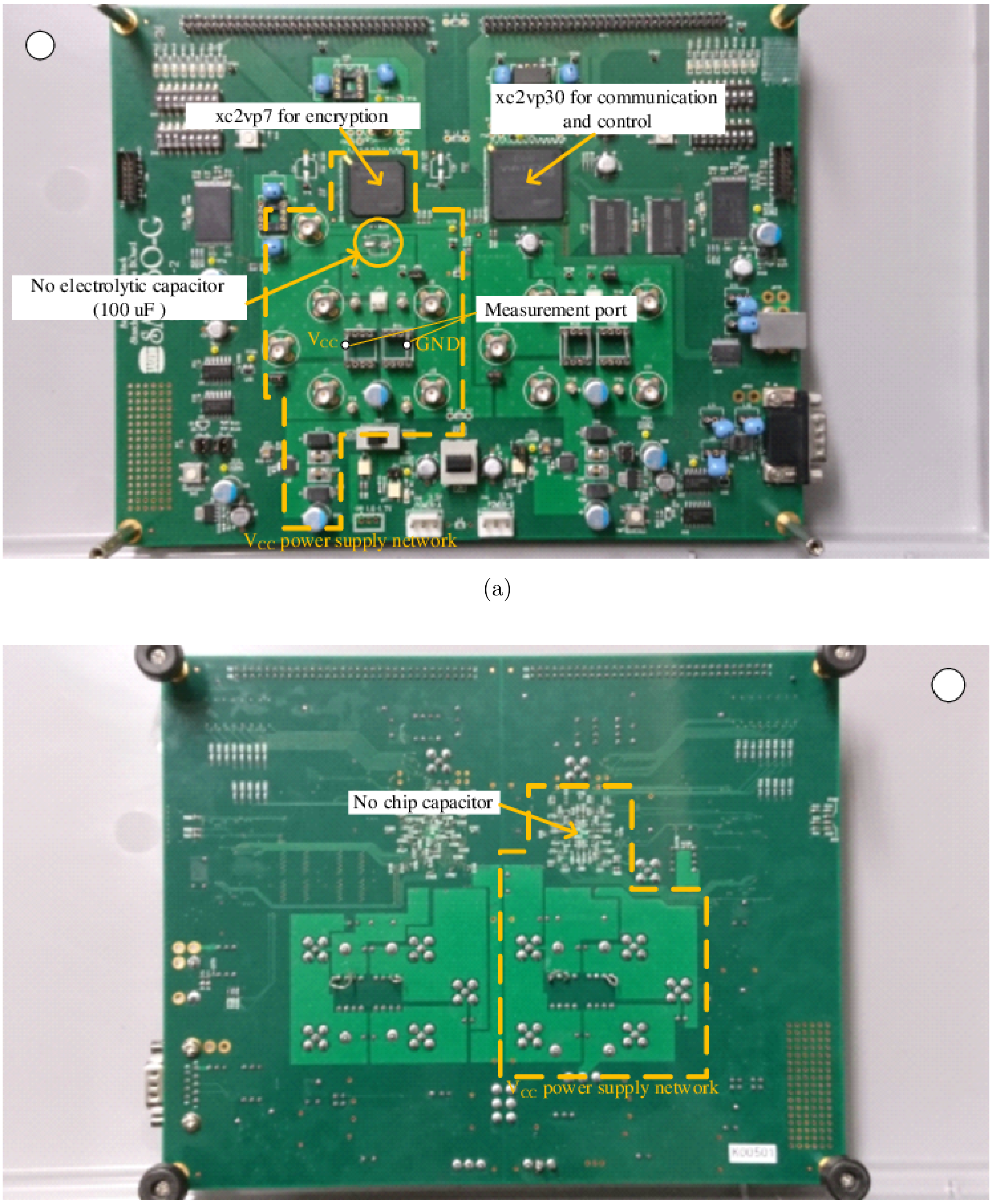


(a)


No chip capacitor at V_{cc} pin
V_{CC} power supply network
SENPU No. 1
D27002

(b)

Figure 3.1 Appearance of SENPU (EUT-A): (a) component side and (b) solder side.



(a)

(b)

Figure 3.2 Appearance of SASEBO (EUT-B): (a) component side and (b) solder side.

Table 3.4 Specifications of System for Measuring SNR of Side-channel Traces on EUT-A.

Component	Specifications
Cryptographic module	SENPU, AIST
FPGA	Cyclone V (5ECEFA5F23)
Clock freq.	48 MHz
Oscilloscope	DSO-S 104A, KEYSIGHT Technologies
Bandwidth	1 GHz
Sampling rate	1 GS/s
Resolution	10 bits
N_{avg}	1, 4, 20
Power rail probe	N7020, KEYSIGHT Technologies
Bandwidth	2 GHz
Passive probe	1161A, Agilent Technologies
Bandwidth	500 MHz
Personal computer	HP, ProBook 450 G2

Table 3.5 Specifications of System for Measuring SNR of Side-channel Traces on EUT-B.

Component	Specifications
Cryptographic module	SASEBO-G, AIST and Tohoku Univ.
FPGA	xc2vp7 ,Xilinx (for encryption) xc2vp30 ,Xilinx (for communication and control)
Clock freq.	24 MHz
Oscilloscope	54845A, Agilent Technologies
Bandwidth	1.5 GHz
Sampling rate	1 GS/s
Resolution	8 bits
N_{avg}	1, 2, 3, 5, 10, 20, 50
Passive probe	1161A, Agilent Technologies
Bandwidth	500 MHz
Personal computer	HP, ProBook 450 G2

For the following explanation, Measurement conditions for each SNR measurement is listed in Table 3.7.

Table 3.6 Common parameters in both SNR measurement.

Item	Parameters
Plaintext sets	Random plaintext set for measuring $V_{\mathrm{data}} + V_{\mathrm{noise}}$ Constant plaintext set for measuring V_{noise}
Secret-key	$(\mathrm{2B\ 7E\ 15\ 16\ 28\ AE\ D2\ A6\ AB\ F7\ 15\ 88\ 09\ CF\ 4F\ 3C})_{16}$
The number of trace measurements	10000

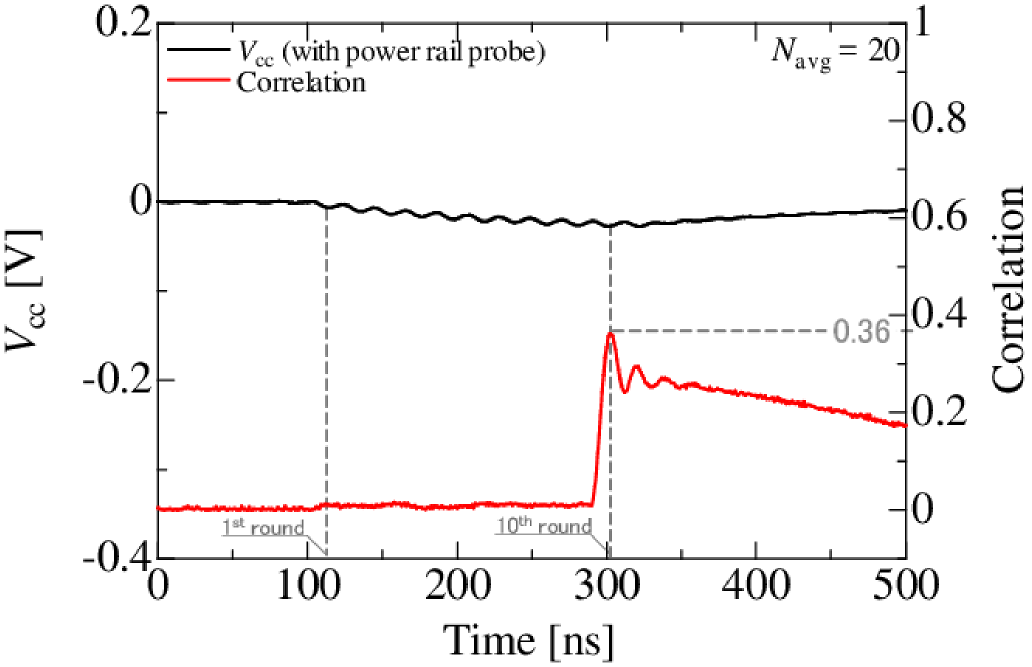
Table 3.7 List of Conditions for each SNR Measurement.

Target	Probe	Plaintext set	
		Constant for measuring V_{noise}	Random for measuring $V_{\mathrm{data}} + V_{\mathrm{noise}}$
EUT-A	Power rail probe	Condition A $N_{\mathrm{avg}} = 1, 4, 20$	Condition B $N_{\mathrm{avg}} = 1, 4, 20$
	Coaxial cable	Condition C $N_{\mathrm{avg}} = 1, 20$	Condition D $N_{\mathrm{avg}} = 1, 20$
EUT-B	Passive probe	Condition E $N_{\mathrm{avg}} = 1, 2, 3, 5, 10, 20, 50$	Condition F $N_{\mathrm{avg}} = 1, 2, 3, 5, 10, 20, 50$

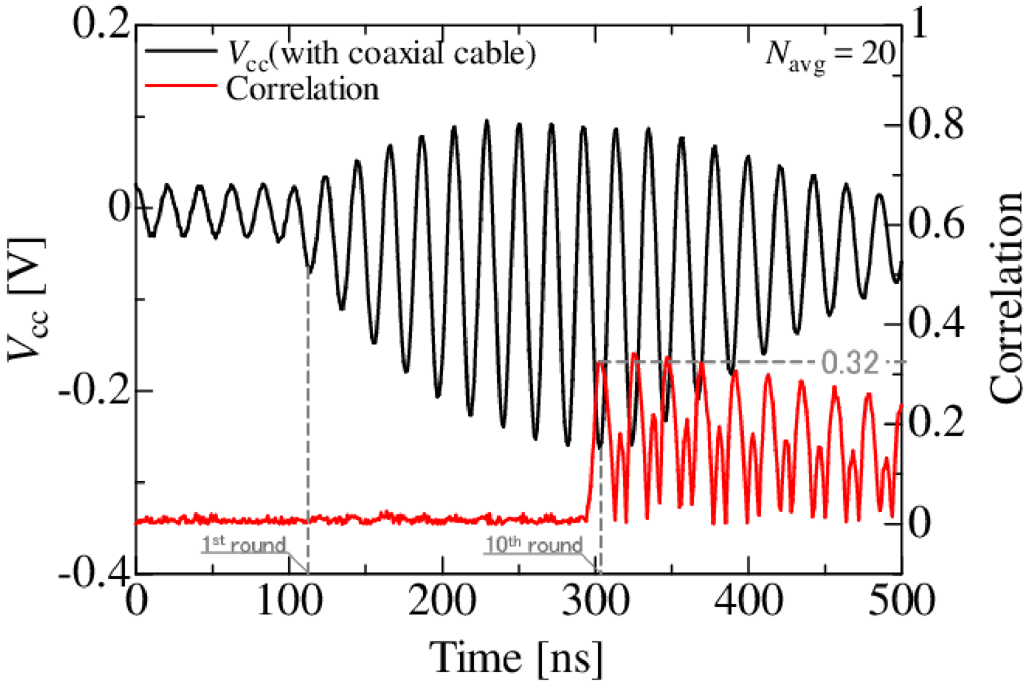
3.4.2 Identification of Relationship Between Leakage Trace SNR and Correlation Coefficient

In side-channel trace measurement with EUT-A, the SNR and the correlation coefficient were calculated from measured traces by proposed methods shown in Section 3.4. Fig. 3.3 shows the measured traces and calculated correlation coefficient when N_{avg} was 20 as a example. Traces shown in Fig. 3.3(a) and Fig. 3.3(b) were measured with the power rail probe and the coaxial cable, respectively. There are differences in the amplitude of traces and the correlation coefficients in the encryption due to difference in probe characteristics.

The SNR of target round is calculated from the variances of signal and noise components by (3.5). Each variance of target round (10th round) was measured following the method described in Section 3.4. The measured variance in each EUT-A condition shown in Table 3.7 is plotted in Fig. 3.4. In Fig. 3.4, it can be seen that the different variance was measured in each condition and Vnoise decreases as Nave increases. For calculating the SNR, $\mathrm{Var}(V_{\mathrm{data}})$ was calculated for each probe condition. $\mathrm{Var}(V_{\mathrm{data}})$ was calculated by (3.5) using the variances when N_{avg} was 20 because even though the traces averaged 20 times, $\mathrm{Var}(V_{\mathrm{noise}})$ was not zero. Each variance of condition A and C was used as $\mathrm{Var}(V_{\mathrm{noise}})$. The correlation coefficients were calculated from the traces measured with condition B and D.



(a)



(b)

Figure 3.3 Measured traces and calculated correlation coefficients in EUT-A measurement: (a) for power rail probe and (b) for coaxial cable.

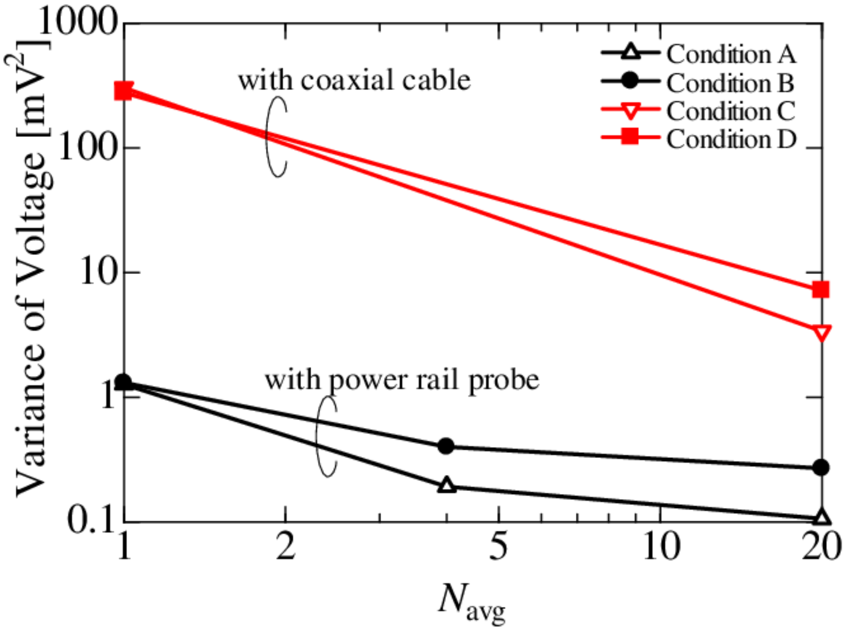


Figure 3.4 Variances of measured voltages at the target round with respect to change in the plaintext in EUT-A measurement.

It was verified whether the SNR and the correlation coefficients calculated from the measured traces satisfy the relationship described in Section 3.3. The SNRs and correlation coefficients calculated from the measured trace are plotted in Fig. 3.5. Moreover, the prediction values of ρ_2 at arbitrary SNR_2 calculated by (3.3) are drawn by the broken line in Fig. 3.5, where, SNR_1 and ρ_1 were set the values which are measured with the power rail probe when N_{avg} was 20. In Fig. 3.5, it was confirmed that the SNR and the correlation coefficient calculated from measured traces agree well with the predicted ones of equation (3.3) regardless of the measurement conditions: the probes and the number of averaging. This result suggests that the SNR and the correlation coefficient of the side-channel trace leaking from the same cryptographic circuit follow to (3.3).

Then, the result in the case of EUT-B is described. In side-channel trace measurement with EUT-B and SNR calculation, the SNR and the correlation coefficient were calculated from measured traces by the same method as the case of EUT-A. Fig. 3.6 shows the measured traces and calculated correlation coefficient when N_{avg} was 50 as a example. Understandably, different traces in appearance was observed from the Fig. 3.3. The measured variance at the target round in EUT-B measurement is plotted in Fig. 3.7. In Fig. 3.7, it can be seen the same feature as Fig. 3.4 which is the different variance was measured in each condition and V_{noise} decreases as N_{avg} increases. The SNRs and correlation coefficients calculated from the measured trace are plotted in Fig. 3.8. Moreover, the prediction values of ρ_2 at arbitrary SNR_2 calculated by (3.3) are drawn by the broken line in Fig. 3.8, where, SNR_1 and ρ_1 were set the values which are measured when N_{avg} was 50. In Fig. 3.8, it was also confirmed that the SNR and the correlation coefficient

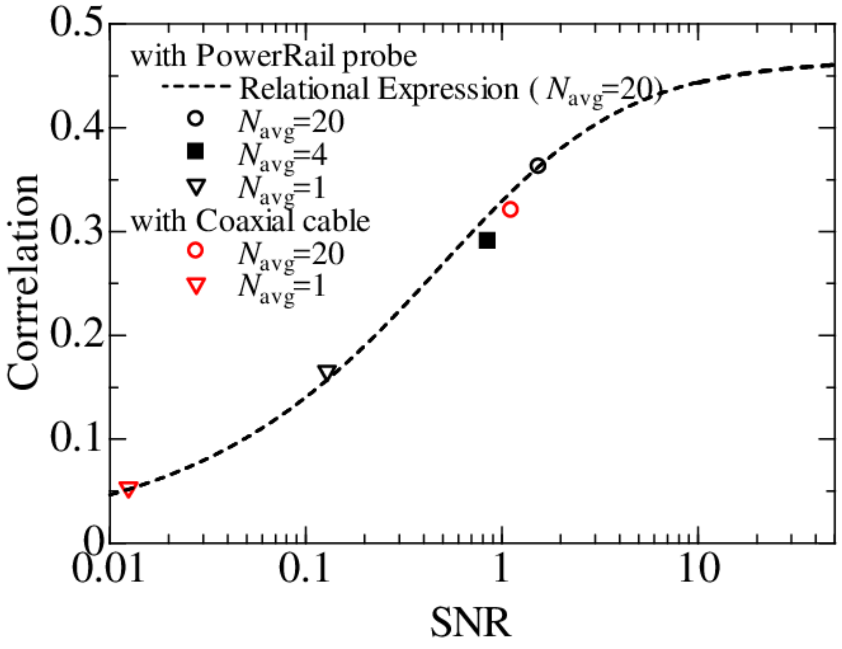


Figure 3.5 Variation of the correlation coefficient by SNR and comparing with ones calculated by (3.3) in EUT-A measurement

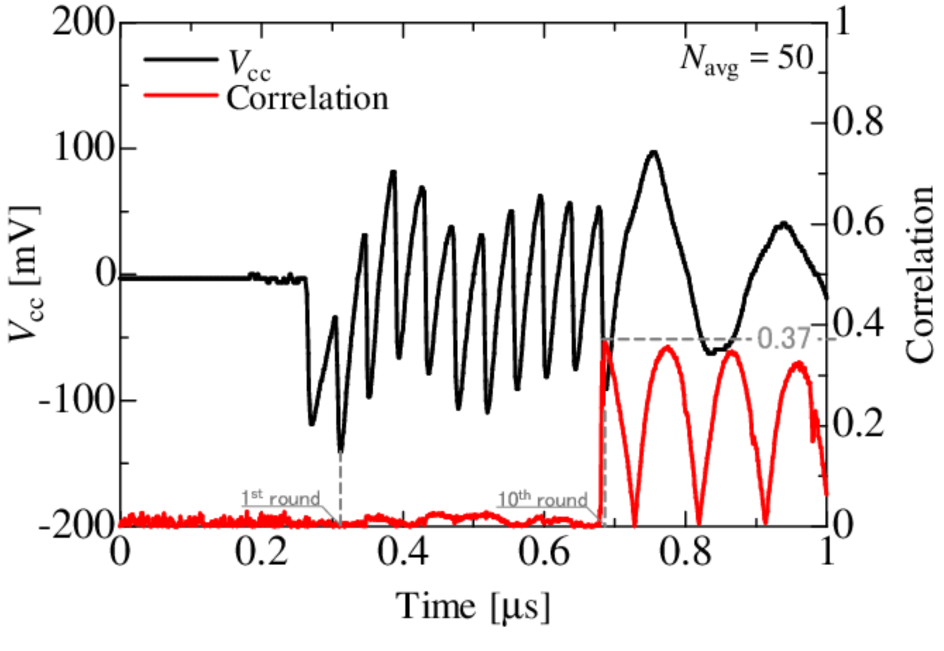


Figure 3.6 Measured trace and calculated correlation coefficient in EUT-B measurement

calculated from measured traces agree well with the predicted ones of equation (3.3) regardless of N_{avg}. This result also suggests that the SNR and the correlation coefficient of the side-channel trace leaking from the same cryptographic circuit follow to (3.3).

In the research above, it is verified that the SNR measured by the proposed method

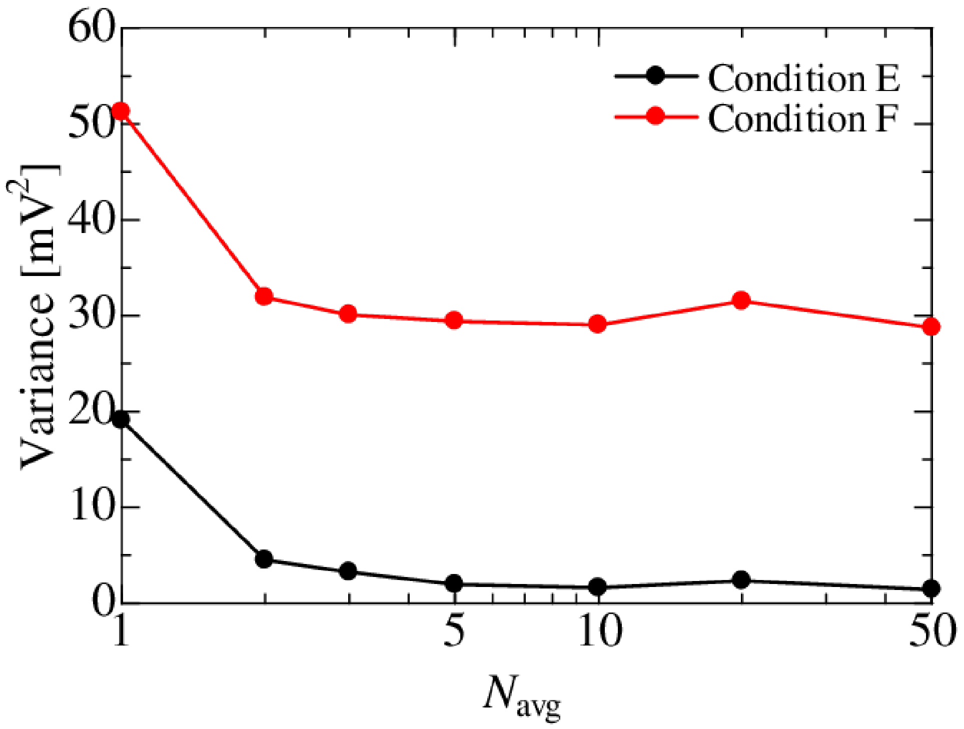


Figure 3.7 Variances of measured voltages at the target round with respect to change in the plaintext in EUT-B measurement.

is appropriate.

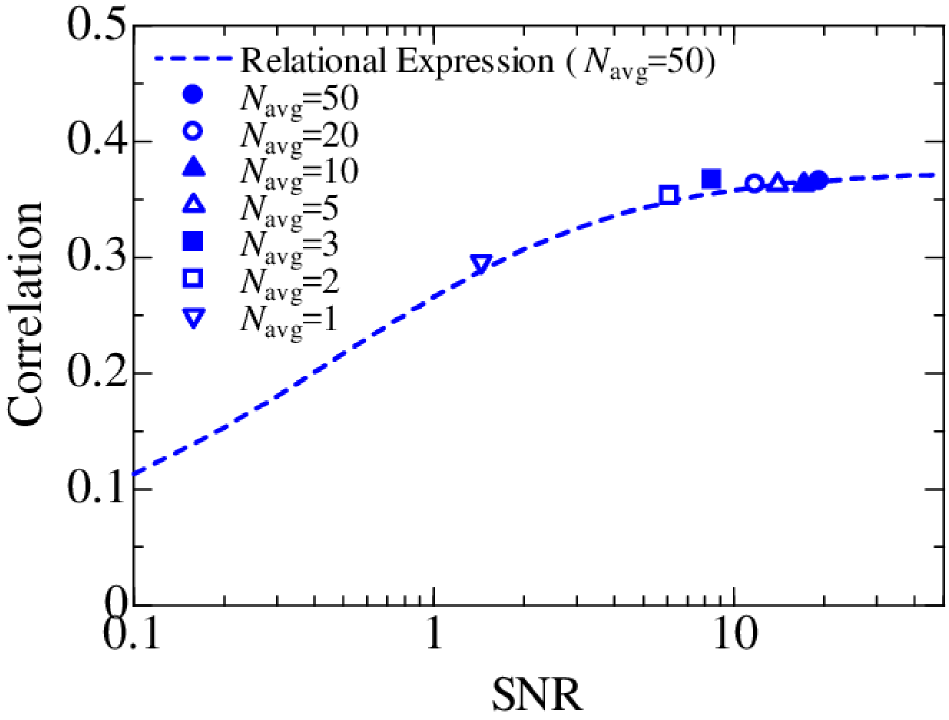


Figure 3.8 Variation of the correlation coefficient by SNR and comparing with ones calculated by (3.3) in EUT-B measurement

3.5 Side-channel Trace Estimation Based on RTL Simulation

First, this section describes a side-channel trace simulation method. Then a conversion method from measured traces to current consumption is described.

3.5.1 Proposed Simulation Method

The dynamic current during encryption is estimated via side-channel traces. Fig. 3.9 shows the procedure of the dynamic current estimation based on RTL simulation. The traces are calculated in the following steps:

1. creating a dump file from the RTL simulator of an EDA tool by using a test bench and an HDL file written for the RTL,

2. calculating the dynamic current of a device while encrypting arbitrary plaintexts, by using the power analyzer of the EDA tool, and

3. resetting the simulation timing, repeating the power analysis (step 2), and generating as many traces as necessary for SCA resistance prediction.

The dump file is a file recording the entirety of all data transitions of circuits in a device, such as resistors at a certain moment. Here, the HDL file before logic synthesis, which includes no detailed design information such as propagation delays, is used. The test bench is a file that sets up the virtual environment for RTL simulation and describes the input/output signals of the device: the clock, communication signals with external devices, and so on. The plaintext sets to be encrypted are also controlled by the test bench file.

The dynamic current is calculated by the power analyzer according to the simulation conditions, device-specific characteristics, and the toggle rate determined from the dump file. Here, only the simulation conditions (i.e., supply voltages to the device and simulation timing) must be specified. The supply voltages must be set to the same values as for the actual EUT. The power analyzer only calculates the average current over an arbitrary time period Δt, which is determined by setting the start time and the end time. By specifying a small period, the average consumption over the period can be calculated as the instantaneous consumption in the target round. In the RTL simulation, all signals are switched simultaneously in synchronization with the clock, as shown in Fig. 3.10. Therefore, Δt must be set to a value encompassing a round operation in AES and half the clock period or less. In contrast, if Δt is set to a value exceeding half the clock period, the simulation is affected by processing at timing other than the target process timing. The calculated dynamic current value depends on the value of Δt. This is because the average current is calculated according to Δt, even though the total number of processed

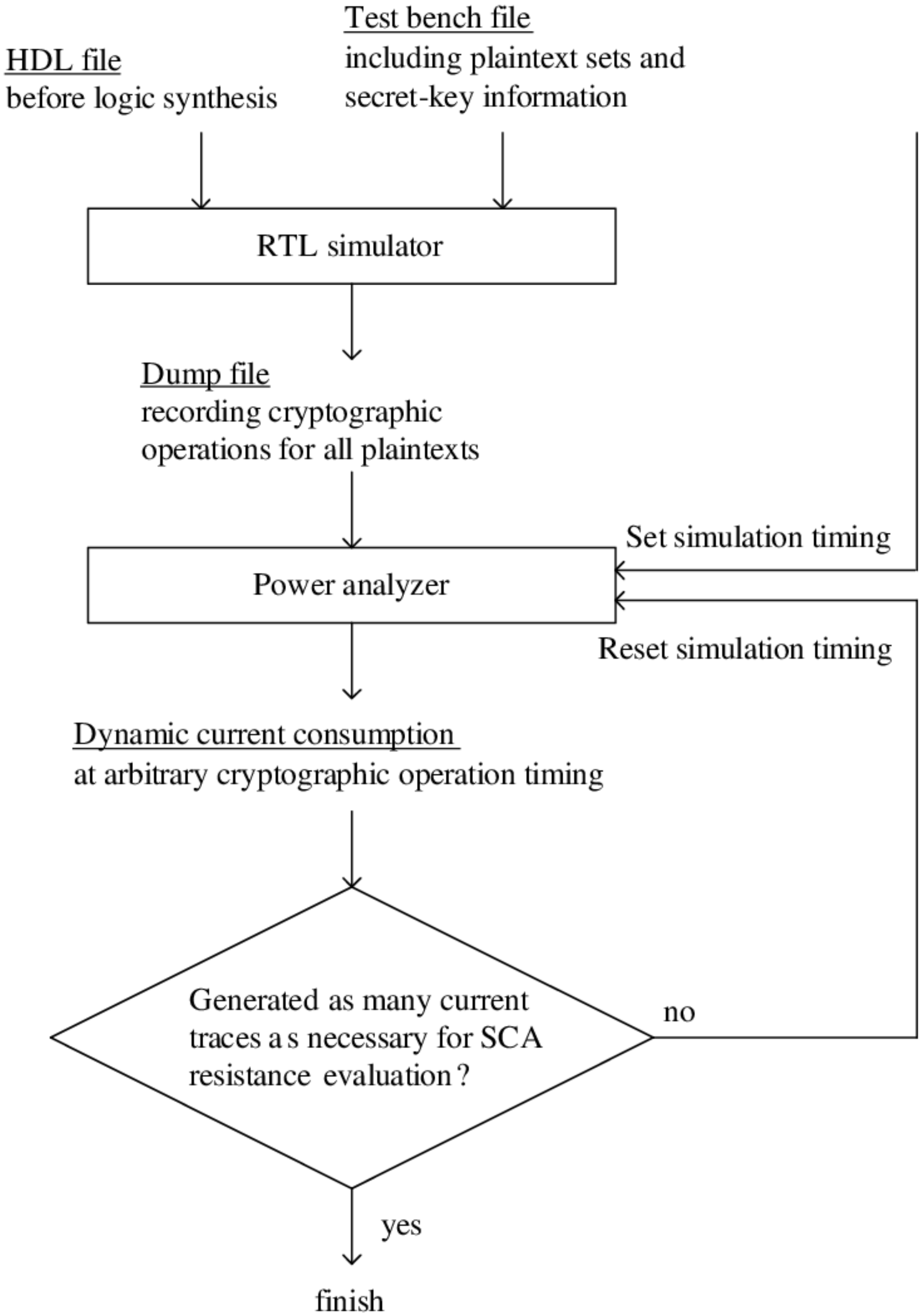


Figure 3.9 Flowchart of current consumption simulation

signals is constant, meaning that the total amount of dynamic current is constant. Therefore, to adjust the peak value of the calculated dynamic current to actual measurement, adjustment of Δt is necessary. As the total number of processed signals is constant, however, the amount of side-channel information contained in the calculated dynamic current for any Δt is also considered constant. Setting the device-specific characteristics and toggle rate is unnecessary, because they are calculated automatically by the EDA tool; that is, burdensome tasks in physical device-level simulation such as simulation model construction are unnecessary.

The current obtained from one iteration of step 2 is a value at the set simulation timing. That is, only one current value with respect to one plaintext is acquired in one step. Hence, it is necessary to generate a large number of traces by repeating step 2, because side-channel information cannot be analyzed from a single trace in CPA. Then, by resetting the simulation timing for power analysis, it is possible to acquire current values for processing of different plaintexts. Finally, when as many current traces as necessary for SCA resistance evaluation have been generated, the simulation ends.

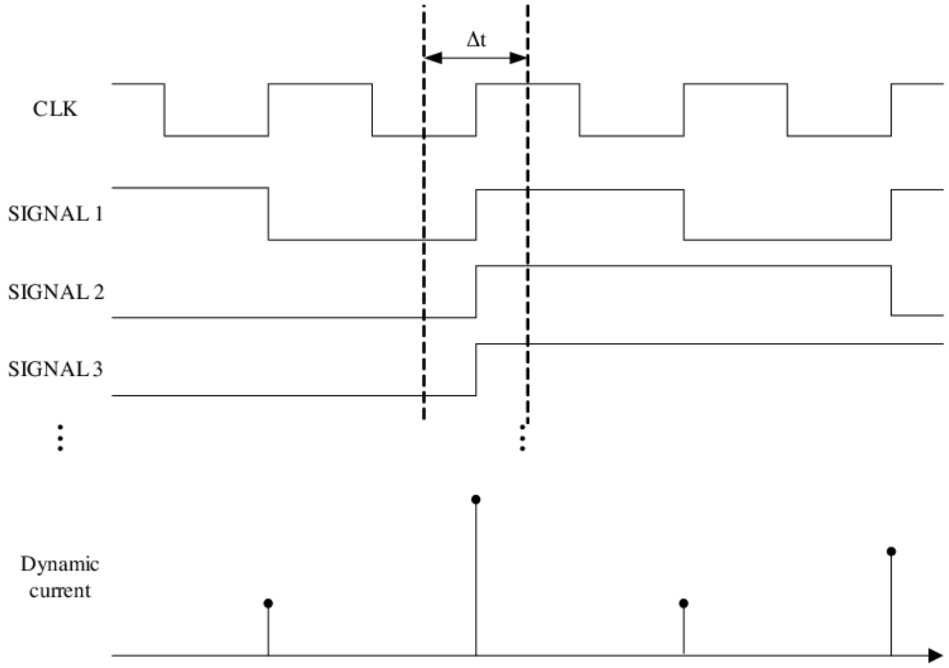


Figure 3.10 Simulated dynamic current in RTL simulation

All the steps above are easily repeated by implementing a shell script. By incorporating the simulation timing of the target round for all plaintexts into the script, this simulation can be automated, thus avoiding troublesome operations during the simulation.

The steps above are similar to the methods shown in [24–27]. The input data for the simulation behavior, however, is different. In [24–27], a configuration file obtained by logic synthesis from an HDL file was input to the timing simulator; that is, timing analysis was executed. Such timing analysis is suitable for eliminating processing of timing gaps in circuits such as wave dynamic differential logic (WDDL) and for accurately predicting traces; it is not suitable, however, for analysis in the early design process, because the analysis time is long. On the other hand, the method that we use here executes the RTL simulation by inputting the HDL file before logic synthesis, enabling high-speed RTL simulation and power analysis. The reason for this is that detailed design information such as propagation delays may be unnecessary. In [31, 32], it was reported that the frequency spectrum around the clock frequency and below that has a large amount of side-channel information. Therefore, it is inferred that analysis at higher frequencies is not required. This suggests that most of the side-channel information can be simulated with a time resolution the same as the clock period. Moreover, when observing the trace for an external circuit of a cryptographic device such as a PDN, the trace is slowed, so timing analysis becomes less important. Altogether, detailed design information may be unnecessary.

For realizing side-channel simulation with the method proposed here, it is needed to examine whether generated traces have side-channel information.

3.5.2 Conversion Method from Measured Trace to Current Consumption

Unfortunately, the estimated dynamic current is just the current of a cryptographic device and does not directly represent a measurable trace. For evaluating the simulation, it is necessary to directly compare the generated trace with a measured trace in some way. Therefore, this research uses a method that converts the measured trace into the current consumption by using an equivalent circuit of the PCB including the cryptographic device. The conversion method [50, 51] is described as follows.

As shown in Fig. 3.11, it is assumed that voltage V_{meas} is measured at the measurement port on a PDN as the side-channel trace, and the internal circuit of the FPGA is represented by an equivalent current source I_{source} and an equivalent impedance Z. Here, I_{source} represents the dynamic current during encryption, while Z represents the impedance of the semiconductor cells and on-chip capacitors. I_{meas} is the current flowing through the measurement port. Z_{in} is the input impedance of the measurement probe or measurement equipment.

First, a transfer function K from I_{source} to the measurement port is calculated by

$$K = \frac{I_{\mathrm{meas}}}{I_{\mathrm{source}}}. \tag{3.6}$$

K can easily be calculated through simulation by using the equivalent circuit of the EUT. For example, it can be calculated by setting I_{source} to 1 and observing I_{meas}. Second, I_{meas} is calculated by

$$I_{\mathrm{meas}} = \frac{V_{\mathrm{meas}}}{Z_{\mathrm{in}}}. \tag{3.7}$$

Finally, I_{source} is calculated by

$$I_{\mathrm{source}} = \frac{I_{\mathrm{meas}}}{K}. \tag{3.8}$$

A current equivalent to the simulated dynamic current is thus obtained from the measured trace through these steps.

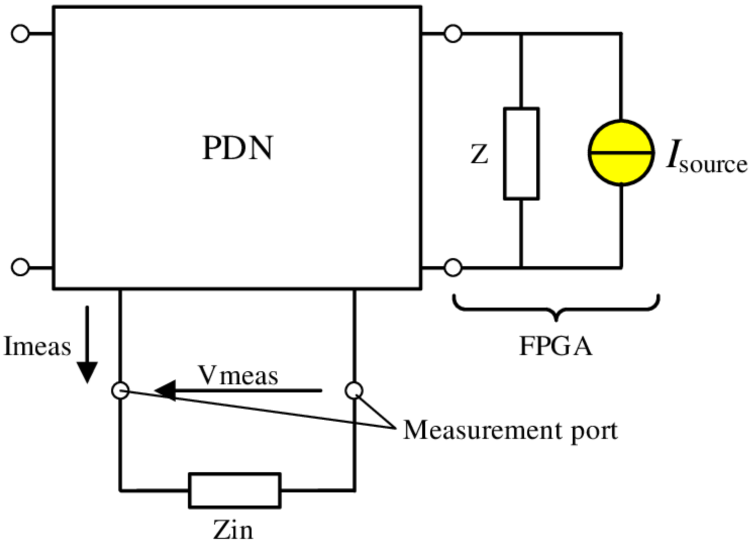


Figure 3.11 FPGA model.

The applicaiton and the examination are respectively described in next section.

3.6 Simulated Trace Evaluation

3.6.1 Application and Simulation Settings

In the side-channel trace simulation, EUT-A shown in subsection 3.4.1 was used. To evaluate the simulation, an equivalent circuit of the PDN including the FPGA was determined with an electromagnetic field simulator (HFSS, ANSYS) and measurement using a vector network analyzer (E5061B, Keysight Technologies). The resulting equivalent circuit is shown in Fig. 3.12. The left and the right ends of the circuit represents the voltage regulator module (VRM) and the FPGA, respectively. An SMA connector was mounted at the position of the measurement point shown in the equivalent circuit. The circuit model representing the inside of the FPGA is similar to the model shown in Chapter 2, and is composed of equivalent impedances and an equivalent current source. To determine the impedance characteristics of the equivalent circuit, the impedance characteristics of the PDN excluding the FPGA were analyzed with HFSS, and the impedance characteristics of the PDN including the FPGA were measured with the E5061B. The internal impedance of the FPGA was then obtained by substracting the analyzed impedance from the measured impedance.

To calculate I_{source}, V_{meas} was measured with the system shown in Fig. 3.13. The system specifications for measuring V_{meas} are listed in Table 3.4. In comparing simulated and measured traces, the influence of random noise superimposed on a measurement

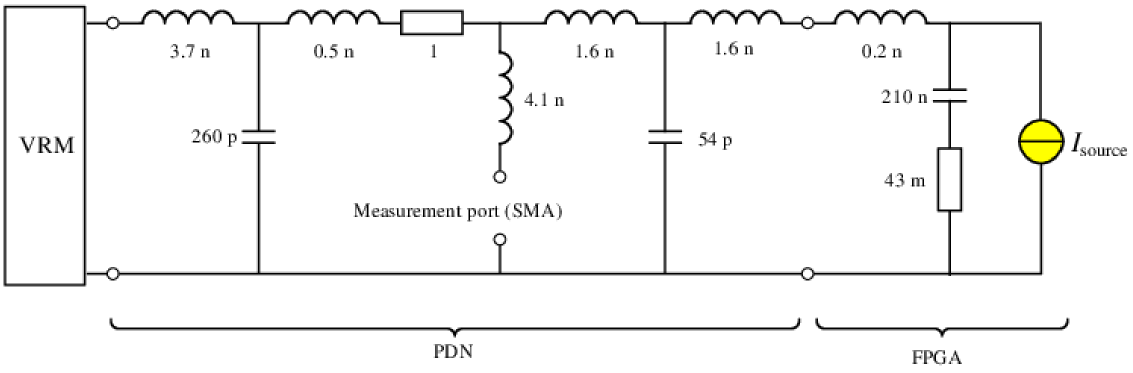


Figure 3.12 Equivalent circuit of EUT-A.

should be suppressed, because the simulation can not express such noise. Hence, the measurement system provided a low noise voltage measurement for accurate evaluation. Specifically, V_{meas} was measured by an oscilloscope (DSO-S 104A, Keysight Technologies)

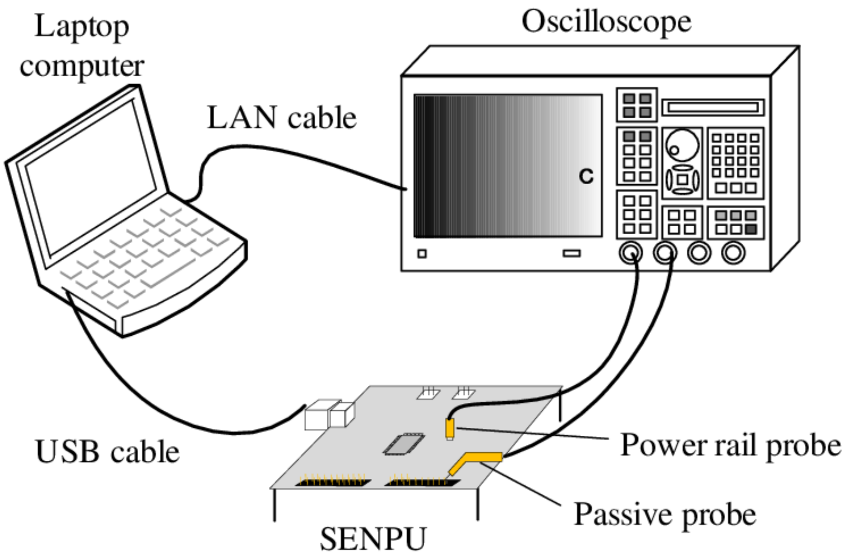


Figure 3.13 System layout for measuring V_{meas} on EUT-A.

with a power rail probe (N7020, Keysight Technologies) at the SMA measurement port shown in Fig. 3.12. The power rail probe has a 1:1 attenuation ratio and a large offset range, so V_{meas} was measured with a high signal-to-noise ratio (SNR). In addition, for accurate voltage measurement, the result was taken as the average of 20 measurements. A passive probe (1161A, Agilent Technologies) was used for trigger acquisition. A laptop computer was for controlling EUT-A and the oscilloscope.

For CPA and MTD evaluation, we used a varied set of plaintexts, in which all bits were changed randomly, and obtained 10000 traces. For the power model, an HD set between the ninth and tenth rounds with respect to the secret key (2B 7E 15 16 28 AE

D2 A6 AB F7 15 88 09 CF 4F 3C$)_{16}$ was used.

The transfer function K used for the conversion is shown in Fig. 3.14. It was calculated by SPICE simulation using the equivalent circuit shown in Fig. 3.12. The V_{meas} spectrum shown in Fig. 3.15 was measured at the measurement port shown in Fig. 3.12. The I_{source} spectrum shown in Fig. 3.16 was then calculated from equations (3.7) and (3.8), where Z_{in} was set to 50 Ω, the input impedance of the power rail probe. Finally, the I_{source} result shown in Fig. 3.17 was calculated by an inverse fast Fourier transform from the I_{source} spectrum and used for comparison with the simulated result. The measurement accuracy was insufficient at frequencies above 200 MHz because the measured voltage was not large enough with respect to the noise floor, thus, data at frequencies up to 200 MHz was used.

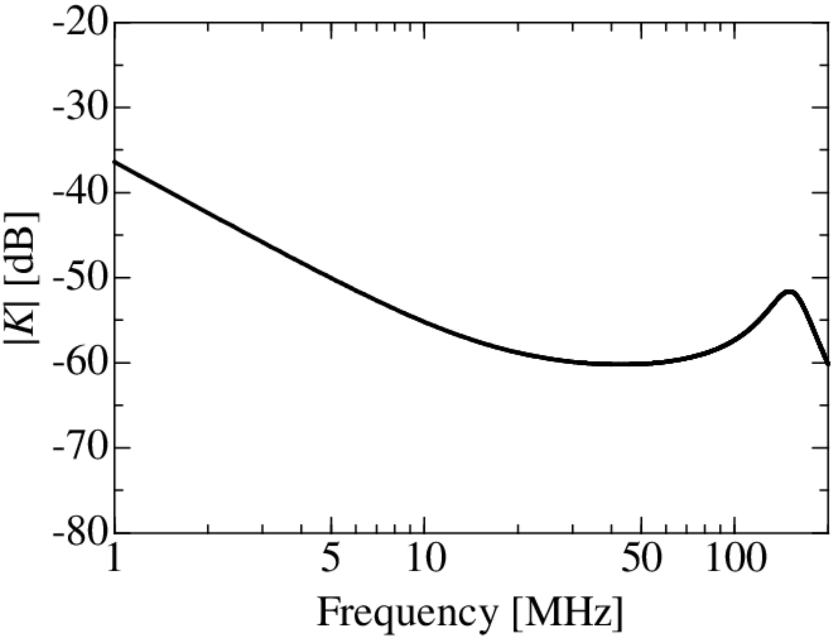


Figure 3.14 Transfer function K for converting from V_{meas} to I_{source}.

The CPA result for I_{source} was obtained with the tenth round of AES as the target round. An HD model in terms of all 16 bytes between the ninth and tenth rounds was used as the power model. For CPA a strong correlation of 0.71 was seen at the 10th round. As for MTD, a 128-bit secret key was divided into 16 partial keys. The number of traces needed for secret-key disclosure was 1000, which was the result of estimating all partial keys, and this result is shown later in Fig. 3.19.

In the side-channel simulation, a PowerPlay Power Analyzer (PPPA) of a commercial EDA tool (Quartus Prime 16.1, ALTERA) was used as the power analyzer mentioned in the previous section. The power supply voltages and simulation timing settings for

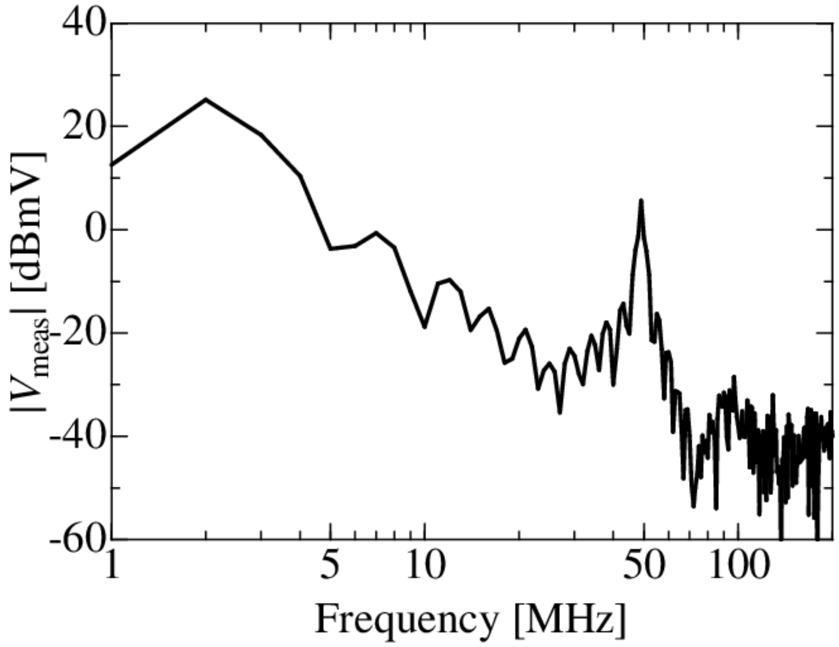


Figure 3.15 Spectra of V_{meas} calculated from Fig. 3.3(a).

Table 3.8 Power supply voltage settings for PPPA.

Name	Value (V)
VCC voltage	1.1
VCCA_FPLL voltage	2.5
VCCPGM voltage	1.8
VCCBAT voltage	1.2
VCCE_GXBL voltage	1.1
VCCE_GXBR voltage	1.1
VCCL_GXBL voltage	1.1
VCCL_GXBR voltage	1.1
VCCH_GXBL voltage	2.5
VCCH_GXBR voltage	2.5
VCCAUX voltage	2.5

PPPA are described here. The power supply voltages were set to the same conditions as for EUT-A, and the values are listed in Table 3.8. The other FPGA settings such as temperature and device power characteristics were set to default values.

For examining that the amount of side-channel information contained in the calculated dynamic current for a particular Δt, Δt was set to four values: 8, 20.832, 4, and 2 ns. The Δt of 8 ns corresponded to when the peak value of the calculated dynamic current roughly

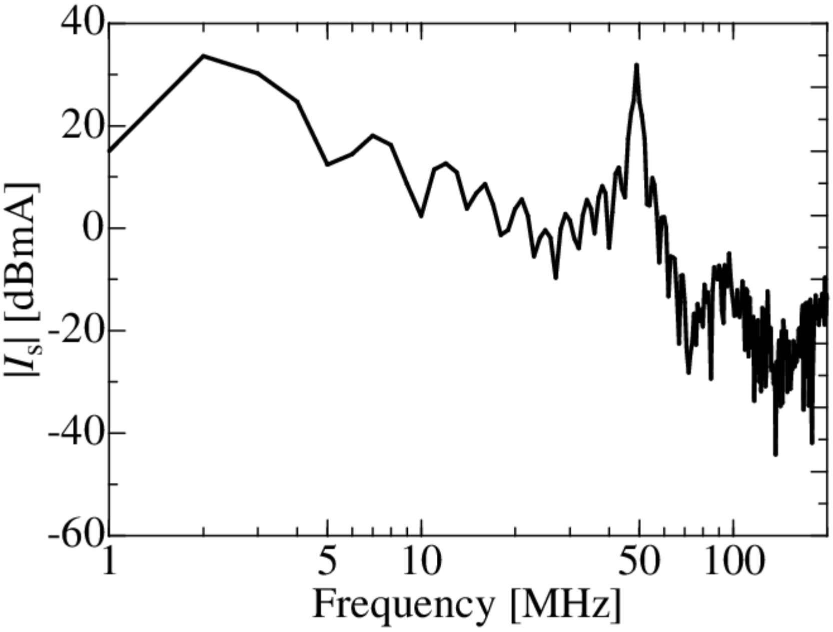


Figure 3.16 Current spectra of I_{source}.

agreed with the measured value. The value of 20.832 ns was half the clock period and thus the maximum value that could be used for simulation while excluding the influence of processing another round. Finally, the values of 2 and 4 ns were respectively one-tenth and one-fifth of the clock period.

3.6.2 Comparison with Measured Traces

The dynamic current was calculated from RTL simulation with four values of Δt: 8, 20.832, 4, 2 ns. These results are shown in Fig. 3.18. The gray line represents the measured I_{source}. The white circles, black circles, triangles, and squares represent the simulated I_{source} with Δt was 8, 20.832, 4, and 2 ns, respectively. To evaluate the estimated I_{source} while accounting for the offset of the measured I_{source}, the peak-to-peak amplitude of each current result in the target round was calculated, as listed in Table 3.9. The peak-to-peak amplitude of the simulated current with Δt of 8 ns agreed approximately with the measured value. The results thus confirmed that the simulated trace can roughly express the actual trace even in RTL simulation.

The simulated amplitude with Δt of 20 ns was smaller, however, than the measured value, while the simulated amplitudes with Δt of 4 and 2 ns were larger than the measured values. An inverse proportional relationship between Δt and the simulated current amplitude was thus seen. The reason was that the average current was calculated from

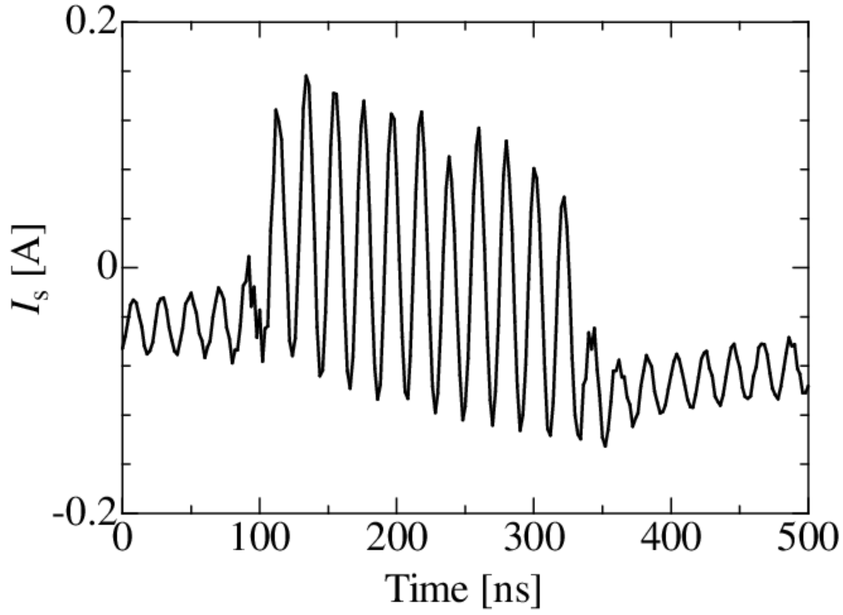


Figure 3.17 I_{source} for conparison with simulated trace.

Table 3.9 Peak-to-peak amplitude of each I_{source} shown in Fig. 3.18.

		Peak-to-peak amplitude (A)
Measurement		0.213
Simulation	Δt = 8 ns	0.210
	Δt = 20.832 ns	0.088
	Δt = 4 ns	0.356
	Δt = 2 ns	0.713

Δt, even though the total number of processed signals was constant; that is, the total amount of dynamic current was constant, as mentioned in previous section. To simulate a side-channel trace outside the FPGA, such as the power supply voltage for the PDN, it is necessary to adjust the amplitude. Developing a method for appropriately determining Δt to match the simulated and measured amplitudes is a future challenge.

Note that this RTL simulation could analyze the dynamic current faster than a gate-level simulation. In [27], it was reported that 20 hours are required to calculate 5000 traces, while it is possible to calculate 5000 traces in 4 hours with the RTL simulation shown in this paper. This result means that the RTL simulation is suitable for use in the early design process.

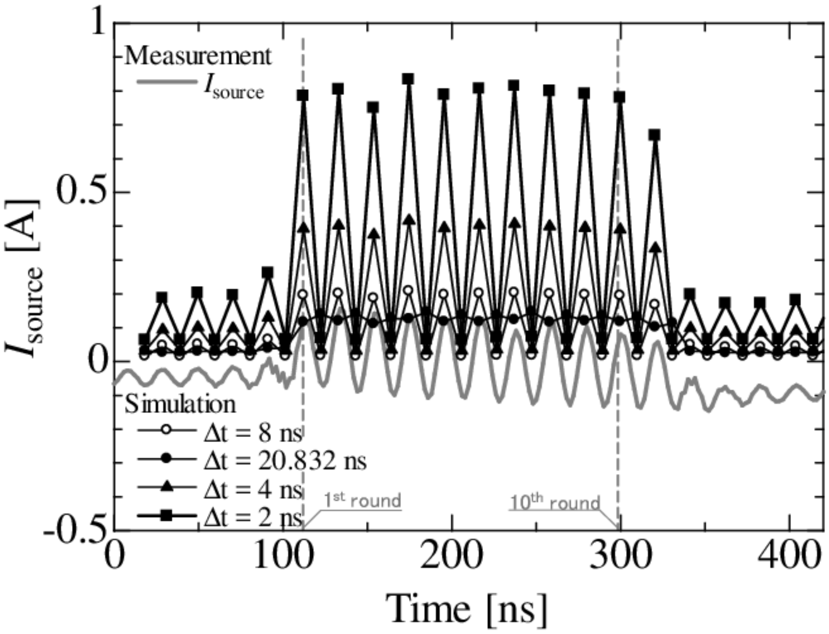


Figure 3.18 Measured and simulated I_{source} with four values of Δt: 8, 20.832, 4, 2 ns.

Table 3.10 CPA result for each I_{source} shown in Fig. 3.18.

		Correlation (10000 traces)
Measurement		0.710
Simulation	Δt = 8 ns	0.680
	Δt = 20.832 ns	0.648
	Δt = 4 ns	0.681
	Δt = 2 ns	0.674

3.6.3 CPA and MTD Results

Next, we evaluated the amount of side-channel information included in the simulated current by CPA and MTD. For these evaluations, 10000 dynamic current values were calculated at the tenth round. The CPA results are listed in Table 3.10.

In the CPA results, correlation coefficients comparable to those in the measurements were obtained for all values of Δt. This result suggests that the RTL simulation described in this paper can predict dynamic currents containing side-channel information, like physical- simulation and gate-level simulation.

We presume that the error between the measured and simulated correlation coefficients was due to noise during measurement. As explained in Section 4.4, we constructed a low-

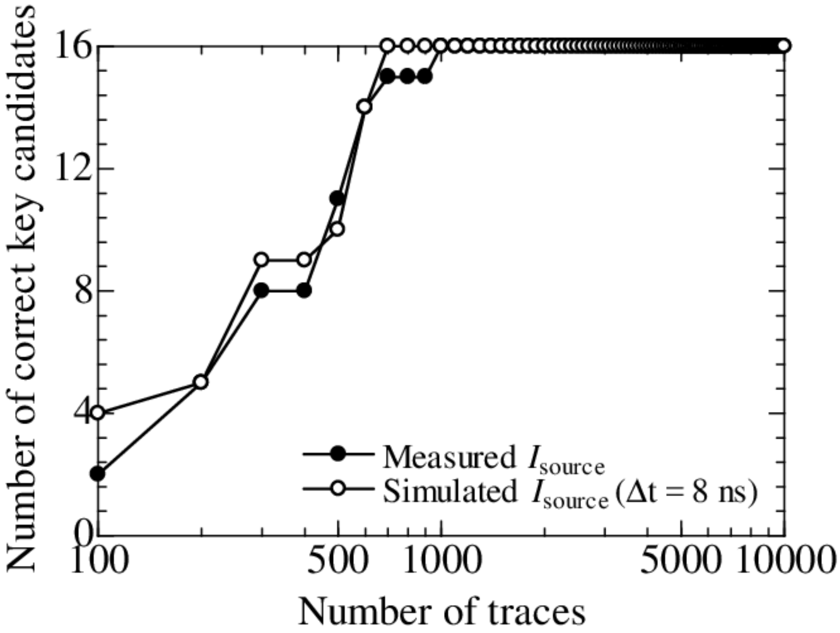


Figure 3.19 MTD results of measured and simulated I_{source}.

noise measurement system, but it did not completely eliminate the measurement noise.

In the RTL simulation, comparable correlation coefficients were obtained regardless of Δt. This was because the total number of processed signals was constant, regardless of Δt. This result suggests that side-channel information leakage generated in the FPGA can be evaluated without fitting Δt, meaning that encryption circuits implemented in the FPGA can easily be evaluated. As mentioned in the previous subsection, the RTL simulation enables faster analysis of the dynamic current than with gate-level simulation. Therefore, side-channel trace simulation based on the RTL simulation described in this paper is suitable for use in the early design process.

The MTD results for estimating all partial keys are shown in Fig. 3.19. The black and white circles respectively show the measured and simulated I_{source} results. The measured and simulated numbers of traces needed for secret-key disclosure were 1000 and 700, respectively, so these results agreed well. Furthermore, the trends from the start to the completion of partial key estimation also agreed well.

Error between the measurement and simulation is also seen in Fig. 3.19. We again presume that the error was due to the measurement noise mentioned above.

Altogether, this section has shown that RTL simulation can predict the dynamic current quickly and accurately via a side-channel trace. It thus suggests that RTL simulation can be used for side-channel trace prediction in the early design process instead of existing simulation methods.

3.7 Conclusion

This chapter proposed two methods: a SNR measurement method for realizing an SCA resistance evaluation method based on the SNR of side-channel traces and a side-channel trace simulation method using an EDA tool for efficient SCA resistance estimation. These methods are the prior examinations for establishing a SNR estimation method.

Firstly, it was experimentally verified whether the measured SNR and correlation coefficients satisfy the analytical relationship by a SNR measurement method we proposed. Here, it is assumed that SNR is used as SCA resistance design targets. In the proposed method, the SNR is calculated using a signal component obtained from the trace when encrypting a random plaintext set and a noise component obtained from the trace when encrypting a constant plaintext set. The correlation coefficient is calculated from measured traces based on the CPA. A PCB having an FPGA implemented an AES circuit was used as an EUT, and the core power supply voltage fluctuation of the FPGA on the PCB was measured as side-channel traces. The SNR was changed in the range of 20 dB by changing measurement conditions. As a result of the relationship verification, the SNRs and the correlation coefficients of the measured trace followed the analytical relational expression. This result means that the proposed method is appropriate and the evaluation based on the SNR is effective for efficient SCA resistance evaluation.

Secondly, in this paper, to enable efficient design of SCA countermeasures, we examined a method to predict SCA resistance at an early stage of the design process. We focused on a side-channel trace simulation method based on RTL simulation, because the method has two advantages. The first is that it requires no information about device characteristics, which is indispensable in physical device-level simulation but difficult to obtain for reasons of confidentiality and for analysis tools other than an EDA tool. The second advantage is that detailed design information decided at a later design stage, such as propagation delays, is unnecessary, unlike in gate-level simulation. In RTL simulation, because the amount of information handled is smaller than for physical device- and gate-level simulations, high-speed simulation is possible in exchange for somewhat reduced prediction accuracy of side-channel traces. Therefore, we investigated whether the dynamic current predicted via side-channel traces by RTL simulation contains side-channel information equivalent to that of the measured dynamic current. A side-channel standard evaluation board, the Senpu board, with an FPGA implementing a lookup-table-based AES-128 circuit, was used as an EUT. A free version of an EDA tool supplied by the FPGA vender, Quartus Prime, was used as the RTL simulator, and the bundled PowerPlay Power Analysis (PPPA) tool was also used. To evaluate the simulation method, the simulated current was compared with the measured dynamic current. The latter was obtained by converting the measured voltage fluctuation in the onboard power supply network for the FPGA core circuit to the dynamic current of the FPGA, according to the impedance characteristics of the PCB and FPGA. The simulated current agreed well with the measured one. In the simulation results using PPPA, because the peak value of the dynamic current varied depending on the set time period, it was necessary to adjust the period to correctly simulate the magnitude of the side-channel trace. CPA and MTD results, however, also agreed with adjustment of the time period. This indicates that the side-channel information included in the dynamic current consumed by the FPGA can easily be simulated without fitting the time period. In addition, this RTL simulation method can analyze the dynamic current faster than other simulation methods can. For gate-level simulation, it has been reported that 20 hours are required to calculate 5000 traces, whereas we could calculate 5000 traces in 4 hours with the RTL simulation. This paper has demonstrated that RTL simulation can predict the dynamic current quickly and accurately via side-channel traces. It thus confirms that RTL simulation is useful for side-channel trace prediction in the early design process.

Altogether, the two methods shown in this chapter are expected to contribute to the efficient HWS design.

Chapter 4

Optimum Design Method of Snubber Circuit for Efficient EMC and HWS Design

4.1 Introduction

The use of high-speed switching to achieve miniaturization and high efficiency in synchronous buck converters is leading to an increase in electromagnetic interference (EMI) [52]. One of the causes is the parasitic LC resonance caused by the output capacitance C_{oss} on the low-side MOSFET and the equivalent series inductance (ESL) of the circuit input side [53]. The LC resonance has been reported to occur in the 50–300 MHz frequency band [53], [54]. In this paper, we focus on LC resonance in synchronous buck converters.

Two types of methods are generally used to damp LC resonance [35]. The first type uses PCB-level countermeasures. The radiated fields are minimized by carefully designing the input side of the circuit [54]. The second type uses circuit-level countermeasures. The radiated fields are minimized by adding resistance to the resonant loop. Methods of this type include inserting an RL snubber into the power distribution network [33–38], adding an RC snubber to the switch node [35,39], and using a MOSFET with high R_{oss} [55], [56]. In the work reported here, we focused on the RL and RC snubbers.

Previous work [37], [38] has shown that a snubber inductance three times greater than the ESL of the entire resonant loop damps the resonance sufficiently. Previous work [34] has also shown that a snubber resistance is larger than the typical natural loss in the resonant loop. Several methods have been proposed for optimally designing RL snubbers [34,37,38], but they are insufficient as an optimum design method because they optimize only one parameter and not the others. This means that the inductance or resistance is determined on a rule-of-thumb basis.

A simple and common way to select optimum parameters from many SPICE simulation results while changing the snubber parameters has been used in previous work [35], [36].

However, considerable trial and error may be required, and determining optimum parameters may be difficult.

An analytical method for optimally designing RC snubbers has been developed [39] that uses the root locus method to suppress surge voltage across a transistor. The optimum parameters are analytically designed while taking into consideration increases in overshoot and loss. However, since the method is based on the assumption that there is no oscillation, the RC snubbers may be over-designed when little oscillation is allowed to achieve the damping effect design target. This may result in higher-than-necessary power loss.

In this paper we present a method for optimizing all snubber parameters for any damping effect design target. The Q factor of the resonance is used as the objective function since it can indicate a damping effect quantitatively. It is analytically derived as a function of the snubber parameters using a simplified equivalent circuit of the resonant loop in the target circuit. Contour plots of the Q factor are used for uniquely determining the optimum parameters.

The EMI from the PCB and system depends on various components, such as the LC resonance, the PCB layout, and the field coupling to antenna structure. To determine a reasonable design target Q factor to practically control the EMI, the contribution of each factor to the EMI should be quantified; however, such quantification is still a challenging task. The proposed method therefore assumes that the contribution of the LC resonance is quantified.

A synchronous buck converter is used here as an example application of the proposed method. The optimized snubbers were evaluated in terms of not only resonance damping but also in terms of their negative effects; overshoot and power loss.

The rest of the paper is organized as follows. Section 4.2 introduces existing optimal design methods of snubber circuits and an objective of this research. Section 4.3 describes LC resonance due to parasitic impedance in the synchronous buck converter as a preliminary toward optimally designing snubbers. Section 4.4 introduces the method we propose for optimally designing RL and RC snubbers using the Q factor of the resonance as the design criterion. Section 4.5 shows that the damping effect obtained with the optimized snubber parameters can achieve various Q factor design targets. Section 4.6 describes our evaluation demonstrating that the proposed method can produce snubbers that minimize the negative effects. Section 4.7 concludes the paper with a summary of the key points.

4.2 Existing Optimal Design Methods of Snubber Circuits

An electrical and electronic circuit is composed of a combination of several circuit elements to realize a wide variety of functions. For efficient EMC design, it is necessary to optimize all elements for each function. A snubber circuit we focused here is no exception.

A snubber circuit is a types of EMI filters, are widely known for suppressing resonance causing EMI or protecting switching devices, and is composed of two elements: resistor and inductor or resistor and capacitor.

Existing optimal design methods of RL and RC snubber circuits are shown in Table 4.1. The methods are not unified, two and one types of methods are proposed respectively for an RL snubber circuit [33–38] and an RC snubber circuit [39].

For the RL snubber, first one is a simulation-based fitting method [33–36]. The previous work [34] have shown that a snubber resistance larger than the typical natural loss in the resonant loop damps the resonance sufficiently. In design procedure I, therefore, 1 Ω snubber resistance has been regarded as an appropriate value. In design procedure II, the method adjust snubber inductance appropriately through simulation-based fitting. A simple and common way to select optimum parameters from many simulation results while changing the parameters has been used, however, considerable trial and error may be required, and determining optimum parameters may be difficult. Besides, the prameter optimization is insufficient because the resistance is determined on a rule-of-thumb basis in procedure I and its resistance is not always optimum for all resonant circuits.

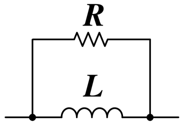
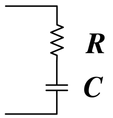
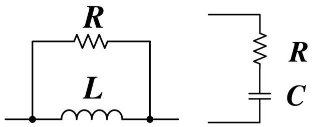
For the RL snubber, second one is a root locus analysis method using a simplified circuit of while resonant circuit [37, 38]. The previous works have shown that a snubber inductance three times greater than the ESL of the entire resonant loop is appropriate. In design procedure I, therefore, the snubber inductance is set to its value. In design procedure II, the optimal resistance is calculated analytically based on the root locus method using a simplified circut of while resonant circuit. However, the parameter optimization of this method is also insufficient because the inductance is determined on a rule-of-thumb basis in procedure I and its inductance is not always optimum for all resonant circuits.

For the RC snubber, a method that calculate snubber parameters satisfying the non-vibration condition (having the multiple root) based on root locus method is proposed for protecting switching devices [39]. This method optimizes two parameters simultaneously, so the parameter optimization is sufficient. However, in most resonant circuits, it is impossible that this method is applied to resonant circuits because there are no parameters satisfying the non-vibration condition.

The three existing methods have a common potential issue: the snubbers may be over-designed when little oscillation is allowed to achieve the damping effect design target.

One objective of this thesis is that solving the issues of the existing methods and providing an optimally designing method applicable to both the RL and the RC snubber circuits. This thesis proposed an optimal design method of RL and RC snubber circuits. The method proposed here optimizes simultaneously two electronic components of the RL or RC snubber. To determine optimum snubber parameters analytically and uniquely, a contour plot drawn by a formula for the Q factor as a function of the snubber parameters derived from a simplified equivalent circuit of the resonant loop is used. The Q factor is a parameter that describes how underdamped an resonance is, and it is often used for design target in EMC design. The RL and RC snubbers are applied to a synchronous buck converter as an example. The effects of the snubbers optimized using this method were reproduced by SPICE simulation to validate the method from the perspective of resonance damping, overshoot and power loss. Details of investigations are described in Chapter 4.

Table 4.1 Features of existing methods for optimizing snubber circuits

<table>
<tr><td>Design method</td><td>Simulation-based fitting [33–36]</td><td>Root locus analysis [37, 38]</td><td>Root locus analysis [39]</td><td>Q factor analysis (proposed method)</td></tr>
<tr><td>Target</td><td colspan="2">
RL snubber</td><td>
RC snubber</td><td>
RL & RC snubbers</td></tr>
<tr><td>Design procedure</td><td><b>I.</b> Set snubber resistance to a value larger than the typical natural loss in the resonant loop. <b>II.</b> Adjust snubber inductance appropriately through circuit simulation.</td><td><b>I.</b> Set snubber inductance to a sufficiently large value than ESL of while resonance circuit. <b>II.</b> Calculate optimal snubber resistance by the root locus method.</td><td><b>I.</b> Calculate optimal snubber parameters satisfying the non-vibration condition (having the multiple root) by root locus method.</td><td><b>I.</b> A formula for the Q factor as a function of the snubber parameters derived from a simplified equivalent circuit of the resonant loop is used. <b>II.</b> Select optimal parameters from a contour plot drawn by the formula.</td></tr>
<tr><td>Parameter optimization</td><td colspan="2"><b>Insufficient</b>
(In procedure <b>I</b>, the inductance or resistance is determined on a rule-of-thumb basis. That is, these methods optimize only one parameter and not the other.)</td><td><b>Sufficient</b></td><td><b>Sufficient</b>
(Parameters are optimized analytically and uniquely by a contour plot drawn by a formula for the Q factor.)</td></tr>
<tr><td>Application to resonant circuits</td><td colspan="2"><b>Possible</b></td><td><b>Impossible</b>
(In most cases, there are no parameters satisfying the non-vibration condition.)</td><td><b>Possible</b></td></tr>
<tr><td>Potential issue</td><td colspan="3">The snubbers may be over-designed when little oscillation is allowed to achieve the damping effect design target.</td><td></td></tr>
</table>

4.3 LC Resonance in Synchronous Buck Converter

This section describes LC resonance due to parasitic impedance in a synchronous buck converter as a preliminary to optimally designing snubber circuits.

Fig. 4.1 shows an original equivalent circuit of a synchronous buck converter with step-down from 12 V to 3.3 V and an output of 3.3 A that operates at 300 kHz [33], [55]. C_{bulk} on the input side is a bulk capacitor, C_{bp} is a bypass capacitor, L_{charge} and C_{out} on the output side are an inductor and a capacitor for smoothing the output voltage, and R_{load} is the load. The inductances and resistances connected in series with C_{bulk}, C_{bp} and C_{out} are the ESLs and equivalent series resistances (ESRs). L_{trace1} is the board wiring ESL between the DC power supply and C_{bulk}. L_{trace2} is the board wiring ESL between C_{bulk} and C_{bp}. L_{trace3} represents the sum of the board wiring ESL and the MOSFET device ESL. Two general-purpose devices, an FDMC4435BZ and an FDMS8680 (ON Semiconductor Co.), were respectively used as the high-side MOSFET M_1 and the low-side MOSFET M_2.

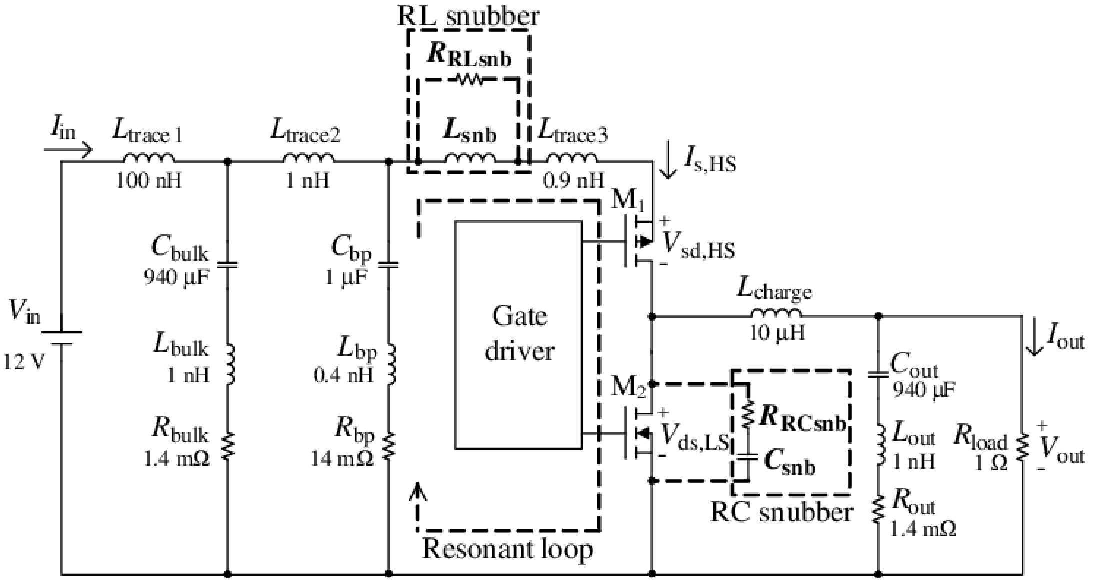


Figure 4.1 Original equivalent circuit of synchronous buck converter.

The RL snubber comprises inductance L_{snb} and resistance R_{RLsnb}, as shown in Fig. 4.1. The RC snubber comprises capacitance C_{snb} and resistance R_{RCsnb}. The snubbers should include the parasitic impedance; however, in this paper, we omit the parasitic impedance for simplicity. In actual circuits, this could increase the error between the damping effect of the snubbers and the design target. The deterioration of the damping effect by the parasitics can be neglected since experimental results [37] have shown that a sufficient damping effect can be obtained for the EMI control of digital ICs as predicted by using an equivalent circuit that omits the parasitics of the snubber components. The locations where snubbers are inserted and the method proposed for optimally designing the parameters are described in Section 4.4.

For the SPICE simulation, C_{bulk}, C_{bp}, L_{charge}, and C_{out} were set to the values previously used [33], [55]. The ESR and ESL parameters of the original equivalent circuit (i.e., those for C_{bulk}, C_{out}, and C_{bp}) were obtained from data sheets provided by the electronic components manufacturer. Typical values for the wiring inductances (L_{trace1}, L_{trace2}, and L_{trace3}) were used: 100, 1, and 1 nH, respectively.

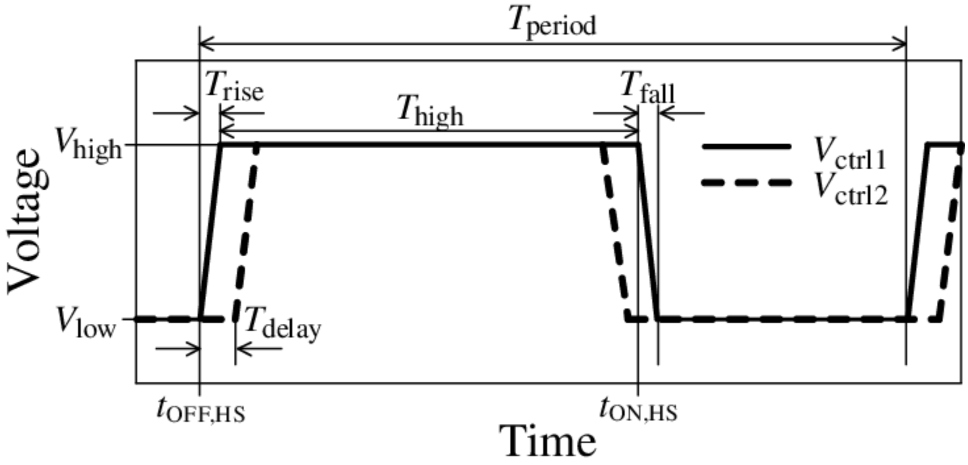


Figure 4.2 Gate control signals used for SPICE simulation.

Table 4.2 Switching Characteristics of Gate Control Signals

Signal	V_{low} (V)	V_{high} (V)	T_{delay} (ns)	T_{rise} (ns)	T_{fall} (ns)	T_{high} (μs)	T_{period} (μs)
V_{ctrl1}	0	12	0	5	5	2.3925	3.3
V_{ctrl2}	0	12	100	5	5	2.1925	3.3

The parameters for the gate control signal switching characteristics were set to the values shown in Fig. 4.2 and Table 4.2. V_{ctrl1} and V_{ctrl2} are the gate control signals applied respectively to the high- and low-side MOSFET gates. The signal levels V_{low} and V_{high} were set to 0 V and 12 V. The rise time T_{rise} and fall time T_{fall} were set to 5 ns because the operating frequency was 300 kHz; T_{period} was set to 3.3 μs. To enable step-down from 12 V to 3.3 V, the duty ratio of the signals was set to 72.5 %. T_{high} of V_{ctrl2} was set 200 ns shorter than that of V_{ctrl1} to prevent through current from the power to the ground when the MOSFETs were turned on at the same time. $t_{\text{OFF,HS}}$ and $t_{\text{ON,HS}}$ respectively represent the timing when V_{ctrl1} was set high and low. The gate driver output stages had realistic resistances of 3 Ω.

The steady-state waveforms calculated by SPICE simulation are shown in Fig. 4.3. The LTspice software (ANALOG DEVICES, Inc.) was used. The thin and thick lines respectively represent the source-drain voltage of the high-side MOSFET $V_{\text{sd,HS}}$ and the drain-source voltage of the low-side MOSFET $V_{\text{ds,LS}}$. Two large resonances are seen in

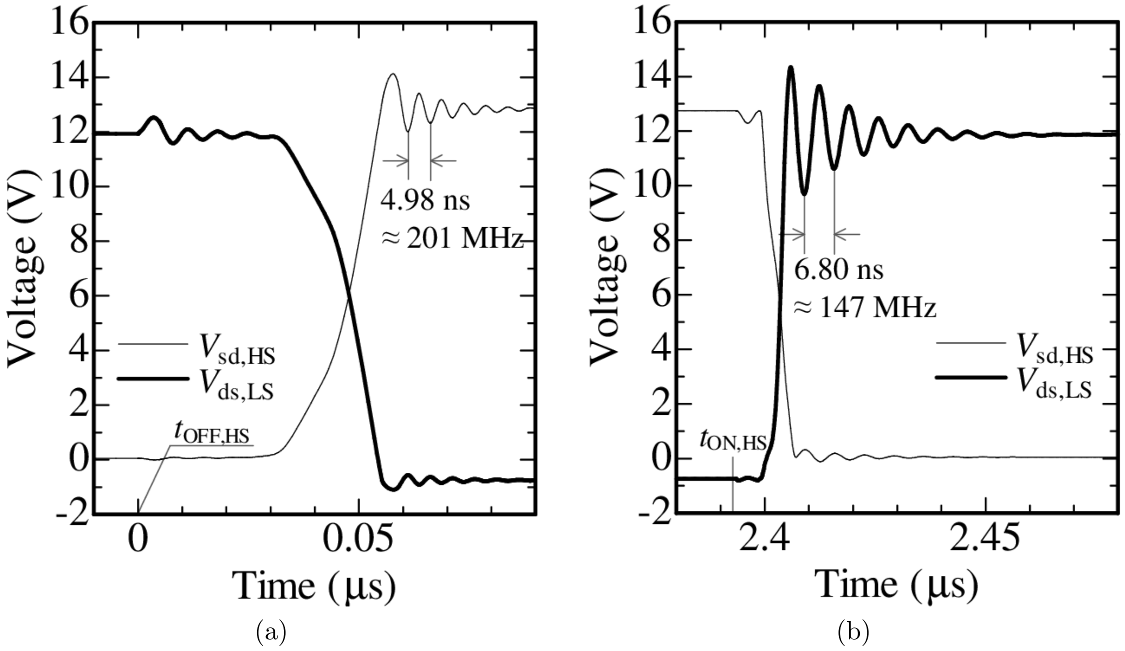


Figure 4.3 Simulated steady-state waveforms of characteristic voltages $V_{\mathrm{sd,HS}}$ and $V_{\mathrm{ds,LS}}$ w/o snubber circuits at (a) $t_{\mathrm{OFF,HS}}$ and (b) $t_{\mathrm{ON,HS}}$.

the graphs; the first is in $V_{\mathrm{sd,HS}}$ after 0.055 μs from $t_{\mathrm{OFF,HS}}$ and the second is in $V_{\mathrm{ds,LS}}$ after 0.01 μs from $t_{\mathrm{ON,HS}}$. These resonances occur due to the ESLs and the parasitic impedances of the MOSFETs in the closed circuit shown by the broken line in Fig. 4.1.

Two resonance frequencies match the frequencies calculated by $f_0 = 1/(2\pi\sqrt{L_{\mathrm{loop}}C_{\mathrm{loop}}})$, where L_{loop} and C_{loop} are the ESL and capacitance of the entire resonant loop shown in Fig. 4.1. L_{loop} is calculated by $L_{\mathrm{loop}} = L_{\mathrm{trace3}} + \{L_{\mathrm{bp}}//[L_{\mathrm{trace2}} + (L_{\mathrm{trace1}}//L_{\mathrm{bulk}})]\} + L_{\mathrm{MOS}}$, where L_{MOS} is the total ESL of the MOSFETs. M_1 and M_2 respectively have the ESLs of 0.14 and 0.32 nH. Thus L_{loop} is 1.7 nH. C_{loop} is calculated by $C_{\mathrm{loop}} = (C_{\mathrm{bulk}} + C_{\mathrm{bp}})C_{\mathrm{oss}}/(C_{\mathrm{bulk}} + C_{\mathrm{bp}} + C_{\mathrm{oss}})$, where C_{oss} is the output capacitance of the MOSFET. M_1 and M_2 respectively have the output capacitance of 370 and 690 pF. C_{loop} approximately equals to C_{oss} because C_{oss} is much smaller than C_{bulk} and C_{bp}. After 0.055 μs from $t_{\mathrm{OFF,HS}}$, C_{loop} is 370 pF because M_1 is turned off and M_2 is turned on. Thus f_0 becomes 201 MHz matching the resonance frequency in Fig. 4.3(a). After 0.01 μs from $t_{\mathrm{ON,HS}}$, C_{loop} is 690 pF because M_1 is turned on and M_2 is turned off. Thus f_0 becomes 147 MHz matching the resonance frequency in Fig. 4.3(b). It has been reported that the resonance of $V_{\mathrm{ds,LS}}$ dominantly contributes to EMI [53]. Fig. 4.3 also shows that the resonance of $V_{\mathrm{ds,LS}}$ is larger than that of $V_{\mathrm{sd,HS}}$ and that the resonance frequency is approximately consistent with the one previously reported [53]. Therefore, in this work reported here, we focus on the larger resonance of $V_{\mathrm{ds,LS}}$ at $t_{\mathrm{ON,HS}}$.

4.4 Proposed Method

In our proposed method for optimally designing snubber circuits using the Q factor of the resonance, either an RL or an RC snubber is inserted into the resonant loop shown in Fig. 4.1. The insertion locations are the same as those used in previous studies [33–36,39].

The snubbers produce not only resonance damping but also negative effects: overshoot (surge voltage and inrush current) and power loss. The RL snubber increases the surge voltage at $t_{\mathrm{OFF,HS}}$ due to an increase in the inductance of the power supply line. The RC snubber increases the inrush current at $t_{\mathrm{ON,HS}}$ due to an increase in the capacitance of the low-side. Furthermore, the snubbers slow MOSFET switching, increasing the power loss. These negative effects should be minimized because they shorten device lifetime and reduce product reliability. Our method for optimally designing snubbers

- achieves accurate identification of the target damping effect,
- minimizes the overshoot increase, and
- minimizes the power loss increase.

The Q factor used as the design criteria is calculated from a simplified equivalent circuit of the buck converter. The optimal snubber parameters are determined by

1. creating a simplified equivalent circuit of the resonant loop (excluding the snubber circuit) [37], [38],
2. inserting a snubber into the simplified circuit,
3. deriving an equation from the simplified circuit giving the Q factor as a function of the snubber parameters, and
4. drawing a contour plot of the Q factor at the resonance frequency and determining the optimum snubber parameters.

The optimum design procedures for RL and RC snubbers are described in detail in the following two subsections.

4.4.1 RL Snubber

First, the original circuit of the buck converter excluding the snubbers in Fig. 4.1 is reduced to the simplified one in Fig. 4.4. The simplified one represents the equivalent circuit when the high-side MOSFET is on. We focus here on the resonance induced by turn-on. The original circuit is simplified by first replacing L_{charge} with an open circuit since its inductance is usually several μH or more and the impedance of L_{charge} is much higher than those of the other elements in the resonance frequency range. Next, C_{bulk} and C_{bp} are replaced with a short circuit because these impedances are considerably smaller than those of the other elements. Moreover, to avoid complexity of the simplified equivalent circuit, the MOSFET gate terminals and the gate driver circuits are omitted.

All parameters of the simplified circuit excluding the snubber parameters are determined from data sheets and measurements. C_{oss} is the output capacitance of the low-side MOSFET. L_{loop} is the ESL of the entire resonant loop. R_{loop} is the ESR of the entire resonant loop; it is determined by the dominant parameter, R_{oss}, which is equivalent to the C_{oss} loss of the low-side MOSFET. C_{oss}, L_{loop} and R_{loop} are respectively 690 pF, 1.7 nH, and 0.4 Ω.

Next, the RL snubber is inserted in series into the resonant loop of the simplified equivalent circuit. The resulting simplified circuit is shown in Fig. 4.5.

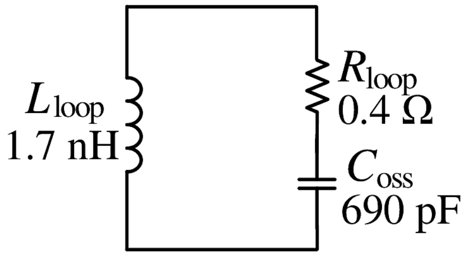


Figure 4.4 Simplified equivalent circuit of resonant loop excluding snubbers.

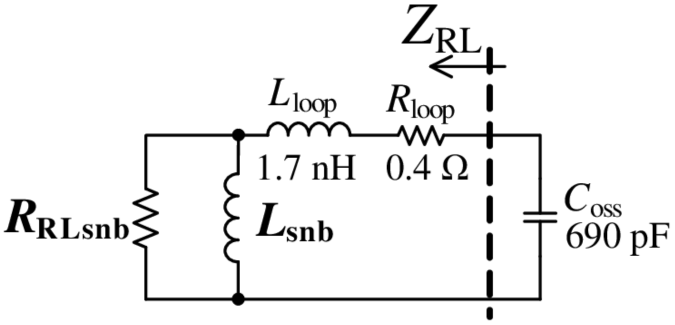


Figure 4.5 Simplified equivalent circuit of resonant loop including RL snubber.

Then, the relationship between the Q factor and the RL snubber parameters is derived from the simplified circuit. The Q factor at the resonance frequency is generally defined as

$$Q := \frac{X_{\text{L}}}{R} = \frac{X_{\text{C}}}{R}, \tag{4.1}$$

where X_{L} is the inductive reactance, X_{C} is the capacitive reactance, and R is the resistance. The inductive part impedance of the simplified circuit Z_{RL} can be separated from the capacitance C_{oss}, as shown in Fig. 4.5, giving the Q factor as

$$Q = \frac{|\mathrm{Im}\{Z_{\mathrm{RL}}(\omega_0)\}|}{\mathrm{Re}\{Z_{\mathrm{RL}}(\omega_0)\}} \tag{4.2}$$

$$= \frac{\omega_0^3 L_{\mathrm{snb}}^2 L_{\mathrm{loop}} + R_{\mathrm{RLsnb}}^2 \omega_0 (L_{\mathrm{loop}} + L_{\mathrm{snb}})}{\omega_0^2 L_{\mathrm{snb}}^2 (R_{\mathrm{loop}} + R_{\mathrm{RLsnb}}) + R_{\mathrm{RLsnb}}^2 R_{\mathrm{loop}}}, \tag{4.3}$$

where ω_0 is the resonance angular frequency of the simplified circuit. At the resonance frequency, the imaginary part of the impedance of the simplified circuit becomes zero $\mathrm{Im}\{Z_{\mathrm{RL}}(\omega_0)\} - \mathrm{Im}\{Z_{\mathrm{Coss}}(\omega_0)\} = 0$, giving ω_0 as

$$\omega_0 = \sqrt{\frac{-b + \sqrt{b^2 - 4ac}}{2a}}, \tag{4.4}$$

where a, b, and c are given by

$$a = L_{\mathrm{snb}}^2 L_{\mathrm{loop}} C_{\mathrm{oss}},$$

$$b = R_{\mathrm{RLsnb}}^2 C_{\mathrm{oss}} (L_{\mathrm{loop}} + L_{\mathrm{snb}}) - L_{\mathrm{snb}}^2,$$

$$c = -R_{\mathrm{RLsnb}}^2.$$

A larger L_{snb} can easily result in large resonance damping; however, it also increases the negative effects, i.e., surge voltage and power loss. Thus, L_{snb} should be set as small as possible to minimize the negative effects. Therefore, a pair of L_{snb} and R_{RLsnb} that is optimum satisfies two conditions: it achieves the target Q factor and it minimizes L_{snb}.

Finally, a contour plot of the Q factor is drawn in accordance with (4.3) to determine the optimum parameters. Fig. 4.6 shows a contour plot of the Q factor with the two variables, L_{snb} and R_{RLsnb}. The optimum parameters can be easily determined using Fig. 4.6. For example, if the Q factor design target is 2.5, the L_{snb} and R_{RLsnb} pair labeled D,Ⅳ in Fig. 4.6 is identified as the optimum pair of parameters.

4.4.2 RC Snubber

The procedure for optimally designing RC snubbers is similar to that for designing RL snubbers. First, a simplified circuit of the resonant loop shown in Fig. 4.4 is created.

Next, the RC snubber is inserted into the simplified circuit in parallel with the low-side MOSFET. The resulting simplified circuit is shown in Fig. 4.7.

Then, the relationship between the Q factor and the RC snubber parameters is derived from the simplified circuit. The capacitive part impedance of the simplified circuit Z_{RC} can be separated from the inductance L_{loop}, as shown in Fig. 4.7, giving the Q factor as

$$Q = \frac{|\mathrm{Im}\{Z_{\mathrm{RC}}(\omega_0)\}|}{\mathrm{Re}\{Z_{\mathrm{RC}}(\omega_0)\}}, \tag{4.5}$$

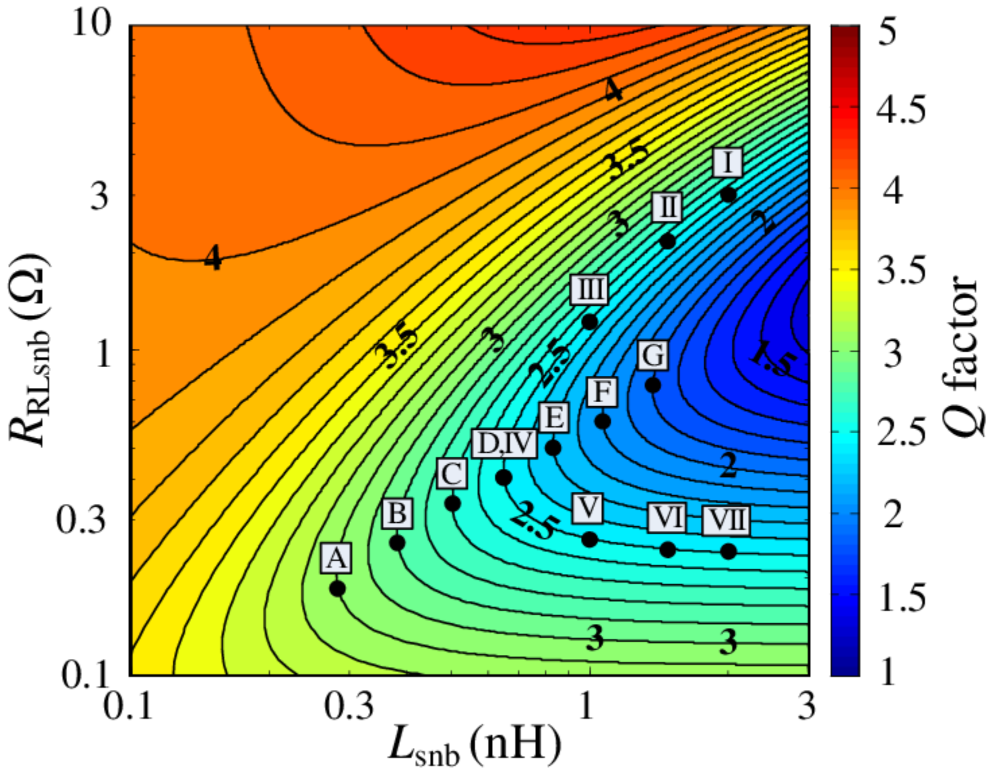


Figure 4.6 Q factor contour plot drawn in accordance with (4.3) for use in optimally designing RL snubbers.

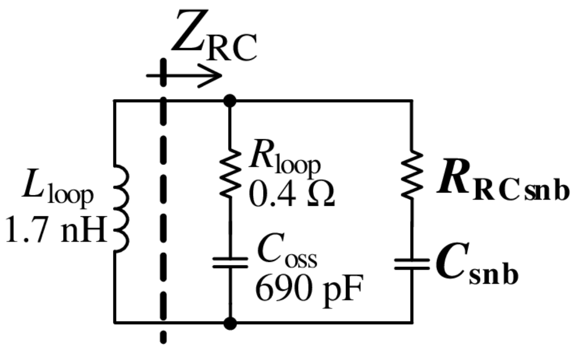


Figure 4.7 Simplified equivalent circuit of resonant loop including RC snubber.

where the numerator N_{Q} and the denominator D_{Q} of (4.5) are given as

$$\begin{aligned} N_{\mathrm{Q}} &= (R_{\mathrm{loop}}R_{\mathrm{RCsnb}} - \frac{1}{\omega_0^2 C_{\mathrm{oss}}C_{\mathrm{snb}}})(\frac{1}{\omega_0 C_{\mathrm{oss}}} + \frac{1}{\omega_0 C_{\mathrm{snb}}}) \\ &\quad -(\frac{R_{\mathrm{loop}}}{\omega_0 C_{\mathrm{snb}}} + \frac{R_{\mathrm{RCsnb}}}{\omega_0 C_{\mathrm{oss}}})(R_{\mathrm{loop}} + R_{\mathrm{RCsnb}}) \\ D_{\mathrm{Q}} &= (R_{\mathrm{loop}}R_{\mathrm{RCsnb}} - \frac{1}{\omega_0^2 C_{\mathrm{oss}}C_{\mathrm{snb}}})(\frac{1}{\omega_0 C_{\mathrm{oss}}} + \frac{1}{\omega_0 C_{\mathrm{snb}}}) \\ &\quad -(\frac{R_{\mathrm{loop}}}{\omega_0 C_{\mathrm{snb}}} + \frac{R_{\mathrm{RCsnb}}}{\omega_0 C_{\mathrm{oss}}})(\frac{1}{\omega_0 C_{\mathrm{oss}}} + \frac{1}{\omega_0 C_{\mathrm{snb}}}). \end{aligned}$$

Furthermore, ω_0 is derived using (4.4) from the condition $\mathrm{Im}\{Z_{\mathrm{Lloop}}(\omega_0)\} - \mathrm{Im}\{Z_{\mathrm{RC}}(\omega_0)\} = 0$, where a, b, and c are given as

$$\begin{aligned}
a &= L_{\mathrm{loop}}(R_{\mathrm{loop}} + R_{\mathrm{RCsnb}})^2 \\
b &= R_{\mathrm{loop}}R_{\mathrm{RCsnb}}(\frac{1}{C_{\mathrm{oss}}} + \frac{1}{C_{\mathrm{snb}}}) + L_{\mathrm{loop}}(\frac{1}{C_{\mathrm{oss}}} + \frac{1}{C_{\mathrm{snb}}})^2 \\
&\quad -(\frac{R_{\mathrm{loop}}}{C_{\mathrm{snb}}} + \frac{R_{\mathrm{RCsnb}}}{C_{\mathrm{oss}}})(R_{\mathrm{loop}} + R_{\mathrm{RCsnb}}) \\
c &= -\frac{1}{C_{\mathrm{oss}}C_{\mathrm{snb}}}(\frac{1}{C_{\mathrm{oss}}} + \frac{1}{C_{\mathrm{snb}}}).
\end{aligned}$$

A larger C_{snb} can easily result in large resonance damping; however, it also increases the negative effects, i.e., inrush current and power loss. Thus, C_{snb} should be set as small as possible. Therefore, a pair of C_{snb} and R_{RCsnb} that is optimum satisfies two conditions: it achieves the target Q factor and it minimizes C_{snb}.

Finally, a contour plot of the Q factor is drawn in accordance with (4.5) to determine the optimum parameters. Fig. 4.8 shows a contour plot of the Q factor with the two variables C_{snb} and R_{RCsnb}. For example, if the Q factor design target is 2.5, the C_{snb} and R_{RCsnb} pair labeled D,IV in Fig. 4.8 is identified as the optimum pair of parameters.

Although the optimum design method introduced in this section can be used for any Q factor design target, calculating the Q factor on the basis of simplified equivalent circuits can produce more errors than if the original circuit was used due to the simplification of the equivalent circuit. The next section describes how we tested the optimum parameters using the original circuit to identify potential errors.

4.5 Identification of Potential Erros Due to Use of Simplified Equivalent Circuits

We first consider whether the Q factor of the original circuit with optimum snubbers added meets the design target. The RL and RC snubbers labeled A–G in Fig. 4.6 and Fig. 4.8 were used as the optimized ones for Q factor design targets ranging from 1.9 to 3.1. Next, we evaluate the error between the Q factor design target and that of the original circuit with the added snubbers. The snubber parameters used correspond to labels I–VII in Fig. 4.6 and Fig. 4.8 for the same Q factor design target of 2.5. They are listed in Table 4.3.

4.5.1 Observed Q Factor in SPICE Simulation

The Q factor of the original circuit was obtained by reading the resonance frequency f_0 and the full-width at half maximum Δf from the envelope of the spectrum of the ringing

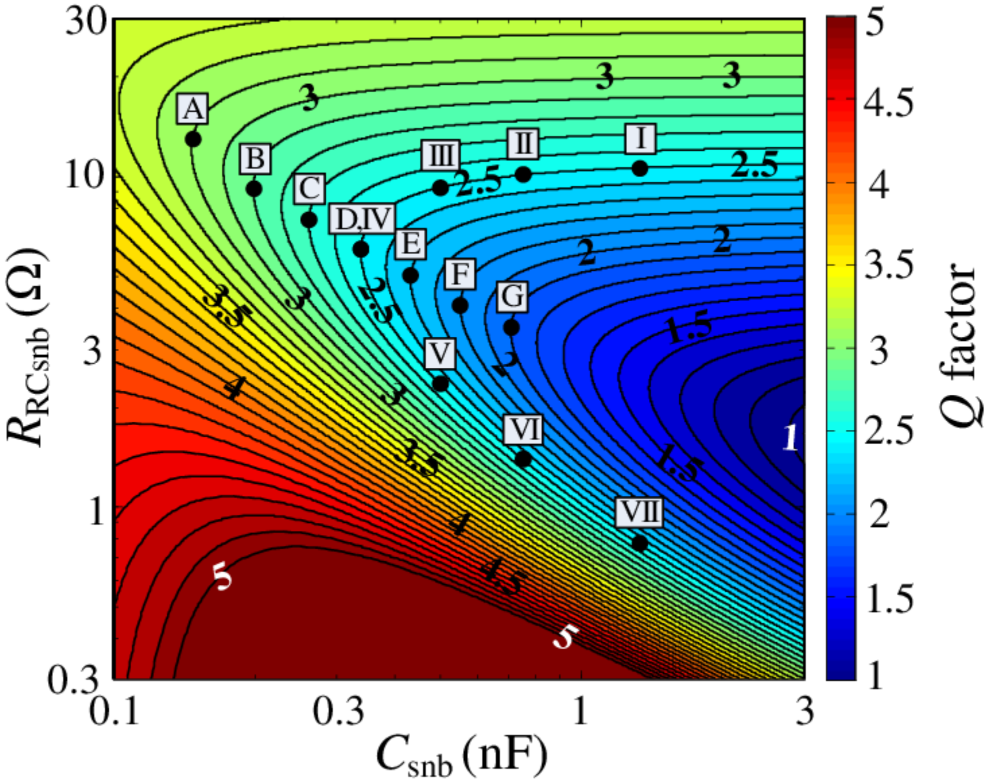


Figure 4.8 Q factor contour plot drawn in accordance with (4.5) for use in optimally designing RC snubbers.

waveform simulated by SPICE and calculated using

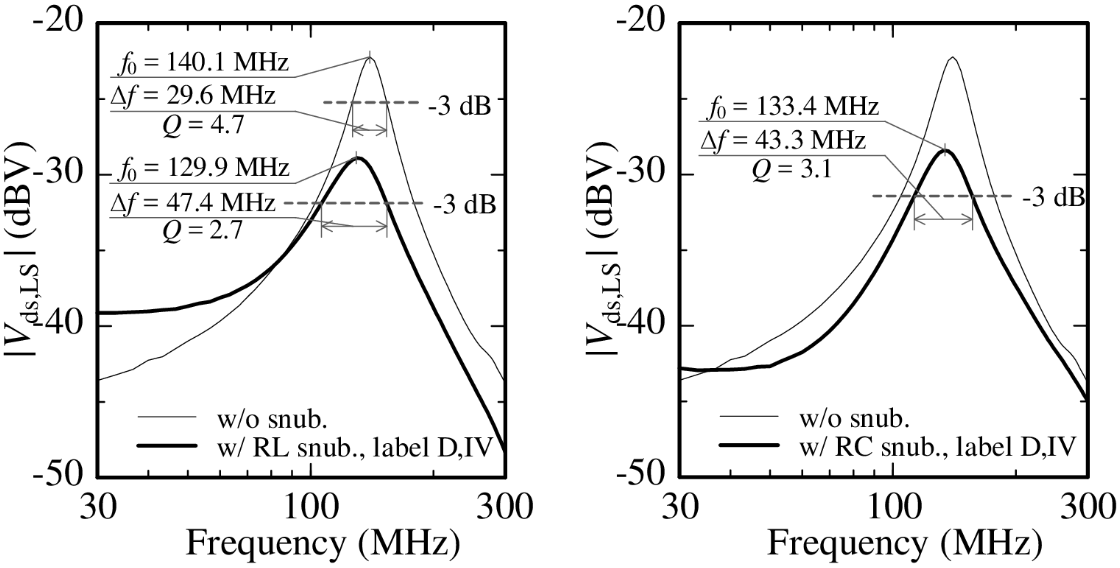
$$Q = \frac{f_0}{\Delta f}. \tag{4.6}$$

As an example of the simulation results, Fig. 4.9 shows the spectrum envelopes of the ringing waveforms $V_{\mathrm{ds,LS}}$. The frequency response of $V_{\mathrm{ds,LS}}$ for the original configuration without snubbers is shown by the thin lines. That with the snubbers labeled D,IV is shown by the thick lines. From the simulated spectra, the Q factors were respectively found to be 2.7 for the RL snubber and 3.1 for the RC snubber. Although these values do not agree completely with the design target of 2.5, a significant reduction from the original value of 4.7 was achieved for both snubbers.

The Q factors of the original circuit were calculated and were compared to those of the design target for the additional six optimized snubber configurations, labels A–C and E–G in Fig. 4.10(a). The circles correspond to the RL snubbers, the triangles correspond to the RC snubbers, and the broken lines represent the Q factor design targets. Although the obtained Q factors roughly matched the design targets, they include errors that were inconsistent with the design targets. For both snubbers, the errors for labels A–C were larger than that of label D,IV while those for labels E–G were smaller. The gradients of the obtained Q factors were slightly higher than those of the design targets.

Table 4.3 Optimized Snubber Parameters Labeled A–G for Different Q Factor Design Targets and Parameters Labeled I–Ⅶ for Same Q Factor Design Target

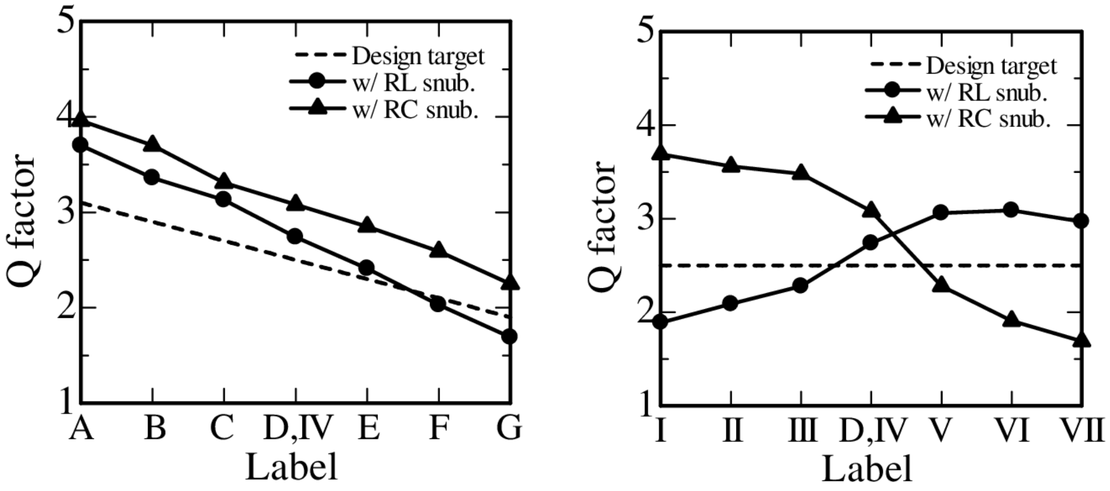
	Target	RL snubber		RC snubber	
Label	of Q	L_{snb} (nH)	R_{RLsnb} (Ω)	C_{snb} (nF)	R_{RCsnb} (Ω)
A	3.1	0.28	0.19	0.15	12.47
B	2.9	0.38	0.25	0.20	9.27
C	2.7	0.50	0.33	0.26	7.48
D,Ⅳ	2.5	0.66	0.40	0.35	6.00
E	2.3	0.83	0.50	0.43	5.13
F	2.1	1.07	0.64	0.55	4.17
G	1.9	1.37	0.76	0.71	3.49
I	2.5	2.00	2.98	1.25	10.80
Ⅱ		1.50	2.15	0.75	10.00
Ⅲ		1.00	1.22	0.50	9.30
D,Ⅳ		0.66	0.40	0.35	6.00
V		1.00	0.27	0.50	2.41
Ⅵ		1.50	0.25	0.75	1.38
Ⅶ		2.00	0.25	1.25	0.82



(a) (b)

Figure 4.9 Spectral envelopes of simulated ringing waveforms $V_{\mathrm{ds,LS}}$ w/o and w/ optimized snubbers labeled D,Ⅳ for (a) RL snubber and (b) RC snubber.

These results show that the Q factor design target was met by adding optimally designed snubbers to the original circuit. In the next subsection, we evaluate the small error between the Q factor of the original circuit and the design target and examine the cause of the differences in gradient.



(a) (b)

Figure 4.10 Q factors obtained from spectral envelopes of simulated ringing waveforms with (a) optimized snubbers labeled A–G for different Q factor design targets and (b) snubbers labeled I–VII for same Q factor design target.

4.5.2 Evaluation of Errors

As shown in Fig. 4.10(a), some of the obtained Q factors were larger than the design targets. A similar difference was seen without the snubbers. Without the snubbers, the Q factor of the original circuit calculated using (4.6) was 4.7 while that of the simplified circuit was 3.9. This difference was mainly caused by paths other than the resonant loop being omitted in the simplified circuit. In this case, the dominant factors were the omitted MOSFET gate terminals and the gate driver circuit. Similarly, the obtaining of Q factors higher than the design target in Fig. 4.10(a) was due to using the simplified circuits.

The cause of the difference in gradients was examined by examining the change in the Q factor due to the snubber parameters. We used (4.6) to calculate the Q factors of the original circuit to which the snubbers labeled I–III and V–VII were added and compared them to the design target of 2.5. All the Q factors are plotted in Fig. 4.10(b) with the circles for the RL snubbers, the triangles for the RC snubbers, and the broken line for the design target. For both snubbers, even though the same design target was set, different Q factors were obtained. The L_{snb} or C_{snb} of labels I–III and V–VII are larger than that of label D,IV. The larger the L_{snb} or C_{snb}, the larger the error; however, even though the same L_{snb} or C_{snb} was used, different Q factors were obtained.

There is an obvious limitation of simplifying the equivalent circuit model. The differences in the Q factor resulted from a change in the switching operation of the high-side MOSFET after an RL or RC snubber was inserted. For example, the RL snubber labeled I, which had a larger R_{RLsnb}, produced better damping with a smaller Q factor than the one labeled VII. This was due to the larger R_{RLsnb}, which increases the inductive reactance of the power supply line. The switching speed thus becomes lower at $t_{\mathrm{ON,HS}}$, resulting a smaller Q factor. In the same manner, the RC snubber labeled VII achieved a smaller Q factor with a smaller R_{RCsnb} than the one labeled I because a larger R_{RCsnb} makes the capacitive reactance of the low-side. This reduces the switching speed at $t_{\mathrm{ON,HS}}$, so a smaller Q factor is obtained. These effects caused by the change in switching operations are not represented in the simplified circuit.

In contrast, the errors for the RL snubber labeled VII and the RC snubber labeled I were close to those without the snubbers, 4.7. These errors were due to the fact that the snubbers have small inductive or capacitive reactance, meaning that they negligibly affect switching operations.

As shown in Fig. 4.10(b), the obtained Q factors were close to the design target for both optimized snubbers. These snubbers provided a Q factor close to the design target because a small L_{snb} or C_{snb} suppresses the negative effects on switching operations.

The reason the high gradients were obtained as seen in Fig. 4.10(a), is that the snubbers for the low Q factor targets had the high reactance, which reduced the switching speed.

Altogether, the proposed method can provide snubber circuits that achieve the Q factor design target. Minimizing the error is a challenge to be addressed in future work.

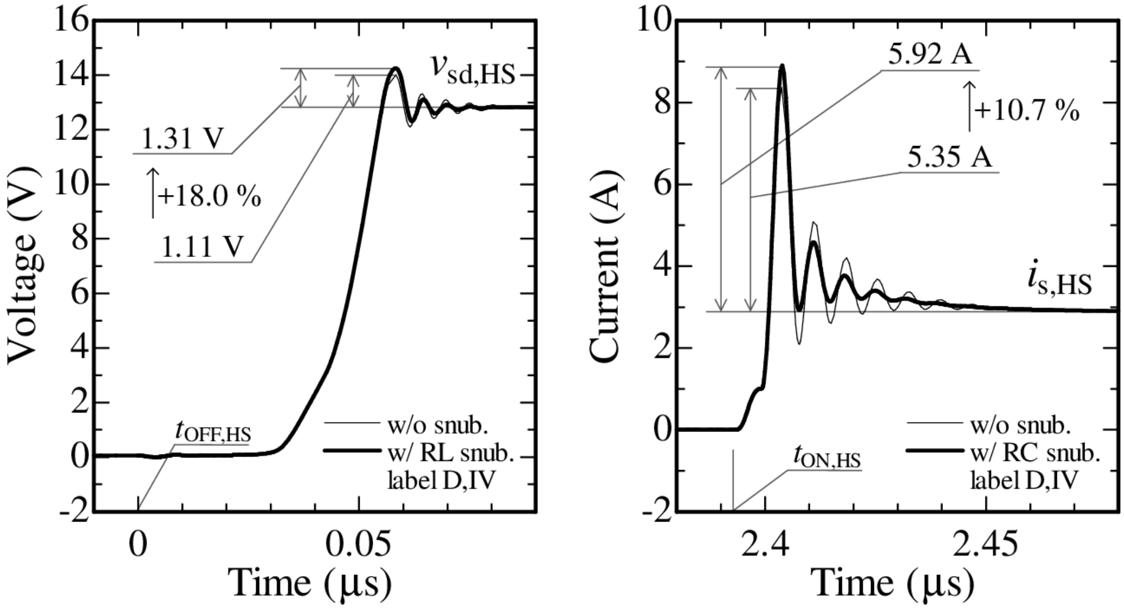
4.6 Evaluation of Negative Effects

As mentioned above, the optimized snubbers were evaluated in terms of not only resonance damping but also the negative effects: overshoot and power loss. The allowable amount of these negative effects is determined by the specifications: device performance, lifetime and heat dissipation, etc. Since these negative effects may limit the use of the snubbers, they should be minimized.

We first evaluated the increase in the negative effects when adding optimized snubbers for different design targets. The snubbers labeled A–G in Table 4.3 were used. Next, we evaluated the proposed method's ability to minimize the negative effects. The minimum L_{snb} or C_{snb} on the target Q factor line was selected as the optimum parameter. This selection method was validated by using the snubber parameters determined for the same design target, those labeled I–VII in Table 4.3.

4.6.1 Overshoots

First, the increase in the overshoot produced by the optimized snubbers was evaluated. Fig. 4.11(a) shows the calculated surge voltage of $V_{\mathrm{sd,HS}}$ at $t_{\mathrm{OFF,HS}}$, and Fig. 4.11(b) shows the inrush current of $I_{\mathrm{s,HS}}$ at $t_{\mathrm{ON,HS}}$. Example SPICE simulation results are shown in both figures, where the thin and thick lines represent transient traces simulated without and with the snubbers labeled D,IV. As shown by the waveforms in Fig. 4.11, the snubbers damped the oscillation, but the overshoot increased. The waveforms in Fig. 4.11(a) show that there were surge voltages after 0.055 μs from $t_{\mathrm{OFF,HS}}$. With the RL snubber labeled



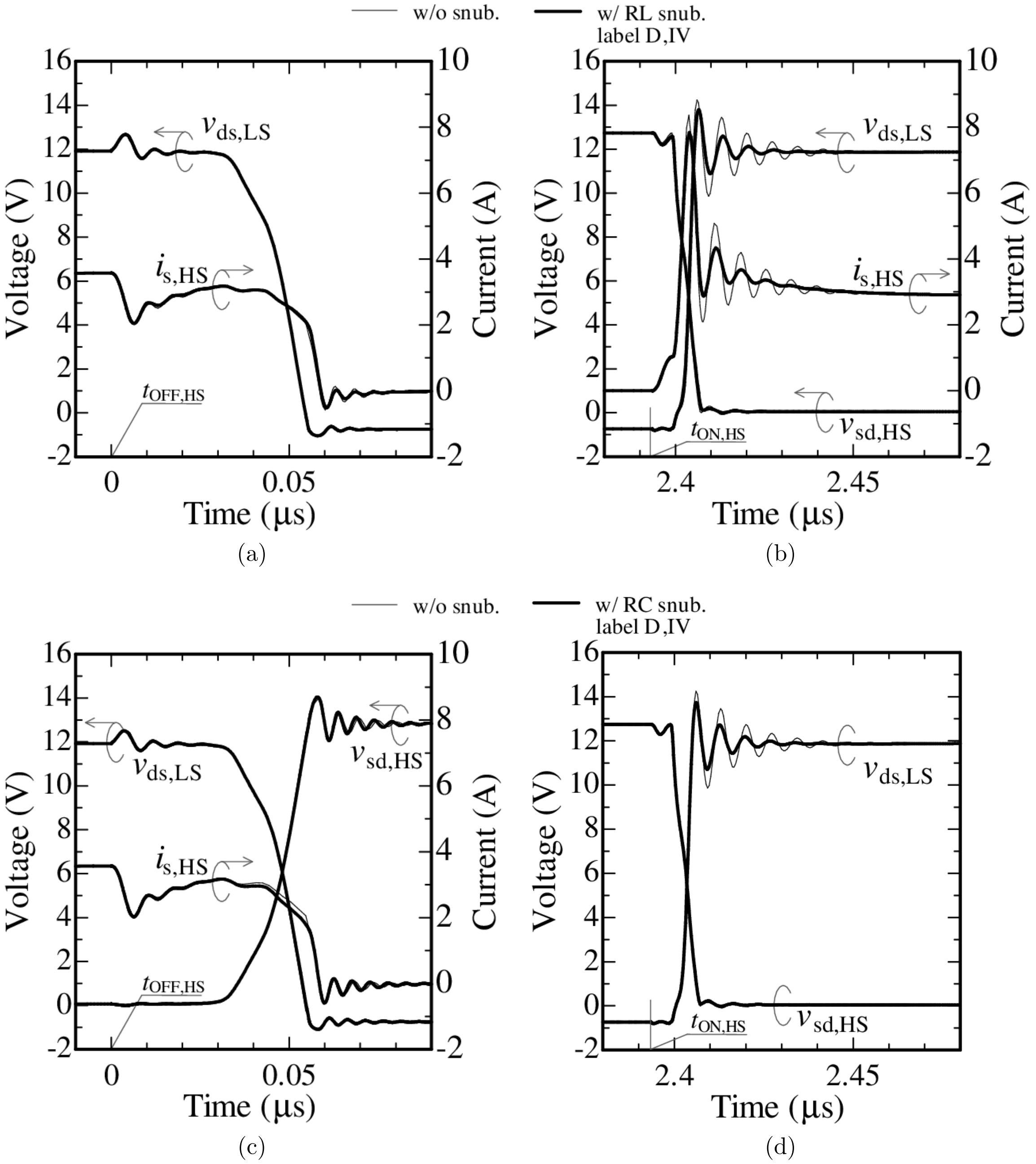
(a) (b)

Figure 4.11 Simulated steady-state waveforms of original equivalent circuit w/o and w/ optimized snubbers labeled D,Ⅳ: (a) surge voltage of $V_{\rm sd,HS}$ at $t_{\rm OFF,HS}$ and (b) inrush current of $I_{\rm s,HS}$ at $t_{\rm ON,HS}$.

D,Ⅳ, the surge voltage increased by 18.0 %. The waveforms in Fig. 4.11(b) show that there were inrush currents after 0.1 μs from $t_{\rm ON,HS}$. With the RC snubber labeled D,Ⅳ, the inrush current increased by 10.7 %. The surge voltage increase with the RL snubber resulted from the inductance increase in the power supply line. The inrush current increase with the RC snubber resulted from the increase in the capacitance of the low-side.

Fig. 4.12 shows the other waveforms simulated at the same time, $t_{\rm OFF,HS}$ and $t_{\rm ON,HS}$. Fig. 4.12(a) and Fig. 4.12(b) show the ones without and with the RL snubber labeled D,Ⅳ. Fig. 4.12(c) and Fig. 4.12(d) show the ones without and with the RC snubber labeled D,Ⅳ. The thin and thick lines represent transient traces simulated without and with the snubbers. There is no indication of an increase in the overshoot in any of the figures. The ringing amplitude reductions in $V_{\rm ds,LS}$ and $I_{\rm s,HS}$ seen in Fig. 4.12(b) and the one in $V_{\rm ds,LS}$ seen in Fig. 4.12(d) reflect the damping effects of the snubbers. The same results were obtained for the snubbers labeled A–G and I–Ⅶ.

Overshoots were also obtained from the SPICE simulations using the original circuit for the other six optimized snubber configurations, labels A–C and E–G. The increases in overshoot compared to that of the original circuit are plotted in Fig. 4.13(a) with circles for the RL snubbers and triangles for the RC snubbers. Fig. 4.13(a) shows that the overshoots increased as the Q factor design target was reduced for both the RL and RC snubbers. This indicates that there is a trade-off relationship between the damping effect and the overshoot. If a smaller overshoot is needed, the snubber inductance or the



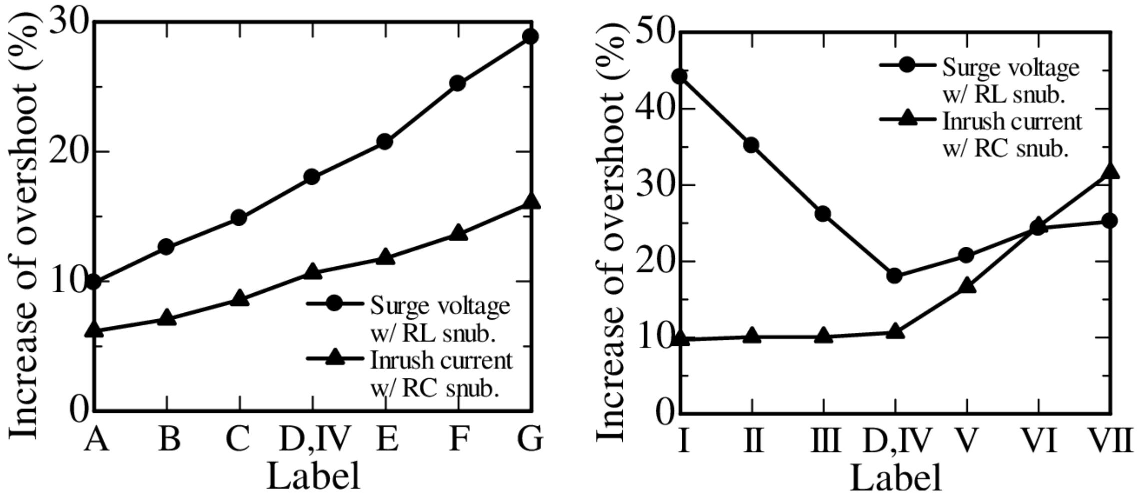
(a)

(b)

(c)

(d)

Figure 4.12 Simulated steady-state waveforms w/o and w/ optimized snubbers labeled D,IV excluding waveforms shown in Fig. 4.11 for (a) and (b) RL snubber, and (c) and (d) RC snubber.



(a)

(b)

Figure 4.13 Calculated increases in surge voltages and inrush currents with (a) optimized snubbers labeled A–G for different target Q factors and (b) snubbers labeled I–VII for same target.

capacitance has to be reduced. However, doing this reduces the damping effect, thus the Q factor design target has to be adjusted upward.

To evaluate the proposed method's ability to minimize the negative effects, we calculated the overshoots for the other sets of RL and RC snubbers labeled I–III and V–VII in the same way as for those labeled A–G. The increases are plotted in Fig. 4.13(b) with circles for the RL snubbers and with triangles for the RC snubbers. For the RL snubbers, the minimum surge voltage was obtained for label D,IV, the optimum parameters obtained with the proposed method. For the RC snubbers, the minimum inrush current was also obtained with the optimum configuration. This shows that overshoot can be minimized by using the proposed method for selecting the minimum L_{snb} or C_{snb} at the target Q factor in the contour plot.

4.6.2 Power Losses

Switching loss in the MOSFETs is the dominant loss in buck converters. To evaluate total circuit loss P_{loss}, we calculated the steady-state power loss in every circuit element, P_{element}, using SPICE simulation. These steady-state power losses are calculated by using the following equations [35]:

$$P_{\mathrm{out}} = \mathrm{average}(i_{\mathrm{out}} v_{\mathrm{out}}) \tag{4.7}$$

$$P_{\mathrm{in}} = \mathrm{average}(i_{\mathrm{in}} v_{\mathrm{in}} + i_{\mathrm{ctrl}} v_{\mathrm{ctrl}}) \tag{4.8}$$

$$P_{\mathrm{loss}} = P_{\mathrm{out}} - P_{\mathrm{in}} \tag{4.9}$$

$$P_{\mathrm{element}} = \mathrm{average}(i_{\mathrm{element}} v_{\mathrm{element}}). \tag{4.10}$$

The losses in the high-side MOSFET P_{HS}, in the low-side MOSFET P_{LS}, and in each snubber circuit P_{snb} correspond to P_{element} and were calculated using (4.10).

First, the losses incurred by adding the optimized snubbers labeled A–G were evaluated. Table 4.4 shows the calculated losses without and with the snubbers labeled D,IV. With the RL snubbers, P_{HS} slightly increased due to the increased overshoot. With the RC snubbers, P_{HS} slightly decreased due to the difference in switching operation. In both cases, P_{LS} changed very little, and P_{loss} was slightly increased and approximately accounted for the loss in the snubber circuits. These observations suggest that snubbers optimized using the proposed method can damp the resonance with an insignificant increase in power loss.

Table 4.4 Calculated Steady-state Power Losses in Original Equivalent Circuit w/o and w/ Optimized Snubber Circuits Labeled D,IV

	Loss (mW)			
Case	P_{HS}	P_{LS}	P_{snb}	P_{loss}
w/o sunb.	295.5	165.1	-	564
w/ RL snub., label D,IV	298.0 (+0.9%)	164.2 (-0.5%)	7.4	579 (+2.7%)
w/ RC snub., label D,IV	290.2 (-1.8%)	164.3 (-0.5%)	7.7	567 (+0.5%)

The calculated increases in P_{HS}, P_{LS}, and P_{loss} for the snubbers labeled A–G compared to those for the original circuit are plotted in Fig. 4.14(a) with circles for the RL snubbers and triangles for the RC snubbers. The thin solid lines, dashed lines, and thick solid lines respectively show the increases in P_{HS}, P_{LS}, and P_{loss} and the wide dashed lines show the value of P_{snb}. For the RL snubbers, there was no increase in P_{LS} while P_{HS} and P_{snb} increased slightly as the design target was reduced. This resulted in an increase in P_{loss}. For the RC snubbers, there was no increase in P_{LS} and P_{HS} while P_{snb} increased as the design target was reduced. This resulted in a slight increase in P_{loss}. This indicates that there is a trade-off relationship between the damping effect and the total power loss. These results suggest that when a smaller power loss is needed, the target Q factor has to be adjusted upward.

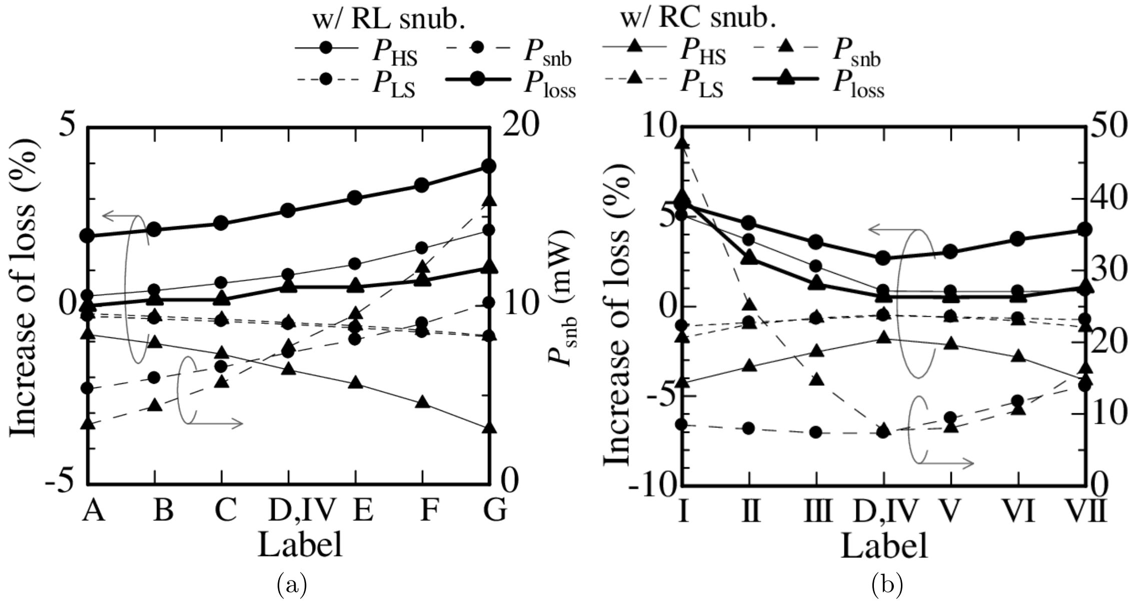


Figure 4.14 Calculated steady-state power losses with (a) optimized snubbers labeled A–G for different target Q factors and (b) snubbers labeled I–VII for same target.

To evaluate the proposed method's ability to minimize the power loss for the same design target, we calculated the power loss for other sets of RL and RC snubbers labeled I–III and V–VII in the same way as for those labeled A–G. The calculated values are plotted in Fig. 4.14(b) with circles for the RL snubbers and triangles for the RC snubbers. The thin solid lines, dashed lines, and thick solid lines respectively show the increases in P_{HS}, P_{LS}, and P_{loss} and the bold dashed lines show the value of P_{snb}. Inserting RL or RC snubbers negligibly changed P_{LS}. For the RL snubbers, label D,IV had the minimum P_{HS}, P_{snb}, and P_{loss}. For the RC snubbers, label D,IV had the minimum P_{snb} and P_{loss} even though P_{HS} was maximum. These results show that power loss can be minimized by using our method for selecting the minimum L_{snb} or C_{snb} at the target Q factor in the contour plot.

These results demonstrate that the proposed method can produce snubbers that minimize negative effects.

4.7 Conclusion

Our proposed method for optimally designing RL and RC snubber circuits to reduce electromagnetic interference caused by parasitic LC resonance uses the Q factor of a resonant loop at the resonance frequency as the design criteria. The optimum parameters are analytically and uniquely determined by deriving an equation giving the Q factor as a function of the snubber parameters from a simplified equivalent circuit and reading the minimum inductance or capacitance of the snubber along the contour line for the target

Q factor.

A synchronous buck converter was used as an application example to ascertain the method's validity. SPICE simulation was used to calculate the damping effect and negative effects (overshoot and power loss) due to adding snubbers. The simulated Q factors of the circuit to which optimized snubbers were added roughly matched various design targets. Moreover, use of these optimized snubbers resulted in minimum overshoot and power loss. These results suggest that our method is valid and useful for damping parasitic LC resonance.

For practical design purposes, it is necessary to determine snubber parameters that not only damp the resonance but also meet the overshoot and power loss requirements. With the proposed method, the optimum parameters can be easily adjusted if the Q factor design target is changed to meet these requirements. This indicates the method is useful in practical design terms.

Chapter 5

General Conclusions

The main objective of this thesis is establishing efficient EMC and HWS design methods. To improve the efficiency in product development, it is necessary two things:

(A) predicting the product performance in the design process without going through the complete trial manufacture and performance evaluation process, and

(B) optimizing the product design without trial and error.

Solving these issues, (A) and (B), with computer-aided engineering (CAE) is a current trend. CAE tools are very powerful because they can reduce trial cost in product performance prediction and design optimization, but reflecting the characteristics of the entire product to the CAE tools is unrealistic in terms of calculation cost. Therefore, a simulation method of efficient EMC and HWS performance prediction is required to reduce the calculation cost. For the efficient simulation, it is important to construct high-speed analyzable models and to narrow down the analysis dimension and range. It is preferable that the number of man-hours for constructing the model is as small as possible, and ease of model building is important. In addition, since the performance of the model depends on the condition at the time of model construction, it is necessary to properly determine the condition. Besides, even if the CAE tool is used, it is difficult to optimize a component of product composed of plural elements. If plural elements can not be simultaneously optimized, the design and simulation processes are repeated. Therefore, an optimal design method is also required. To optimize the plural elements, it is important to derive a function having the elements as a variable with respect to a criterion representing a target performance, and calculate the set of elements that satisfy the target. In deriving the function, it is practically impossible to use all the constituent elements as variables, so it is necessary to simplify the constituent elements. Since the accuracy of optimization and the application limit of optimum design depend on the simplification, appropriate simplification is important.

As concrete methods to realize (A) and (B), three studies were investigated as follows:

- noise-source equivalent circuit modeling to predict conducted disturbance for realizing (A) in EMC design,

- a study of signal-to-noise (SNR) estimation method for realizing (A) in HWS design, and
- an optimal design method of snubber circuits (a kind of filters for suppressing EMI or information leakage) for realizing (B).

The abstracts of each study are described below.

Chapter 2 described a noise-source equivalent circuit model and a proposed model identification method. A simple measurement system consisting of a data logger (or an oscilloscope) and general measurement probes was used to reduce the difficulty of model construction. In addition, the model structure, the measurement method, and the measurement accuracy were examined to decide an appropriate condition of model construction. As a result, it was possible to estimate conduction disturbance with an error within 6 dB which can be said to be practically sufficient accuracy.

Chapter 3 described a study of a SCA resistance estimation for realizing (A). We examinated two methods: a SCA resistance evaluation method based on the signal-to-noise ratio (SNR) of the side-channel trace and a side-channel trace simulation method using the EDA (electronic design automation) tool. For the former, the signal-to-noise ratio measurement method was shown. For the latter, a simpler and faster simulation method than the conventional method was shown. As a result, it showed that it can contribute to efficiency improvement of SCA resistance prediction.

Chapter 4 described an optimal design method of RL and RC snubber circuits in a case where the snubbers are applied to a synchronous buck converter for realizing (B). For optimization, the converter circuit was simplified with considering the inpedance magnitude of components at the target frequency. It was shown that the optimum parameters can be analytically and uniquely determined by deriving the equation with the Q factor (objective function) and the snubber parameters (variables) in the simplified equivalent circuit.

As mentioned above, in each study, a method for realizing efficient EMC or HWS design was proposed and its validity was demonstrated. The innovative techniques presented in this thesis is useful for efficient EMC and/or HWS design.

Appendix A

Impedance Stabilization Network

In Section 2.7, the impedance stabilization network (ISN) was used. The ISN was made by us to keep the impedance of DC power supply side constant. In general, the LISN is used for measuring conducted disturbance, but impedance can not be kept constant at frequencies over 30 MHz. Therefore, a circuit that keeps impedance constant at high frequencies like ISN is necessary.

Fig. A.1 shows the ISN circuit including parasitic impedance. This ISN has the same circuit configuration as LISN. By inserting an inductor in the DC supply line, the DC power supply side and EUT side are decoupled at high-frequency, and input and output impedance are controlled by capacitors and resistors inserted between the DC supply line and GND. Fig. A.2 shows the input impedance of EUT side. The input impedance looking leftward from the EUT is kept at 50 Ω.

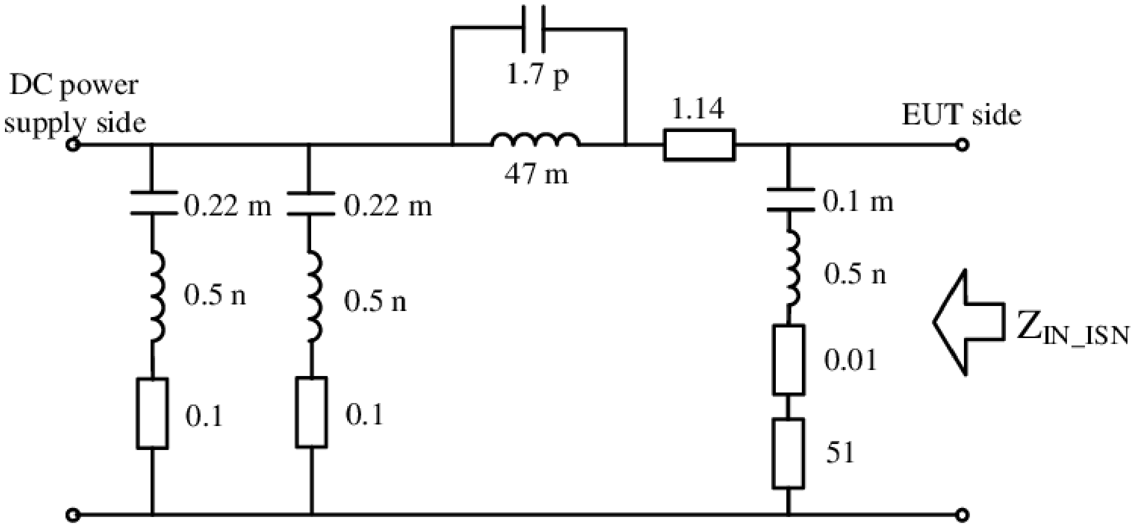
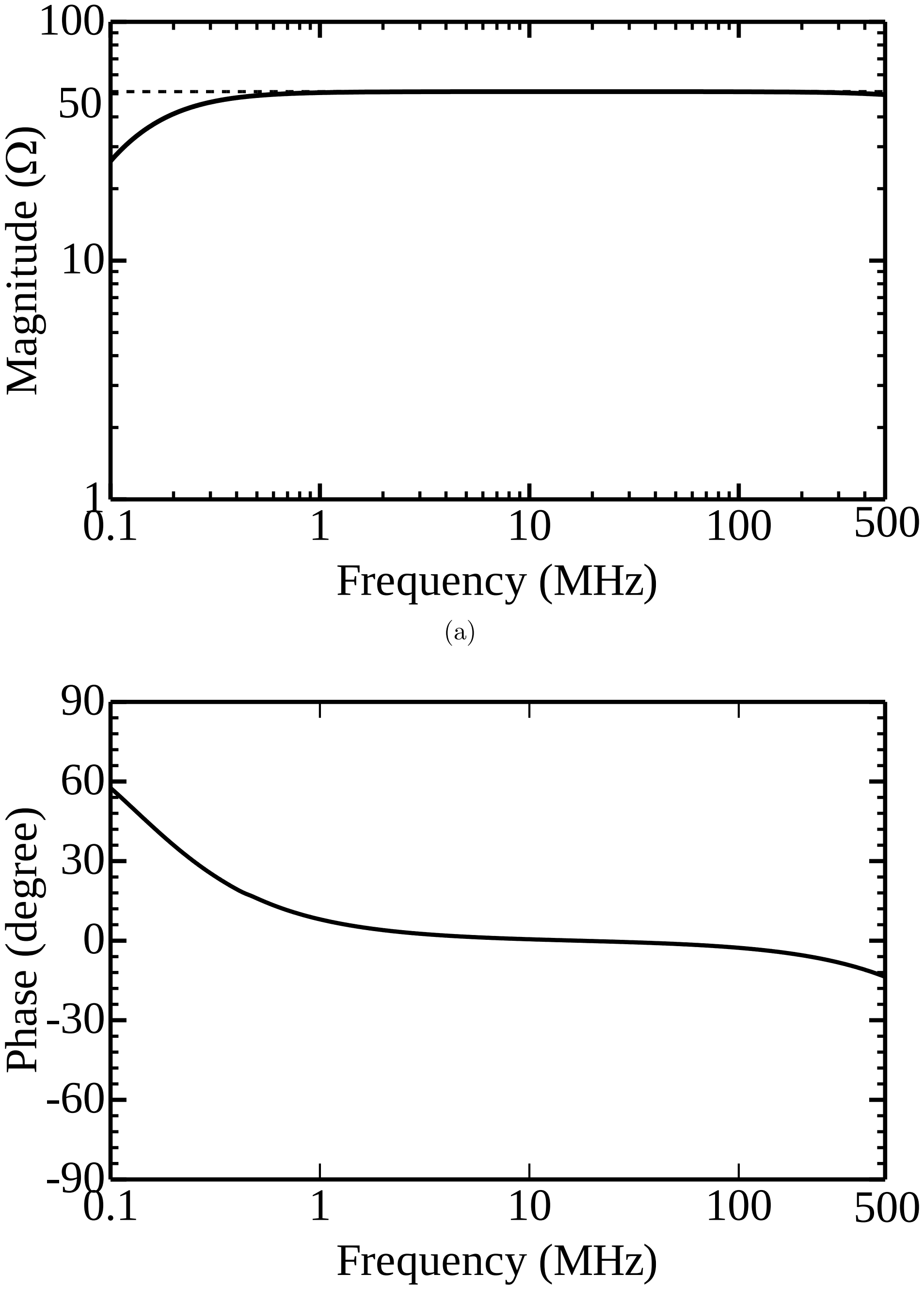


Figure A.1 Impedance stabilization network circuit including parasitic impedance.



(a)

(b)

Figure A.2 Input impedance of impedance stabilization network: (a) magnitude and (b) phase.

Bibliography

[1] J. A. Stankovic, "Research directions for the internet of things," *IEEE Internet of Things Journal*, vol. 1, no. 1, pp. 3–9, Feb 2014.

[2] 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.

[3] Jvndb-2018-001001: Side channel attacks on cpu. [Online]. Available: https://jvndb.jvn.jp/ja/contents/2018/JVNDB-2018-001001.html

[4] Cve-2017-5715. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-5715

[5] J. Miyashita, M. Mitsuzawa, T. Karube, K. Yamazawa, and T. Sato, "A quantitative analysis of common-mode noise of a switching power supply," *IEICE Transactions on Electronics (Japanese edition)*, vol. J84-B, no. 3, pp. 643–646, Mar 2001.

[6] M. Tamate, T. Sasaki, and A. Toba, "Quantitative estimation of conducted emission from an inverter system," *IEEJ Transactions on Industry Applications*, vol. 128, pp. 193–200, Jan 2008.

[7] Y. Fukumoto, Y. Takahata, O. Wada, Y. Toyota, T. Miyashita, and R. Koga, "Power current model of LSI/IC containing equivalent internal impedance for EMI analysis of digital circuits," *IEICE Trans. Commun.*, vol. E84-B, no. 11, pp. 3041–3049, Nov 2001.

[8] K. Iokibe, R. Higashi, T. Tsuda, K. Ichikawa, K. Nakamura, Y. Toyota, and R. Koga, "Validation of multiple power-supply-pin LECCS-core model for conducted RF power current simulation," *IEICE Transactions on Electronics (Japanese edition)*, vol. J93-C, no. 11, pp. 516–520, Nov 2010. (in Japanese).

[9] 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, Jun 2013.

[10] P. Hillenbrand, M. Böttcher, S. Tenbohlen, and J. Hansen, "Frequency domain EMI-simulation and resonance analysis of a DCDC-converter," in *2016 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, Wroclaw, Poland, Sep 2016, pp. 176–181.

[11] C. Marlier, A. Videt, N. Idir, H. Moussa, and R. Meuret, "Hybrid time-frequency EMI noise sources modeling method," in *2013 15th European Conference on Power Electronics and Applications (EPE), DS3a-820*, Lille, France, Sep 2013, pp. 1–9.

[12] V. Tarateeraseth, B. Hu, K. Y. See, and F. G. Canavero, "Accurate extraction of noise source impedance of an SMPS under operating conditions," *IEEE Trans. Power Electron.*, vol. 25, no. 1, pp. 111–117, Jan 2010.

[13] H. Geshi, K. Iokibe, Y. Toyota, and T. Watanabe, "Conducted disturbance estimation of power converter circuits based on linear equivalent circuit model for EMI filter design," in *Eighth 2015 Korea-Japan Joint Conference on EMT/EMC/BE (KJJC-2015)*, Sendai, Japan, Nov 2015.

[14] Y. Yano, H. Geshi, K. Iokibe, T. Watanabe, and Y. Toyota, "Linear equivalent circuit modeling of power converter circuit for condunted disturbance estimation — impact of trigger timing on the modeling —," in *IEICE Tech. Rep.*, vol. 116, no. 26, EMCJ2016-16, May 2016, pp. 41–45. (In Japanese).

[15] ——, "A study of linear equivalent circuit modeling for conducted disturbance estimation of power converter circuit," in *2016 URSI Asia-Pacific Radio Science Conference (AP-RASC 2016), S-E1-5*, Seoul, Korea, Aug 2016.

[16] K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "Prototype IC with WDDL and differential routing – DPA resistance assessment," *in CHES'05*, pp. 354–365, Aug. 2005.

[17] E. Brier, C. Clavier, and F. Olivier, *Correlation power analysis with a leakage model.* Berlin, Heidelberg: in Proc. Cryptographic Hardware and Embedded Systems, Chap.2, Springer, 2007.

[18] ISO/IEC 17825:2016, Information technology – Security techniques – Testing methods for the mitigation of non-invasive attack classes against cryptographic modules, 2016.

[19] S. Bhasin, J. Danger, S. Guilley, and Z. Najm, "NICV: Normalized inter-class variance for detection of side-channel leakage," in *2014 International Symposium on Electromagnetic Compatibility, Tokyo*, May 2014, pp. 310–313.

[20] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security).* Berlin, Heidelberg: Chap.4, Springer, 2007.

[21] ——, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Advances in Information Security).* Berlin, Heidelberg: Chap.6, Springer, 2007.

[22] F. Regazzoni, S. Badel, T. Eisenbarth, J. Grobschadl, A. Poschmann, Z. Toprak, M. Macchetti, L. Pozzi, C. Paar, Y. Leblebici, and P. Ienne, "A simulation-based methodology for evaluating the dpa-resistance of cryptographic functional units with application to cmos and mcml technologies," in *2007 International Conference on Embedded Computer Systems: Architectures, Modeling and Simulation*, July 2007, pp. 209–214.

[23] D. Fujimoto, T. Katashita, A. Sasaki, Y. Hori, A. Satoh, and M. Nagata, "A fast power current simulation of cryptographic VLSI circuits for side channel attack evaluation," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E96.A, pp. 2533–2541, 12 2013.

[24] I. Zamek, P. Boyle, Z. Li, S. Sun, D. G. Beetner, J. L. Drewniak, X. Chen, T. Li, and S. Chandra, "Modeling FPGA current waveform and spectrum and PDN noise estimation," in *DesignCon 2008*, Santa Clara, CA, USA, Jun 2008, pp. 1577–1601.

[25] L. Ren, T. Li, S. Chandra, X. Chen, H. Bishnoi, S. Sun, P. Boyle, I. Zamek, J. Fan, D. G. Beetner, and J. L. Drewniak, "Prediction of power supply noise from switching activity in an FPGA," *IEEE Trans. Electromagn. Compat.*, vol. 56, no. 3, pp. 699–706, Jun 2014.

[26] M. Kirschbaum and T. Pop, "Evaluation of power estimation methods based on logic simulations."

[27] A. Kumar, C. Scarborough, A. Yilmaz, and M. Orshansky, "Efficient simulation of EM side-channel attack resilience," in *2017 IEEE ACM International Conference on Computer-Aided Design (ICCAD)*, Nov 2017, pp. 123–130.

[28] I. Kontorovitch, V. Drabkin, C. Houghton, and J. Laurent, "Measurements of impedance, current and worst-case noise on chip power delivery system under operating conditions," in *DesignCon 2005*, Munich, Germany, Oct 2005.

[29] R. Schmitt, H. Lan, C. Madden, and C. Yuan, "Investigating the impact of supply noise on the jitter in gigabit i/o interfaces," in *2007 IEEE Electrical Performance of Electronic Packaging*, Oct 2007, pp. 189–192.

[30] M. Badaroglu, G. V. der Plas, P. Wambacq, S. Donnay, G. G. E. Gielen, and H. J. D. Man, "Swan: high-level simulation methodology for digital substrate noise generation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 14, no. 1, pp. 23–33, Jan 2006.

[31] T. Sugawara, Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, H. Sone, and A. Satoh, “Spectrum analysis of cryptographic modules to counteract side-channel attacks,” in *2009 International Symposium on Electromagnetic Compatibility*, no. 21P1-6, Kyoto, Japan, Jul 2009, pp. 21–24.

[32] N. Kawata, Y. Yano, K. Iokibe, and Y. Toyota, “Insertion of LC resonator onto cryptographic module for accelerated evaluation of side channel attack,” in *IEICE Tech. Rep.*, vol. 117, no. 384, Kurashiki, Japan, Jun 2018, pp. 77–81. (in Japanese).

[33] K. Kam, D. Pommerenke, F. Centola, C. W. Lam, and R. Steinfeld, “Method to suppress the parasitic resonance using parallel resistor and inductor combination to reduce broadband noise from DC/DC converter,” in *2009 International Symposium on Electromagnetic Compatibility*, Kyoto, Japan, Jul 2009, pp. 353–356.

[34] ——, “EMC guideline for synchronous buck converter design,” in *2009 IEEE International Symposium on Electromagnetic Compatibility*, Austin, TX, USA, Aug 2009, pp. 47–52.

[35] R. Blecic, R. Gillon, B. Nauwelaers, and A. Baric, “SPICE analysis of RL and RC snubber circuits for synchronous buck DC-DC converters,” in *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, Opatija, Croatia, May 2015, pp. 91–97.

[36] H. S. Shin, H. A. Huynh, and S. Kim, “Design and optimization of inductive snubber for DC-DC converter,” in *2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC)*, Seoul, South Korea, June 2017, pp. 148–150.

[37] K. Iokibe, Y. Yano, and Y. Toyota, “Insertion of parallel RL circuits into power distribution network for simultaneous switching current reduction and power integrity,” in *2012 Asia-Pacific Symposium on Electromagnetic Compatibility (APEMC)*, May 2012, pp. 417–420.

[38] K. Iokibe, R. Yamagata, and Y. Toyota, “RL snubbers on power distribution network of integrated circuits for conducted electromagnetic interference reduction and power integrity,” *IEICE Transactions on Communications (Japanese edition)*, vol. J97-B, pp. 497–506, Jul 2014. (in Japanease).

[39] K. Harada and T. Ninomiya, “Optimum design of RC snubbers for switching regulators,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. AES-15, pp. 209–218, March 1979.

[40] CISPR 14-1 : Electromagnetic compatibility - Requirements for household appliances, electric tools and similar apparatus - Part 1: Emission, Ed.6.0, 2016.

[41] CISPR 16-2-1: Specification for radio disturbance and immunity measuring apparatus and methods — Part 2-1, Methods of measurement of disturbances and immunity — Conducted disturbance measurements, Ed.2.0, 2008.

[42] S. Inoue, K. Iokibe, T. Watanabe, and Y. Toyota, “Equivalent circuit modeling of power converter circuit for conducted disturbance estimation — determination of model parameters by use of dual port LISN —,” in *IEICE Tech. Rep.*, vol. 112, no. 100, EMCJ2012-24, Jun 2012, pp. 17–22. (In Japanese).

[43] CISPR 16-1-2: Specification for radio disturbance and immunity measuring apparatus and methods — Part 1-2, Radio disturbance and immunity measuring apparatus — Ancillary equipment — Conducted disturbances, Ed.1.2, 2006.

[44] Y. Osaki, Y. Yano, K. Iokibe, and Y. Toyota, “Parameter identification of a noise-source linear equivalent circuit of DC-DC converter,” in *IEICE Tech. Rep.*, vol. 117, no. 1, EMCJ2017-6, Apr 2017, pp. 29–34. (In Japanese).

[45] Y. Osaki, Y. Yano, T. Uematsu, K. Iokibe, and Y. Toyota, “Parameter identification of noise-source linear equivalent circuit of DC-DC converter and its evaluation,” in *2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2017), TH-AM-5-04*, Seoul, Korea, Jun 2017.

[46] ——, “Improvement of prediction accuracy by improving parameters extraction in a 2-port noise-source equivalent circuit model of DC/DC converter,” in *IEICE Tech. Rep.*, vol. 118, no. 406, EMCJ2018-101, Jan 2019, pp. 7–12. (In Japanese).

[47] S. Okada and R. Onodera, “The simplest equivalent circuit of a multi-terminal network,” in *RAAG Memoirs, 1, A-II*, 1955, pp. 68–112.

[48] M. Hosoya, “The simplest equivalent circuit of a multi-terminal network,” in *Bulletin of the College of Science, University of the Ryukyus*, no. 70, Sep 2000, pp. 1–10.

[49] K. Kawabata, *Application Statistics Handbook (Ouyou toukei handobukku).* Chap.2, Yokendo, 2007. (in Japanese).

[50] 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, Jun. 2013.

[51] 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,” in *2015 IEEE International Symposium on Electromagnetic Compatibility (EMC)*, Aug 2015, pp. 224–229.

[52] F. L. Luo and H. Ye, “Investigation of EMI, EMS and EMC in power DC/DC converters,” in *The Fifth International Conference on Power Electronics and Drive Systems, 2003. PEDS 2003.*, Singapore, Nov 2003, pp. 572–577.

[53] K. W. Kam, D. Pommerenke, C. W. Lam, and R. Steinfeld, “EMI analysis methods for synchronous buck converter EMI root cause analysis,” in *2008 IEEE International Symposium on Electromagnetic Compatibility*, Detroit, MI, USA, Aug 2008, pp. 1–7.

[54] A. Bhargava, D. Pommerenke, K. W. Kam, F. Centola, and C. W. Lam, “DC-DC buck converter EMI reduction using PCB layout modification,” *IEEE Trans. Electromagn. Compat.*, vol. 53, no. 3, pp. 806–813, Aug 2011.

[55] K. Kam, D. Pommerenke, A. Bhargava, B. Steinfeld, C. W. Lam, and F. Centola, “Quantification of self-damping of power MOSFET in a synchronous buck converter,” *IEEE Trans. Electromagn. Compat.*, vol. 53, pp. 1091–1093, Nov 2011.

[56] J. Roig, C. F. Tong, F. Bauwens, R. Gillon, H. Massie, and C. Hoggatt, “Internal self-damping optimization in trench power FETs for high-frequency conversion,” in *2014 IEEE Applied Power Electronics Conference and Exposition (APEC 2014)*, Fort Worth, TX, USA, March 2014, pp. 137–142.

Research Activities

Paper

1. **Yusuke Yano**, Naoki Kawata, Kengo Iokibe, Yoshitaka Toyota, "A Method for Optimally Designing Snubber Circuits for Buck Converter Circuits to Damp LC Resonance," *IEEE Transactions on Electromagnetic Compatibility*, Jun. 2018. DOI: 10.1109/TEMC.2018.2841424. (Early access).

2. Shinpei Yoshino, Kengo Iokibe, **Yusuke Yano**, Yoshitaka, "Intensity Estimation of Electromagnetic Emission from Individual ICs Based on Noise Source Amplitude Modulation and Correlation Analysis," *Journal of The Japan Institute of Electronics Packaging*, (Accepted).

International Conferences

1. Kengo Iokibe, **Yusuke Yano**, Yoshitaka Toyota, Ryuji Koga, "Increase of RF Power Current Due to Coupling between Power Distribution and IO Networks," *2010 Asia-Pacific Radio Science Conference (AP-RASC'10)*, EP-4, Toyama, Japan, Sep. 2010.

2. Kengo Iokibe, **Yusuke Yano**, Yoshitaka Toyota, "Insertion of Parallel RL Circuits into Power Distribution Network for Simultaneous Switching Current Reduction and Power Integrity," *2012 Asia-Pacific Internationl Symposium on Electromagnetic Compatibility in Singapore (APEMC 2012).* WE-PM-SI1-4, pp. 417-420, Singapore, May. 2012.

3. **Yusuke Yano**, Hiroki Geshi, Kengo Iokibe, Tetsushi Watanabe, Yoshitaka Toyota, "A Study of Linear Equivalent Circuit Modeling for Conducted Disturbance Estimation of Power Converter Circuit," *2016 URSI Asia-Pacific Radio Science Conference (AP-RASC 2016)*, S-E1-5, Seoul, Korea, Aug. 2016.

4. **Yusuke Yano**, Toshiaki Teshima, Kengo Iokibe, Yoshitaka Toyota, "Signal-to-Noise Ratio Measurements of Side-Channel Traces for Establishing Low-Cost Countermeasure Design," *2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2017)*, WE-PM-7-02, Seoul, Korea, Jun. 2017.

5. Yuhei Osaki, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Parameter Identification of Noise-source Linear Equivalent Circuit of DC-DC Converter and Its Evaluation," *2017 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2017)*, TH-AM-5-04, Seoul, Korea, Jun. 2017.

6. Kengo Iokibe, Toshiaki Teshima, **Yusuke Yano**, Yoshitaka Toyota, "Extension of Signal-to-Noise Ratio Measurement Method to Byte-by-Byte Side-Channel Attack," *2018 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC 2018)*, WE-PM-I-SS-09-3, Singapore, May 2018.

7. **Yusuke Yano**, Toshiaki Teshima, Kengo Iokibe, Yoshitaka Toyota, "Experimental Identification of Relationship between Leakage Trace SNR and Correlation Coefficient in Differential Power Analysis," *2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility, Sapporo (EMC Sapporo & APEMC 2019)*, Sapporo, Jun. 2019. (submitted)

8. Uematsu Taishi, Yuhei Osaki, Yoshitaka Toyota, **Yusuke Yano**, Kengo Iokibe, "Improvement of Prediction Accuracy of Noise-source Equivalent-circuit Model Based on Parameter Extraction by Port Voltage/Current Measurement," *2019 Joint International Symposium on Electromagnetic Compatibility and Asia-Pacific International Symposium on Electromagnetic Compatibility*, Sapporo (EMC Sapporo & APEMC 2019), Sapporo, Jun. 2019. (submitted)

Technical Report

1. **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, Ryuji Koga, "Effective Position of Decoupling Inductor Taking Parasitic Capacitances on Power Distribution Network Traces into Account," *IEICE technical report*, vol. 110, no. 125, EMCJ2010-28, pp. 39-44, Jul. 2010. (in Japanese)

2. **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Insertion of Dumping Resistor to Reduce RF IC-Power-Current Peak Caused by Resonance due to Parasitic Impedance," *IEICE technical report*, vol. 111, no. 256, EMCJ2011-84, pp. 29-34, Oct. 2011. (in Japanese)

3. Ryosuke Yamagata, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "RL Damper Circuit for Electoromagnetic Compatibility and Power Integrity of Integrated Circuits," *IEICE technical report*, vol. 112, no. 12, EMCJ2012-8, pp. 43-48. Apr. 2012. (in Japanese)

4. **Yusuke Yano**, Hiroki Geshi, Kengo Iokibe, Tetsushi Watanabe, Yoshitaka Toyota, "Linear Equivalent Circuit Modeling of Power Converter Circuit for Condunted Disturbance Estimation — Impact of Trigger Timing on the modeling —," *IEICE*

technical report, vol. 116, no. 26, EMCJ2016-16, pp. 41-45. May 2012. (in Japanese)

5. **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Investigation of Relationship between Signal-to-Noise Ratio of EM Information Leakage and Side-Channel Attacking Cost," *EMC Joint Workshop 2016 Taipei, IEICE technical report*, vol. 116, EMCJ2016-25, pp. 23-24, Jun. 2016.

6. Naoki Kawata, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Validation of Optimization Method of On-board RL Snubber According to Q Factor," *EMC Joint Workshop 2016 Taipei, IEICE technical report*, vol. 116, EMCJ2016-27, pp. 29-30, Jun. 2016.

7. Kengo Iokibe, Naoki Kawata, **Yusuke Yano**, Hiroto Kagotani, Yoshitaka Toyota, "Attempt for Determining Cryptographic Circuit Blocks Leaking Side-Channel Information Based on Internal Current Source — Examination with FPGA Implementation of AES Circuits —," *IEICE technical report*, vol. 116, no. 253, EMCJ2016-74, pp. 79-84. Oct. 2016. (in Japanese)

8. Yuhei Osaki, **Yusuke Yano**, Yoshitaka Toyota, Kengo Iokibe, "Parameter Identification of a Noise-source Linear Equivalent Circuit of DC-DC Converter," *IEICE technical report*, vol. 117, no. 1, EMCJ2017-6, pp. 29-34. Apr. 2017. (in Japanese)

9. Yasunari Kumano, **Yusuke Yano**, Kengo Iokibe, Hiroto Kagotani, Yoshitaka Toyota, "Electromagnetic Information Leakage Analysis of Cryptographic IC in Correlation Power Analysis," *EMC Joint Workshop 2017, IEICE technical report*, vol. 117, no. 32, EMCJ2017-10, pp. 7-8, Singapore, May. 2017.

10. Naoki Kawata, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Insertion of LC Resonator onto Cryptographic Module for Accelerated Evaluation of Side Channel Attack," *IEICE technical report*, vol. 117, no. 384, EMCJ2017-101, pp. 77-81, Jan. 2018. (in Japanese)

11. Yuhei Osaki, **Yusuke Yano**, Taishi Uematsu, Yoshitaka Toyota, Kengo Iokibe, "Improvement of Prediction Accuracy by Improving Parameters Extraction in A 2-port Noise-source Equivalent Circuit Model of DC/DC Converter," *IEICE technical report*, vol. 118, no. 406, EMCJ2018-101, pp. 7-12, Jun. 2019. (in Japanese)

Others

1. Kengo Iokibe, **Yusuke Yano**, Yoshitaka Toyota, "Enhancement of ICs in EMC Performance by Use of Critical Damping of Power Distribution Network Resonance," *The 26th JIEP Annual Meeting*, 8A-19, pp. 98-101, Tokyo, Mar. 2012. (in Japanese)

2. **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "A Study on Signal-to-Noise Ratio of Side-Channel Traces for Evaluation of Attacking Cost of Cryptographic Modules," *The 2016 IEICE General Conference*, B-4-61, Hukuoka, Japan, Mar. 2016. (in Japanese)

3. Naoki Kawata, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Optimization Method of On-board RL Snubber Parameters in Common Power Distribution Networks," *The 2016 IEICE General Conference*, B-4-41, Hukuoka, Japan, Mar. 2016. (in Japanese)

4. Kengo Iokibe, **Yusuke Yano**, Yoshitaka Toyota, "Analysis of Side-Channel Leakage Behavior of Cryptographic Circuit Based on Near Field Magnetic Field Scan," *The 2016 IEICE Society Conference*, B-4-50, Sapporo, Japan, Sep. 2016. (in Japanese)

5. Naoki Kawata, Shinpei Yoshino, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Analysis Formula to Determine Optimal Resistance of On-board RL Snubber Mounted in Power Distribution Network for Digital ICs," *the 67th Chugoku-section Joint Convention of Institutes of Electrical Engineering and Institutes of Electronics Information and Communication Engineers*, R16-09-03, Hiroshima, Japan, Oct. 2016. (in Japanese)

6. **Yusuke Yano**, Toshiaki Teshima, Kengo Iokibe, Yoshitaka Toyota, "Signal-to-Noise Ratio Measurements of Side-Channel Trace for Establishing Low-Cost Countermeasure Design," *2017 Symposium on Cryptography and Information Security (SCIS 2017)*, 3C3-1, Naha, Japan, Jan. 2017. (in Japanese)

7. Toshiaki Teshima, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "A Study of Chosen Plaintexts Having Equivalent Probability Distribution to Population in Hamming Distance for Cost Reduction of Security Evaluation against Side-Channel Attacks," *Technical Committee on Hardware Security (HWS)*, Hirosaki, Jun. 2017. (in Japanese)

8. Yasunari Kumano, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Study of Side Channel Attack Countermeasure for AES Circuit to Suppress Increase of Chip Area Consumption — In Case of Attack with HD Power Model —," *2018 Symposium on Cryptography and Information Security (SCIS 2018)*, 1D2-1, Niigata, Japan, Jan. 2018. (in Japanese)

9. Toshiaki Teshima, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, "Signal-to-Noise Ratio Measurements of Side-Channel Traces Leaked from AES Circuit — Application to key decryption in bytes —," *2018 Symposium on Cryptography and Information Security (SCIS 2018)*, 1D2-2, Niigata, Japan, Jan. 2018. (in Japanese)

10. Toshiaki Teshima, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, “Study on Signal-to-Noise Ratio Simulation of Side-Channel Traces Leaked from AES Circuit using EDA tool,” *Technical Committee on Hardware Security (HWS)*, Osaka, Oct. 2018. (in Japanese)

11. Toshiaki Teshima, **Yusuke Yano**, Kengo Iokibe, Yoshitaka Toyota, “Experimental Identification of Relational Formula Parameters of Leakage Trace SNR and Correlation Coefficient in Differential Power Analysis,” *2019 Symposium on Cryptography and Information Security (SCIS 2019)*, 2D3-4, Shiga, Japan, Jan. 2019. (in Japanese)

Biography

Yusuke Yano was born in Ehime, Japan, on December 20, 1987. He received a B.S. degree in communication and network engineering and an M.S. degree in electronic and information systems engineering from Okayama University, Okayama, Japan, in 2010 and 2012, respectively. From 2012 to 2016, he worked at Sumitomo Electric Industries, Ltd. and he is now working toward a Ph.D. degree in electronic and information systems engineering. His research interests include developing methods for evaluating the security of cryptographic devices against side-channel analysis attacks, electromagnetic compatibility (EMC) design, and EMC modeling of power converter circuits. Mr. Yano is a student member of the Institute of Electronics, Information and Communication Engineers (IEICE).