


May 2017

Exploiting On-Chip Voltage Regulators as a Countermeasure Against Power Analysis Attacks

Weize Yu

University of South Florida, weizeyu@mail.usf.edu

Follow this and additional works at: <http://scholarcommons.usf.edu/etd>

 Part of the [Computer Engineering Commons](#), and the [Electrical and Computer Engineering Commons](#)

Scholar Commons Citation

Yu, Weize, "Exploiting On-Chip Voltage Regulators as a Countermeasure Against Power Analysis Attacks" (2017). *Graduate Theses and Dissertations*.

<http://scholarcommons.usf.edu/etd/6986>

This Dissertation is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

Exploiting On-Chip Voltage Regulators as a Countermeasure Against Power Analysis Attacks

by

Weize Yu

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
Department of Electrical Engineering
College of Engineering
University of South Florida

Major Professor: Selçuk Köse, Ph.D.
Lingling Fan, Ph.D.
Ismail Uysal, Ph.D.
Srinivas Katkoori, Ph.D.
Ulya Karpuzcu, Ph.D.

Date of Approval:
February 22, 2017

Keywords: Hardware security, side-channel attacks, differential power analysis attacks, leakage power analysis attacks, on-chip voltage regulation

Copyright © 2017, Weize Yu

DEDICATION

This work is dedicated to my parents and girlfriend.

ACKNOWLEDGMENTS

Almost three years have passed since I transferred from Virginia Tech to University of South Florida (USF) to pursue my Ph.D. degree. During this period, a number of individuals helped and encouraged me to finish my Ph.D. study. Firstly, I would like to express my great appreciation to my Ph.D. supervisor Dr. Selçuk Köse. I remember when I applied to the Ph.D. program of electrical engineering department of USF in Fall 2014, Dr. Selçuk Köse tried his best to help me to get the prestigious USF presidential doctoral fellowship which is offered only to top five Ph.D. students each year. Owing to the awarded fellowship from USF, I became quite self-confident and produced a good number of creative works during my Ph.D. study. Dr. Selçuk Köse played a significant role in guiding my research. When I was enrolled in USF, Dr. Selçuk Köse wanted me to do research on hardware security. At first, I had made a little progress in my research since I did not have much background in hardware security. In order to strengthen my research abilities, Dr. Selçuk Köse persuaded me to take a lot of courses from computer science and engineering department. These courses facilitated my self-learning and self-analyzing abilities, which helped me greatly in publishing creative works.

I also would like to thank my lab mates Orhun Aras Uzun, Mahmood Azhar, and Longfei Wang for their selfless support. When I was starting my research with Cadence simulations, I came across some technical issues. However, Orhun devoted his time and patience to guide me to solve those issues. When I have new ideas on my research topic, Longfei always showed interest in discussing with me to improve my idea.

I would also like to thank all my Ph.D. committee members: Dr. Lingling Fan, Dr. Ismail Uysal, Dr. Srinivas Katkoori, Dr. Ulya Karpuzcu, and Dr. Mingyang Li for their time, support, and encouragement.

Finally, I would like to thank my parents and Jia Chen for their unconditional support every time when I ran into difficulties in my Ph.D. study.

TABLE OF CONTENTS

LIST OF TABLES	iv
LIST OF FIGURES	v
ABSTRACT	xi
CHAPTER 1: INTRODUCTION	1
1.1 Side-Channel Attacks	1
1.2 Power Analysis Attacks	2
1.2.1 Simple Power Analysis (SPA) Attacks	2
1.2.2 Differential Power Analysis (DPA) Attacks	3
1.2.3 Leakage Power Analysis (LPA) Attacks	4
1.3 On-Chip Voltage Regulation Against Power Analysis Attacks	5
1.3.1 Converter-Gating (CoGa) Voltage Converter Against Power Analysis Attacks	5
1.3.2 Our Contribution	8
CHAPTER 2: CONVERTER-RESHUFFLING TECHNIQUE	9
2.1 Motivation	9
2.2 Treat Model	10
2.3 Review of Converter-Gating (CoGa)	11
2.4 Converter-Reshuffling (CoRe)	12
2.5 Evaluation	12
2.6 Conclusion	18
CHAPTER 3: TIME-DELAYED CONVERTER-RESHUFFLING TECHNIQUE	19
3.1 Motivation	19
3.2 Modeling	19
3.2.1 Converter-Reshuffling (CoRe) Technique	20
3.2.2 Time-delayed Converter-Reshuffling (CoRe) Technique	23
3.3 Results and Discussions	27
3.4 Conclusion	29
CHAPTER 4: CHARGE-WITHHELD CONVERTER-RESHUFFLING TECHNIQUE	31
4.1 Motivation	31
4.2 Architecture Design	32
4.2.1 Architecture of the Converter-Reshuffling (CoRe) Technique	32

4.2.2	Architecture of the Charge-Withheld Converter-Reshuffling (CoRe) Technique	34
4.3	Security Evaluation Model	36
4.3.1	Security Evaluation Against DPA Attacks	36
4.3.2	Security Evaluation Against Machine Learning (ML)-Based DPA Attacks	39
4.4	Efficiency Analysis	41
4.5	Results and Discussions	42
4.6	Conclusion	44
CHAPTER 5: CO-DESIGNING CORE TECHNIQUE WITH AES ENGINE		45
5.1	Introduction	45
5.2	Security of a Switching Converter against Power Analysis Attacks	48
5.3	Correlation Analysis of On-Chip Voltage Regulators	49
5.3.1	Modeling Correlation Coefficient of Converter-Gating (CoGa) and Converter-Reshuffling (CoRe) Regulators	49
5.3.2	Modeling Correlation Coefficient of Conventional On-Chip Voltage Regulators	55
5.3.3	Validation of the Proposed Correlation Coefficient Models with Practical Parameters	56
5.4	Conventional Pipelined (CP) AES Engine with Converter-Reshuffling	60
5.4.1	Practical Power Attacks on a Pipelined AES Engine without On-Chip Voltage Regulation	60
5.4.2	Conventional Pipelined (CP) AES Engine with a Distributed CoRe Technique	60
5.4.3	Conventional Pipelined (CP) AES Engine with a Centralized CoRe Technique	62
5.5	Improved Pipelined (IP) AES Engine with Centralized CoRe Technique	65
5.6	Circuit Level Simulation	71
5.7	Conclusion	72
CHAPTER 6: SECURITY-ADAPTIVE VOLTAGE CONVERSION TECHNIQUE		74
6.1	Introduction	74
6.2	Architecture Design	75
6.3	Parameter Design	76
6.4	Security Evaluation Against LPA Attacks	77
6.4.1	Sampling a Single Clock Period as One Sample of Input Power Data	78
6.4.2	Sampling Multiple Clock Periods as One Sample of Input Power Data	81
6.5	Circuit Level Verification	84
6.6	LPA Attacks Simulation	85
6.7	Conclusion	86
CHAPTER 7: ON-CHIP VOLTAGE REGULATION WITH VFS		87
7.1	Introduction	87
7.2	On-Chip Voltage Regulation with VFS Load	90

7.2.1	Low-Dropout (LDO) Regulator with VFS Load	90
7.2.2	Buck Converter with VFS Load	91
7.2.3	Switched-Capacitor (SC) Converter with VFS Load	94
7.3	Security Evaluation of On-Chip Voltage Regulation with VFS Technique Against DPA Attacks	98
7.3.1	Security of On-Chip Voltage Regulation with True Random VFS Technique Against DPA Attacks	99
7.4	Security Evaluation of On-Chip Voltage Regulation with VFS Technique Against LPA Attacks	104
7.5	Overhead Analysis	107
7.6	DPA and LPA Attack Simulations	109
7.7	Conclusion	111
CHAPTER 8: CONCLUSION		112
CHAPTER 9: FUTURE WORK		114
9.1	Utilizing On-Chip Multi-Phase Buck Converter as a Countermeasure Against Electro-Magnetic (EM) Attacks	114
9.2	Utilizing On-Chip Multi-Phase SC Converter as a Physical Unclonable Function (PUF)	116
REFERENCES		118
APPENDICES		126
Appendix A:	Correlation Coefficient of Conventional On-Chip Voltage Regulators	127
Appendix B:	Guidelines on the Selection of a Suitable Active Critical Frequency F_{ac}	129
Appendix C:	Detailed Explanation of Table 7.1 and Table 7.2	132
Appendix D:	Power Consumption Overhead of Different Countermeasures	134
Appendix E:	On-Chip Voltage Regulation with Normally Distributed VFS Technique	136
Appendix F:	Copyright Permissions	140
ABOUT THE AUTHOR		End Page

LIST OF TABLES

Table 7.1	Inserted Noise $N_{j,k}(f_c, V_{dd})$, ($j, k = 1, 2, 3$) into the Power Consumption Profile of a Cryptographic Circuit through Countermeasures that Employ Different Voltage Regulators against DPA Attacks (Detail Explanation can be Found in Appendix C).	98
Table 7.2	Inserted Noise $M_{j,k}(V_{dd})$, ($j, k = 1, 2, 3$) into the Power Consumption Profile of a Cryptographic Circuit through Countermeasures that Employ Different Voltage Regulators against LPA Attacks.	105
Table 7.3	Correlation Coefficient Reduction Ratio (CCRR), Dynamic Power (D-Power) Consumption, and Leakage Power (L-Power) Consumption of an S-Box that Houses On-Chip Voltage Regulators Implemented with True Random and Normally Distributed VFS-based Countermeasures against DPA and LPA Attacks (Supply Voltage Range $V_{DD2} - V_{DD1} = 0.7V$), X_d and X_l Are, Respectively, the Dynamic and Leakage Power Consumption of an S-box without any Countermeasure (Detail Explanation can be Found in Appendix D).	108
Table C.1	(a) Parameter Leakage of Three Different Voltage Regulators with VFS Load, (b) Inserted Noise Induced by Three Different VFS Techniques against DPA Attacks, and (c) Inserted Noise Induced by Three Different VFS Techniques against LPA Attacks.	133

LIST OF FIGURES

Figure 1.1	SPA attacks on the input power profile of RSA cryptographic circuit in [1].	2
Figure 1.2	Flow of implementing DPA attacks from [2].	3
Figure 1.3	Relationship between the hamming-weight of input data and leakage current of a cryptographic circuit in [3].	4
Figure 1.4	All the possible keys versus the correlation coefficient from [3]: (a) LPA attacks and (b) DPA attacks.	5
Figure 1.5	(a) 2:1 single phase SC converter [4] and (b) Power efficiency of a single phase SC converter versus load current and flying capacitance [4].	5
Figure 1.6	(a) Schematic of an 8-phase CoGa regulator [4], (b) Modulation blocks of GoGa regulator [4], and (c) Power efficiency of CoGa regulator versus output current [4].	6
Figure 1.7	Relationship between the input and load current profiles for different on-chip voltage regulators [4]: (a) Load power profile, (b) Input current profile of an LDO voltage regulator, (c) Input current profile of a conventional 8-phase SC voltage converter, (d) Zoomed current profile during transitions for the conventional 8-phase SC voltage converter, (e) Input current profile of an 8-phase CoGa voltage converter, and (f) Zoomed current profile during transitions for the 8-phase CoGa voltage converter.	7
Figure 2.1	Proposed technique disrupts the one-to-one transformation and accomplishes a non-injective relationship between the load current and input current.	10
Figure 2.2	Active and gated converters are juggled with converter-reshuffling.	11
Figure 2.3	Relationship between the input power and AES core power.	14
Figure 2.4	Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes without employing DVFS (DVFS in this work represents random DVFS).	15
Figure 2.5	Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes with DVFS enabled AES core.	16

Figure 3.1	Schematic of the CoRe technique.	20
Figure 3.2	Input power profile of the CoRe technique.	21
Figure 3.3	Schematic of the proposed time-delayed CoRe technique with an $N/2$ -bit PRNG.	22
Figure 3.4	Input power of the time-delayed CoRe technique.	23
Figure 3.5	Schematic of the proposed time-delayed CoRe technique with an N -bit PRNG.	25
Figure 3.6	PTE value versus the phase difference between switching frequency and data sampling frequency (time delay $T_0 = T_s/2$).	27
Figure 3.7	Lowest PTE value versus the time delay.	28
Figure 3.8	Lowest PTE value versus the number of phases ($T_0 = T_s/2$).	29
Figure 4.1	Architecture of the conventional CoRe technique.	32
Figure 4.2	One of the identical 2:1 SC voltage converter stages in CoRe.	33
Figure 4.3	Logic level of the signals that control the switches ($S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i}$) within the CoRe technique.	33
Figure 4.4	Architecture of the proposed charge-withheld CoRe technique.	34
Figure 4.5	Logic level of the signals that control the switches ($S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i}$) within the charge-withheld CoRe technique.	35
Figure 4.6	Input power profile of the CoRe technique.	36
Figure 4.7	PTE value versus the phase difference θ between the switching frequency and data sampling frequency for CoRe and charge-withheld CoRe techniques.	42
Figure 4.8	Average PTE value versus the number of switch cycles sampled by the attacker for CoRe and charge-withheld CoRe techniques.	43
Figure 4.9	Average PTE value versus the number of SC voltage converter phases N for CoRe and charge-withheld CoRe techniques.	44
Figure 5.1	One-to-one relationship between the input current and load current in conventional voltage regulator.	46
Figure 5.2	CoGa regulator in [4] (8-phase) exhibits a constant sequence of active stages if the variation in load current is small.	47

Figure 5.3	Input power data sampling for the attacker within K consecutive switching periods when the CoGa or CoRe techniques are enabled (T_s is the switching period of the CoGa or CoRe regulator).	50
Figure 5.4	Phase difference versus correlation coefficient of CoGa and CoRe techniques.	56
Figure 5.5	Sampling switching periods versus average correlation coefficient.	57
Figure 5.6	Sampling switching periods versus MTD enhancement ratio ($M_1 \approx 5$).	58
Figure 5.7	Number of phases and power undertaken by each phase versus average correlation coefficient.	59
Figure 5.8	1 st encryption round of a typical 128-bit pipelined AES engine.	61
Figure 5.9	A conventional pipelined AES engine with a distributed on-chip CoRe technique.	62
Figure 5.10	A conventional pipelined AES engine with a centralized on-chip CoRe technique.	63
Figure 5.11	Sampling switching periods versus average correlation coefficient and variance of power noise of the distributed and centralized CoRe architectures.	64
Figure 5.12	Sampling switching periods versus MTD enhancement ratios of the distributed and centralized CoRe architectures ($M_1 \approx 5$).	65
Figure 5.13	Full encryption rounds of an 128-bit improved pipelined (IP) AES engine, please note that invert boxes are added before the 1 st round and the mask removal operation is performed after the 11 th round (the architecture of the reconstructed S-box can be founded in [5, 6]).	66
Figure 5.14	Internal logic circuits of the y^{th} invert box.	67
Figure 5.15	Sampling switching periods versus average correlation coefficient and variance of power noise of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator.	68
Figure 5.16	Sampling switching periods versus MTD enhancement ratio of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator ($M_1 \approx 3, 5, \text{ and } 7$).	69
Figure 5.17	(a) Masking operation in conventional masked AES engine and (b) Masking operation in the IP AES engine that we proposed.	70

Figure 5.18	8-phase CoGa regulator and 8-phase CoRe regulator are simulated: a) Distribution of load current, b) transient output voltage profile, and c) input current profile of CoGa regulator and CoRe regulator, sequence of active stages in CoRe regulator is variable while sequence of active stages in CoGa regulator is invariable if a constant load current is enabled, as shown in d), e), f), and g).	72
Figure 5.19	(a) Load current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator, (b) Input current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator (The total number of phases of the centralized CoRe regulator is 64).	73
Figure 6.1	Architecture of the proposed security-adaptive (SA) voltage converter (N is the total number of phases (N is an even), switch $M_{i_1} = 1$, ($i_1 = 1, 2$) represents that it is in on-state and <i>vice versa</i>).	76
Figure 6.2	Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a single clock period as one sample of input power data (T_s is the switching period of the SA voltage converter, Y_i is the starting time point of the 1^{st} switching period for sampling the i^{th} input power data, and θ is the phase difference between the switching period and input power data sampling).	78
Figure 6.3	(a) Average correlation coefficient versus clock period $1/f_c$ and (b) MTD enhancement ratio $R_1(FT_s)$ versus clock period $1/f_c$.	80
Figure 6.4	Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a variable number of clock periods as one sample of input power data (X_i is the starting time point of the 1^{st} switching period for sampling the i^{th} input power data).	81
Figure 6.5	(a) Average correlation coefficient versus sampling time period KF_0T_s and (b) MTD enhancement ratio $R_2(KF_0T_s)$ versus sampling time period KF_0T_s ($F_0=10$ and $N=32$).	82
Figure 6.6	(a) Load current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter, (b) Input current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter.	84

Figure 6.7	LPA attacks simulation: (a) All of the possible keys versus absolute value of the correlation coefficient for an S-box without countermeasure after analyzing 500 leakage power traces, (b) All of the possible keys versus absolute value of correlation coefficient for an S-box that employs a CoRe voltage converter after analyzing 2 million leakage power traces, and (c) All of the possible keys versus absolute value of the correlation coefficient for an S-box that employs an SA voltage converter after analyzing 2 million leakage power traces.	85
Figure 7.1	Relationship between the clock pulse and power consumption of a cryptographic circuit [7].	88
Figure 7.2	Schematic of a conventional LDO voltage regulator.	90
Figure 7.3	(a) Transient load current profile of an LDO voltage regulator with VFS load and (b) Transient input power profile of an LDO voltage regulator with VFS load.	92
Figure 7.4	Schematic of a conventional buck converter.	93
Figure 7.5	(a) Transient supply voltage (output voltage) V_{dd} of a buck converter with VFS load and (b) Transient input power profile of a buck converter with VFS load.	94
Figure 7.6	Relationship between the supply voltage V_{dd} and the slope of the input power S_2 in the charging state.	95
Figure 7.7	Basic architecture of a switched-capacitor (SC) voltage converter.	96
Figure 7.8	Transient input power of an SC converter with variable $\sum_{i=1}^M \alpha_i$.	97
Figure 7.9	Relationship between the input data and monitored power consumption P_{dyn} of a cryptographic circuit that employs an on-chip voltage regulation based VFS technique (<i>Conventional cryptographic circuit</i> represents a cryptographic circuit without any countermeasure).	102
Figure 7.10	Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an-S-box that employs different VFS-based countermeasures (Since a high f_v does not enhance the variance of noise induced by VFS technique, as explained in [7, 8], a moderate voltage scaling frequency of $f_v = 10MHz$ [9] is used for the security analysis to not increase the system design complexity).	103
Figure 7.11	Variance of the supply voltage V_{dd} versus the correlation coefficient reduction ratio for an S-box that employs RDVFS technique with an SC converter with various possible (f_c, V_{dd}) pairs.	104

Figure 7.12	Supply voltage V_{dd} versus leakage current of an S-box implemented in 130nm CMOS technology under two different input data.	106
Figure 7.13	Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an S-box that employs different countermeasures ($f_v = 10MHz$ and $N = 50$).	107
Figure 7.14	Absolute value of the correlation coefficient versus all of the possible keys after inputting 1,000 plaintexts with the hamming-weight model: (a) An S-box without countermeasure under DPA attacks and (b) An S-box without countermeasure under LPA attacks.	109
Figure 7.15	Absolute value of correlation coefficient versus all the possible keys after inputting 1 million plaintexts with hamming-weight model ($V_{DD2} - V_{DD1} = 0.7V$): (a) An S-box that employs RDVFS technique with an SC converter under DPA attacks and (b) An S-box that employs RDVFS technique with an SC converter under LPA attacks.	110
Figure 9.1	Attacker can bypass the on-chip voltage regulator and implement EM attacks directly.	115
Figure 9.2	Distribute inductors of multi-phase buck converter uniformly among the cryptographic circuit in the layout.	115
Figure 9.3	Architecture of conventional RO PUF in [10].	116
Figure D.1	Supply voltage V_{dd} versus clock frequency f_c under different VFS techniques: (a) RDVS technique, (b) RDVFS technique, and (c) AVFS technique.	135
Figure E.1	Variance of supply voltage V_{dd} versus correlation coefficient reduction ratio of an S-box that employs different techniques (VFS techniques conform to normal distribution, $f_v = 10MHz$, and $N = 50$) as compared to uniformly distributed RDVFS with an SC voltage converter.	137
Figure E.2	Variance of the supply voltage V_{dd} versus the supply voltage range ($V_{DD2} - V_{DD1}$) for uniformly and normally distributed V_{dd} .	138

ABSTRACT

Non-invasive side-channel attacks (SCA) are powerful attacks which can be used to obtain the secret key in a cryptographic circuit in feasible time without the need for expensive measurement equipment. Power analysis attacks (PAA) are a type of SCA that exploit the correlation between the leaked power consumption information and processed/stored data. Differential power analysis (DPA) and leakage power analysis (LPA) attacks are two types of PAA that exploit different characteristics of the side-channel leakage profile. DPA attacks exploit the correlation between the input data and dynamic power consumption of cryptographic circuits. Alternatively, LPA attacks utilize the correlation between the input data and leakage power dissipation of cryptographic circuits.

There is a growing trend to integrate voltage regulators fully on-chip in modern integrated circuits (ICs) to reduce the power noise, improve transient response time, and increase power efficiency. Therefore, when on-chip voltage regulation is utilized as a countermeasure against power analysis attacks, the overhead is low. However, a one-to-one relationship exists between the input power and load power when a conventional on-chip voltage regulator is utilized. In order to break the one-to-one relationship between the input power and load power, two methodologies can be considered: (a) selecting multi-phase on-chip voltage regulator and using pseudo-random number generator (PRNG) to scramble the activation or deactivation pattern of the multi-phase voltage regulator in the input power profile, (b) enabling random voltage/scaling on conventional on-chip voltage regulators to insert uncertainties to the load power profile.

In this dissertation, on-chip voltage regulators are utilized as lightweight countermeasures against power analysis attacks. Converter-reshuffling (CoRe) technique is proposed as a countermeasure against DPA attacks by using a PRNG to scramble the input power profile. The time-delayed CoRe technique is designed to eliminate machine learning-based DPA attacks through

inserting a certain time delay. The charge-withheld CoRe technique is proposed to enhance the entropy of the input power profile against DPA attacks with two PRNGs. The security-adaptive (SA) voltage converter is designed to sense LPA attacks and activate countermeasure with low overhead. Additionally, three conventional on-chip voltage regulators: low-dropout (LDO) regulator, buck converter, and switched-capacitor converter are combined with three different kinds of voltage/frequency scaling techniques: random dynamic voltage and frequency scaling (RDVFS), random dynamic voltage scaling (RDVS), and aggressive voltage and frequency scaling (AVFS), respectively, against both DPA and LPA attacks.

CHAPTER 1: INTRODUCTION

1.1 Side-Channel Attacks

Hardware security has become an important design metric during the past decade with the increase in the number of attacks at different hardware abstraction levels¹. Along with the other important metrics such as higher power efficiency, better performance, and lower noise, hardware security is also added as an important design objective in modern computing devices. It has been demonstrated that software level countermeasures may not be sufficient to protect the encrypted data from an attacker who has physical access to the device under attack (DuA). Even flawless implementations of state-of-the-art encryption algorithms are typically vulnerable against hardware attacks. The primary reason is that the modern integrated circuits (ICs) heavily depend on complementary metal oxide semiconductor (CMOS) transistors which have switching characteristics that are easily analyzed to determine the underlying circuit functionality. The side channel leakage originating from the switching activity of transistors can be monitored with simple measurement equipment by an attacker. This side channel leakage can manifest itself in the form of power consumption profile, timing profile, electromagnetic emanations (EME), acoustic waveforms, and heat. An efficient implementation of side-channel attacks can retrieve the secret key from an advanced encryption standard (AES) algorithm in a couple of minutes whereas it can take up to 149 trillion years to crack a 128-bit AES key with a supercomputer [12].

Various techniques have been proposed as a countermeasure against different types of side-channel attacks both at the circuit and architectural levels [13]. To reduce the dependency of the side-channel leakage on the actual power consumption profile, leakage reduction techniques have

¹The content of this Chapter partially has been published in [11], the copyright permission can be found in Appendix F.

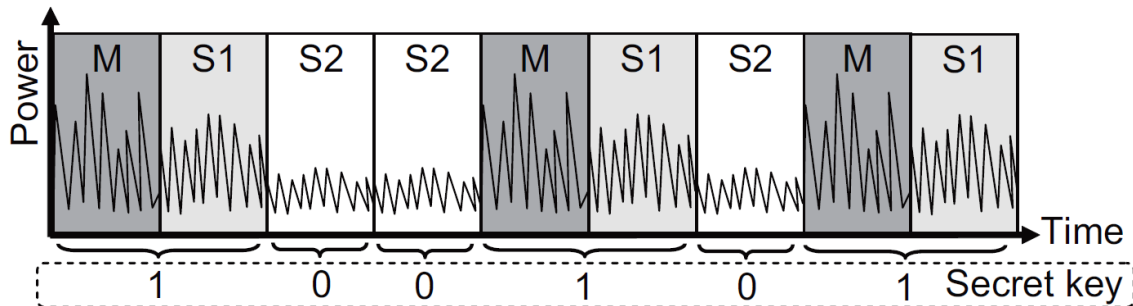


Figure 1.1 SPA attacks on the input power profile of RSA cryptographic circuit in [1].

been proposed. Dummy multiplication operations have been performed for timing attacks against RSA to minimize the leakage in the timing channel in [14], significantly increasing the power consumption. The actual power consumption profile can be smoothed by using different CMOS logic families to provide a more balanced pull-up and pull-down power consumption such as current-mode logic [15] or asynchronous logic [16]. Random or pseudo-random noise has been inserted in the side-channel leakage to make the analysis more difficult for an attacker in [17]. Although the number of required side-channel leakage measurements increases quadratically with decreasing signal-to-noise ratio (SNR) of the side-channel information [18, 19], advanced techniques can be used to average out the injected noise [20]. Frequently updating the secret key is also proposed in [20] to add another level of difficulty for the attacker. One of the primary disadvantages of the existing techniques is the power and area overhead. Although some of these techniques are successful against certain side-channel attacks, power and area overheads typically make them quite costly [21].

1.2 Power Analysis Attacks

Power analysis attacks (PAA) are non-invasive side-channel attacks to acquire critical information from cryptographic circuits by analyzing the power consumption profile [22].

1.2.1 Simple Power Analysis (SPA) Attacks

Simple power analysis (SPA) attacks are a kind of basic PAA, which are utilized by the attacker to reveal the critical information through monitoring a very few number of power traces [1].

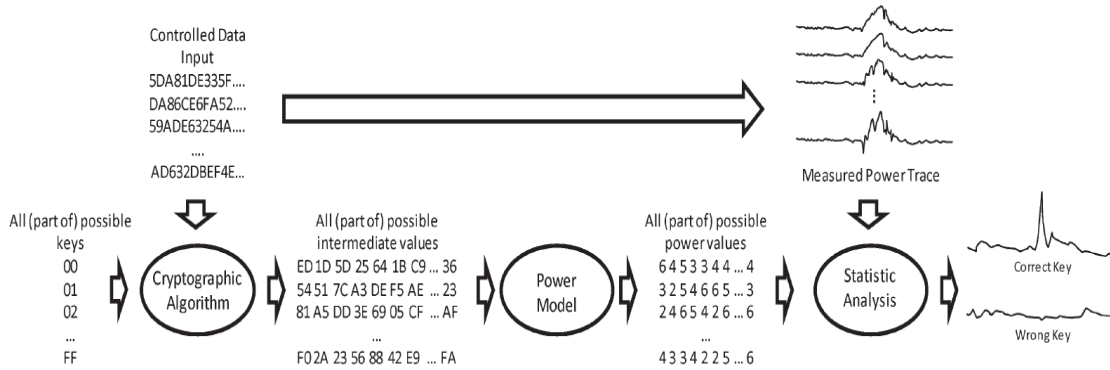


Figure 1.2 Flow of implementing DPA attacks from [2].

As shown in Fig. 1.1², different math operations that occur in the cryptographic cause the circuit to have varying power dissipation profiles. The attacker may obtain the critical information by analyzing the variations of power traces. Although SPA attacks are simple and convenient, implementing SPA attacks on a modern cryptographic circuit may not be sufficient to leak the critical information due to the protection of complex encryption algorithm.

1.2.2 Differential Power Analysis (DPA) Attacks

A differential power analysis (DPA) attack is an advanced PAA that statistically analyzes a large number of dynamic power traces to determine whether a secret key guess is correct or not [20]. DPA attacks are widely utilized by attackers due to the high efficiency and low cost.

The detailed flow of implementing DPA attacks is shown in Fig. 1.2³. First, the attacker inputs a series of plaintexts to the cryptographic circuit and hypothesizes all of the possible keys of the cryptographic circuit. The intermediate data values can be obtained through combining the plaintexts and hypothesized keys with the cryptographic algorithm. When the intermediate data are acquired, the attacker can predict the dynamic power consumption of the cryptographic circuit by combining the intermediate data with a suitable power model. The next step for the attacker is measuring the actual dynamic power consumption of the cryptographic circuit under different plaintexts. When the attacker performs a statistical analysis between the predicted dynamic power

²Copyright permission can be found in Appendix F.

³Copyright permission can be found in Appendix F.

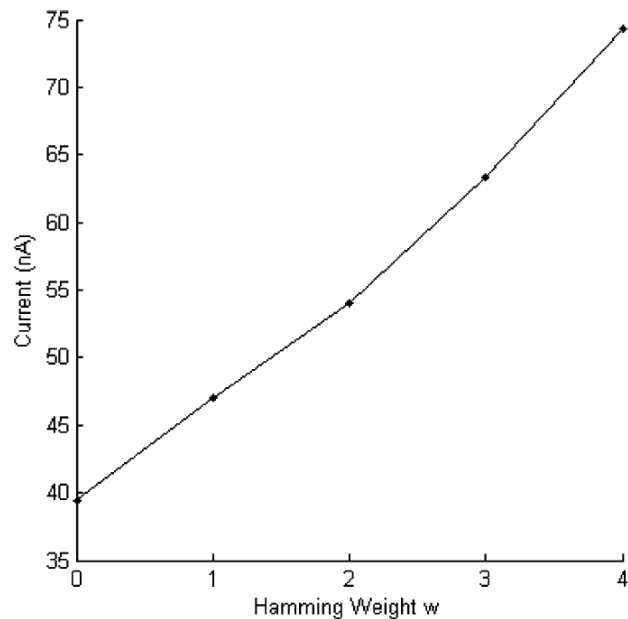


Figure 1.3 Relationship between the hamming-weight of input data and leakage current of a cryptographic circuit in [3].

dissipation and actual dynamic power dissipation, the hypothesized key that makes the predicted power exhibit the highest correlation coefficient with the measured power is likely to be the correct key.

1.2.3 Leakage Power Analysis (LPA) Attacks

A leakage power analysis (LPA) attack is a type of power analysis attack which is utilized by an attacker to leak the secret key of a cryptographic circuit by exploiting the correlation between the input data and leakage power dissipation [3, 19]. Since the leakage current signature of NMOS and PMOS is quite different, a cryptographic circuit designed with CMOS technology would leak a great amount of critical information to the attacker under LPA attacks [3].

As shown in Fig. 1.3⁴, the hamming-weight of input data has a high linear correlation with the leakage current of the cryptographic circuit. Additionally, as compared to DPA attacks, when LPA attacks are implemented on a cryptographic circuit, the correct key exhibits a higher

⁴Copyright permission can be found in Appendix F.

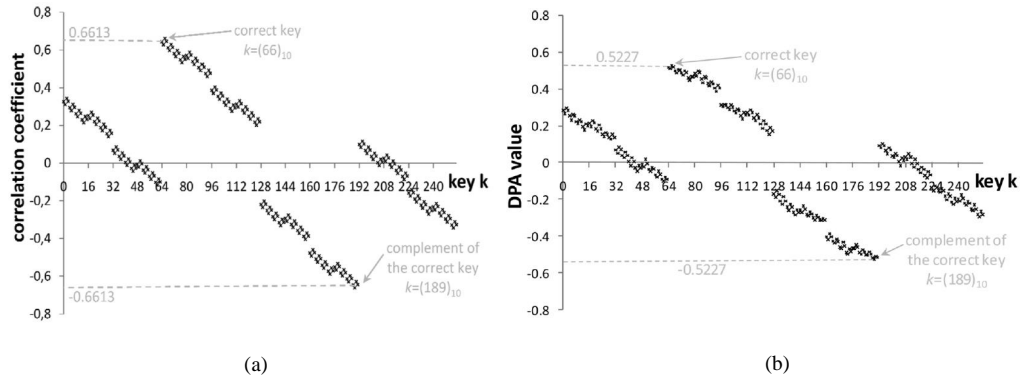


Figure 1.4 All the possible keys versus the correlation coefficient from [3]: (a) LPA attacks and (b) DPA attacks.

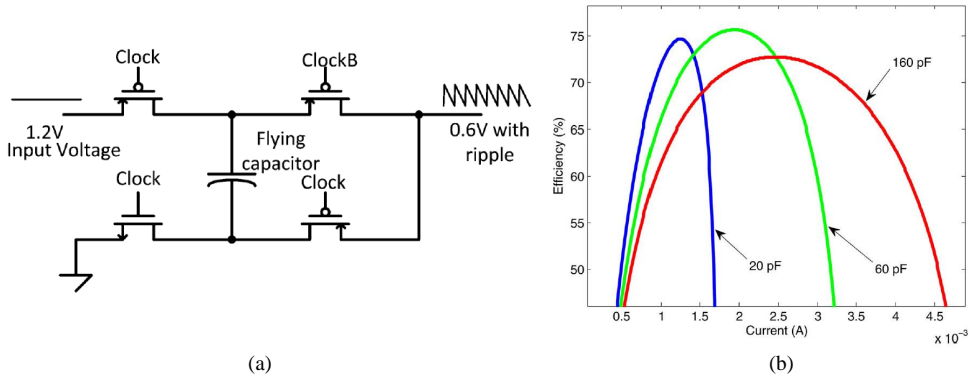


Figure 1.5 (a) 2:1 single phase SC converter [4] and (b) Power efficiency of a single phase SC converter versus load current and flying capacitance [4].

correlation coefficient, as shown in Fig. 1.4⁵. The higher correlation coefficient indicates a larger amount of information leakage. As a result, LPA attacks may be a more serious threat under certain conditions.

1.3 On-Chip Voltage Regulation Against Power Analysis Attacks

1.3.1 Converter-Gating (CoGa) Voltage Converter Against Power Analysis Attacks

On-chip power delivery is an efficient way to reduce the power noise [23–37] and improve transient response time [37–39]. Multi-phase on-chip voltage converter is a kind of fully integrated on-chip voltage converters, which can achieve high power efficiency by optimizing the number of

⁵Copyright permission can be found in Appendix F.

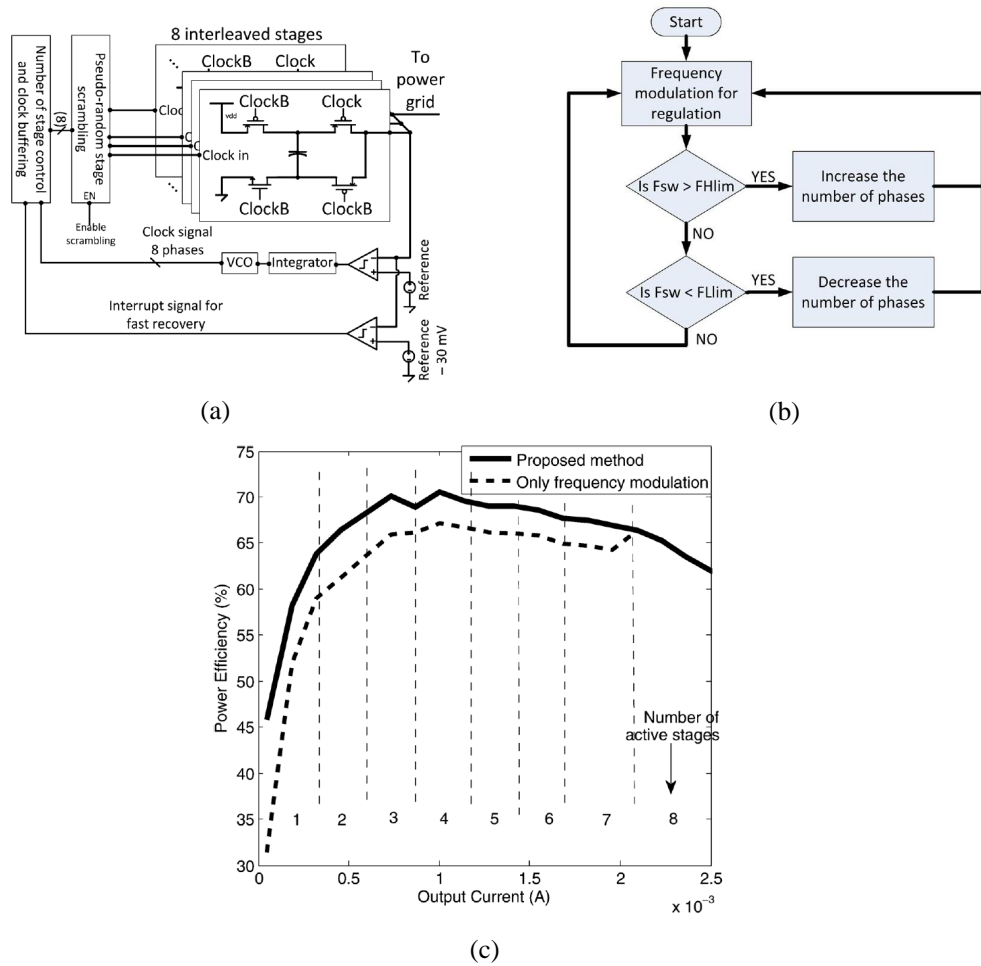


Figure 1.6 (a) Schematic of an 8-phase CoGa regulator [4], (b) Modulation blocks of GoGa regulator [4], and (c) Power efficiency of CoGa regulator versus output current [4].

active phases when the load condition alters [4, 40–42]. For instance, the power efficiency of a 2:1 single phase switched-capacitor (SC) converter (shown in Fig. 1.5(a)⁶) is affected by the load current and flying capacitance, as shown in Fig. 1.5(b). A smaller flying capacitor can achieve the peak power efficiency under light load condition. Therefore, in multi-phase SC converter, when the load current is large, a large number of phases are activated to force each interleaved phase work near the peak power efficiency. However, when the load current is low, a small number of phases are active to maintain the peak power efficiency.

⁶Copyright permission of Fig. 1.5(a)-(b) can be found in Appendix F.

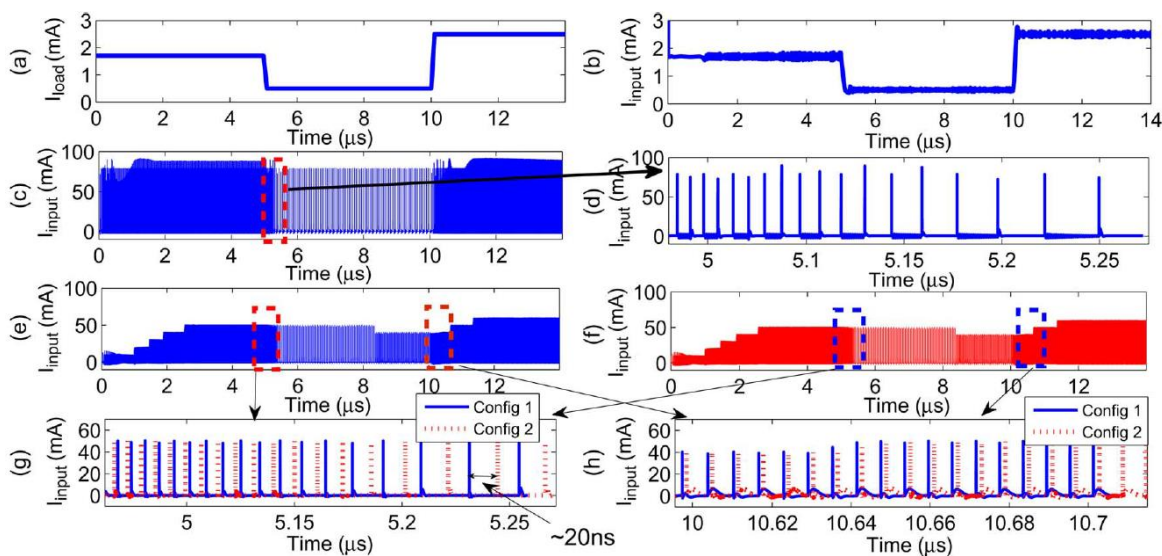


Figure 1.7 Relationship between the input and load current profiles for different on-chip voltage regulators [4]: (a) Load power profile, (b) Input current profile of an LDO voltage regulator, (c) Input current profile of a conventional 8-phase SC voltage converter, (d) Zoomed current profile during transitions for the conventional 8-phase SC voltage converter, (e) Input current profile of an 8-phase CoGa voltage converter, and (f) Zoomed current profile during transitions for the 8-phase CoGa voltage converter.

The converter-gating (CoGa) technique [4] utilizes a multi-phase SC converter. The architecture of an 8-phase CoGa regulator is shown in Fig. 1.6(a)⁷ and the related dual loop control is shown in Fig. 1.6(b). Since the switching frequency of SC converter is proportional to the load current and flying capacitance [43]. When the switching frequency exceeds the maximum frequency, CoGa regulator would increase the number of active phases (increase total flying capacitance). If the switching frequency is lower than the minimum frequency, CoGa regulator would decrease the number of active phases (decrease total flying capacitance). As shown in Fig. 1.6(c), with the phase number modulation, the power efficiency of CoGa regulator can be enhanced around 5% as compared to a conventional multi-phase SC converter which only utilizes frequency modulation (all the phases are active all the time). CoGa technique is therefore a power efficient on-chip voltage regulation technique [4].

⁷Copyright permission of Fig. 1.6(a)-(c) can be found in Appendix F.

As shown in Fig. 1.7(a)⁸ and Fig. 1.7(b), low-dropout (LDO) regulator has a poor security against power analysis attacks since there is an approximated linear relationship between the input current and load current. By contrast, as shown in Fig. 1.7(c) and Fig. 1.7(d), conventional multi-phase SC converter can obscure the correlation between the input and load current profiles by charging and discharging the flying capacitors with a certain switching frequency. However, CoGa converter can further scramble the correlation between the input and load current profiles with a pseudo-random number generator (PRNG) that alters the activation or deactivation pattern of phases, as shown in Fig. 1.7(e), Fig. 1.7(f), Fig. 1.7(g) and Fig. 1.7(h).

1.3.2 Our Contribution

Although CoGa technique was proposed in [4] as a countermeasure against power analysis attacks, it is demonstrated in our work that CoGa technique is not sufficiently secure against power analysis attacks. Therefore, we proposed another five novel efficient on-chip voltage regulation techniques against power analysis attacks. The content of our contribution is summarized as follows⁹

- *Chapter 2* introduces converter-reshuffling (CoRe) voltage conversion against DPA attacks.
- *Chapter 3* proposes time-delayed converter-reshuffling (CoRe) voltage conversion against machine learning-based DPA attacks.
- *Chapter 4* introduces a high entropy charge-withheld converter-reshuffling (CoRe) voltage conversion against DPA attacks.
- *Chapter 5* co-designs on-chip voltage regulation with advanced encryption standard (AES) engine against DPA attacks.
- *Chapter 6* introduces security-adaptive (SA) voltage conversion against LPA attacks.
- *Chapter 7* explores conventional on-chip voltage conversion with voltage/frequency scaling against both DPA and LPA attacks.

⁸Copyright permission of Fig. 1.7(a)-(h) can be found in Appendix F.

⁹The parameters defined in each chapter are independent, different chapters may share the same parameter sign with different meanings.

CHAPTER 2: CONVERTER-RESHUFFLING TECHNIQUE

2.1 Motivation

On-chip voltage regulation is an area with vast amount of research to enable small, fast, efficient, robust, and high power-density voltage regulators on-die close to the load circuits¹ [44, 45]. On-chip voltage regulators provide faster voltage scaling, reduce the number of dedicated I/O pins, and facilitate fine granularity power management techniques [44–46]. Three types of regulators are widely used in modern circuits: buck converters, switched-capacitor (SC) converters, and low-dropout (LDO) regulators [47–49]. Buck converters can provide superior power efficiency over 95%; however, the on-chip area requirement is quite large due to the large passive LC filter [49, 50]. SC voltage converters utilize non-overlapping switches that control the charge-sharing between capacitors to generate a DC output voltage. Linear regulators provide superior line and load regulation but have inferior power efficiency limited to V_{out}/V_{in} [51]. With the utilization of deep-trench capacitors, SC voltage converters can achieve high power densities such as 4.6 A/mm² [52]. SC voltage converters charge and discharge periodically, producing periodic spikes in the input current waveform and therefore reducing the correlation between the input and output current profiles as compared to LDO regulators.

Certain voltage regulator types allow a high correlation between the actual load current and the input current that may be monitored by an attacker to learn “*what is going on inside the chip.*” An injective (one-to-one) relationship should exist to determine $I_{load,n}$ by measuring $I_{in,n}$. When the IC does not employ on-chip voltage regulation, an injective relationship exists between the load current consumed by the cryptographic circuit (CC) and the input current to the IC (*i.e.*,

¹The content of this Chapter has been published in [11], the copyright permission can be found in Appendix F.

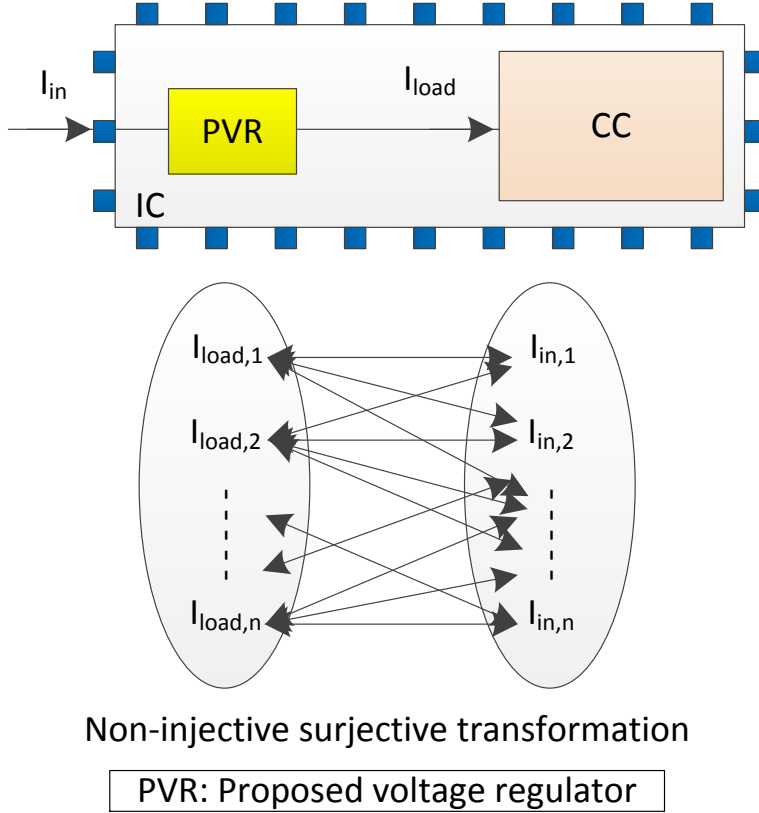


Figure 2.1 Proposed technique disrupts the one-to-one transformation and accomplishes a non-injective relationship between the load current and input current.

$I_{load,n} = I_{in,n}$), as shown in Fig. 2.1. If the on-chip power delivery network can provide a non-injective relationship between the load and input current profiles, as illustrated in Fig. 2.1, (*i.e.*, a particular load current leads to *more than one* input current profile), the outside attacker can no longer obtain the internal information by measuring the input current. SC voltage converters charge and discharge periodically, produce spikes in the input current waveform, and therefore reduce the correlation between the input and output current profiles.

2.2 Treat Model

The attack is assumed to be non-invasive and the attacker is assumed to have access to the circuit where s/he can monitor the side-channel leakage information. For example, the power consumption profile can be monitored by measuring the I/O pins dedicated to power/ground,

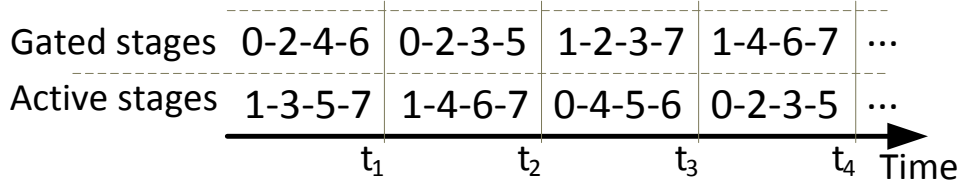


Figure 2.2 Active and gated converters are juggled with converter-reshuffling.

shown as I_{in} in Fig. 2.1. Alternatively, the attacker can use near-field antennas to monitor the EM emanations. Additionally, the DuA is assumed to have on-chip voltage regulators.

2.3 Review of Converter-Gating (CoGa)

Converter-gating (CoGa) is the adaptive activation and deactivation of certain stages of a multiphase on-chip SC voltage converter based on the workload information [4]. When the current demand increases (decreases), an additional passive (active) stage is activated (gated) to provide a higher (lower) load current without sacrificing power conversion efficiency. The additional stage that is being activated or gated is determined based on a pseudo-random number generator (PRNG) to scramble the input current consumption of the SC voltage converter (*i.e.*, I_{in} as shown in Fig. 2.1). Since each interleaved stage within an SC voltage converter is driven with a different phase of the input clock signal, each interleaved stage charges and discharges with a certain time shift. The amount of time shift depends on the frequency of the clock signal. For example, a timing shift of $0.5 \mu s$ can be achieved by activating the 4^{th} stage instead of the 0^{th} stage when an eight stage SC converter operates at 1 MHz.

Although CoGa makes the attackers' job more difficult by scrambling the power consumption profile and inserting additional spikes in the input current profile, the DuA would still be vulnerable under advanced attacks as the activation/deactivation occurs when there is a change in the workload demand. Particularly, an attacker can effectively bypass the CoGa technique if an attack is performed such that the changes in the load current demand are not large enough to trigger CoGa to activate/deactivate interleaved stages. Furthermore, the input current profile that is monitored by an attacker would still be correlated with the actual current profile even if CoGa is triggered since the activation/deactivation occurs when there is a change in the workload demand.

2.4 Converter-Reshuffling (CoRe)

A new control technique, converter-reshuffling (CoRe), is proposed to scramble the input current profile when the change in the load current is not sufficiently large to turn on or off a converter stage. In CoRe technique, a new set of voltage converter stages is periodically determined with a PRNG. Some of the active converter stages are then juggled accordingly with the inactive converter stages. In other words, some of the active stages are gated concurrently while the same number of inactive stages are turned on under constant load current demand.

For example, the number of required active converter stages to efficiently provide a load current of 1 mA is four. Let's assume that these active stages are the 1st, 3rd, 5th, and 7th converter stages. With CoRe, some of these active stages are gated and the same number of inactive stages are simultaneously turned on, as shown in Fig. 2.2. After a certain time period, the converters are shuffled again while keeping the same number of converters active. Please note that CoRe technique can work with or without converter-gating regardless of whether or not the load current demand is sufficiently large to trigger converter-gating and lead to an additional stage to turn on.

The primary advantages of CoRe operation as a side-channel attack countermeasure are twofold. First, the input current profile is disrupted while turning on and off different converter stages. Secondly, the input current profile periodically exhibits a different signature since the phases of the active converter stages vary, generating a quite different input current signature. For example, an eight phase SC voltage converter with three active stages has $\binom{8}{3}=56$ activity patterns that would lead to 56 different input current signatures while delivering the same load current.

2.5 Evaluation

Entropy is a widely used property to quantify the security-performance of countermeasures against side-channel attacks [53]. In this Chapter, the power trace entropy (PTE) is utilized as a security-performance metric while ensuring a constant time trace entropy (TTE) to compare the security levels of different voltage regulation schemes [21]. PTE and TTE are, respectively, the uncertainty of the amplitude and timing of the spikes in the power consumption profile. It has

been shown in [21] that TTE is zero without dynamic voltage and frequency scaling (DVFS). When DVFS is activated, a constant non-zero TTE of 6.02 [21] is used in the evaluation. Intuitively, TTE increases when the operating frequency changes over time as in the case of DVFS. We assume that the power consumption of an advanced encryption standard (AES) core is $P(t)$ at time t , the number of phases N changes between 30 and 100, the switching frequency and period of each phase are, respectively, f_s and T_s , the frequency of the input data for AES core is f_0 , the phase difference between actual power consumption and sampling of the attacker is $2\pi\theta$. The relationship between the input power and AES core power while employing either CoGa or CoRe is illustrated in time domain in Fig. 2.3. Regions 3 and 4 are, respectively, the time periods in which the attacker observes part of the spikes that occur in Regions 1 and 2. The two consecutive power consumption profiles, as shown in Fig. 2.3, may contain different number of spikes k_1 and k_2 if the workload current demand changes. Assuming $k_2 > k_1$, the change in the number of spikes $f(\theta, P(t))(k_2 - k_1)$, as illustrated in Fig. 2.3 in Region 4, can be observed by an attacker and may provide critical information about the workload. $f(\theta, P(t))$ is the ratio of number of additional spikes in Region 4 over the total number of additional spikes in Region 2.

The input power of CoGa $P_{in}^{CoGa}(t)$ observed by an attacker within a switching period T_s can be expressed as

$$P_{in}^{CoGa}(t) = k_1 P_0 + f(\theta, P(t))(k_2 - k_1) P_0, \quad (2.1)$$

where

$$k_1 = \left[\frac{\int_{(m-2)T_s}^{(m-1)T_s} P(t) dt}{\eta_0 P_0 T_s} \right], \quad (2.2)$$

$$k_2 = \left[\frac{\int_{(m-1)T_s}^{mT_s} P(t) dt}{\eta_0 P_0 T_s} \right], \quad (2.3)$$

η_0 is the power efficiency, P_0 is the output power of each individual converter phase, and m is the number of switch cycles that is a function of time t .

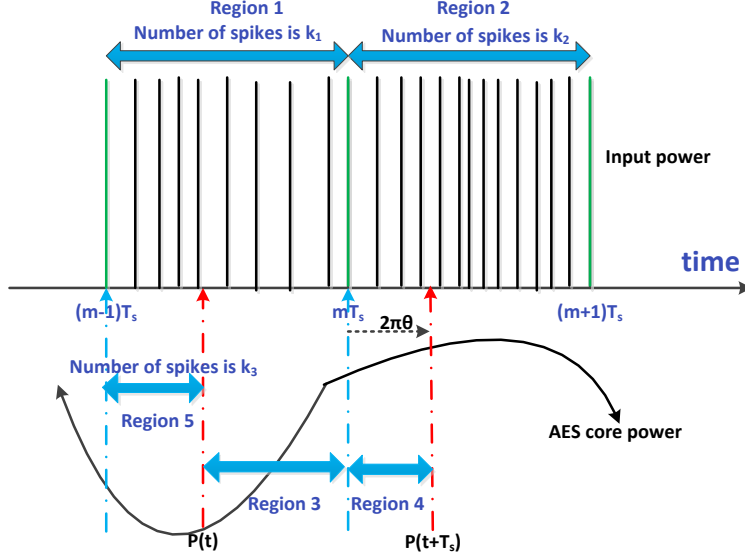


Figure 2.3 Relationship between the input power and AES core power.

The input power of CoRe $P_{in}^{CoRe}(t)$ observed by an attacker within a switching period T_s can be expressed as

$$P_{in}^{CoRe}(t) = \alpha(\theta, P(t))P_0 + \beta(\theta, P(t))P_0, \quad (2.4)$$

where $\alpha(\theta, P(t))$ and $\beta(\theta, P(t))$ are the number of spikes that is monitored by an attacker, respectively, in Regions 3 and 4.

In differential power analysis (DPA) attacks, the attacker monitors the dynamic power consumption [21]. To obtain a useful level of PTE from CoGa and CoRe, the probability of detecting the changes in the power profile for each possible input power value needs to be calculated. This probability $\gamma_i(\theta, P(t))$ for CoGa when $\theta \neq 0$ is

$$\gamma_i(\theta, P(t)) = \frac{\binom{[\theta N] - k_3}{i} \binom{[(1-\theta)N] - k_1 + k_3}{k_2 - k_1 - i}}{\binom{N - k_1}{k_2 - k_1}}, \quad (2.5)$$

$$i \in [A, B] = [\max\{0, k_2 - k_3 - [(1-\theta)N]\},$$

$$\min\{[\theta N] - k_3, k_2 - k_1\}], \quad (2.6)$$

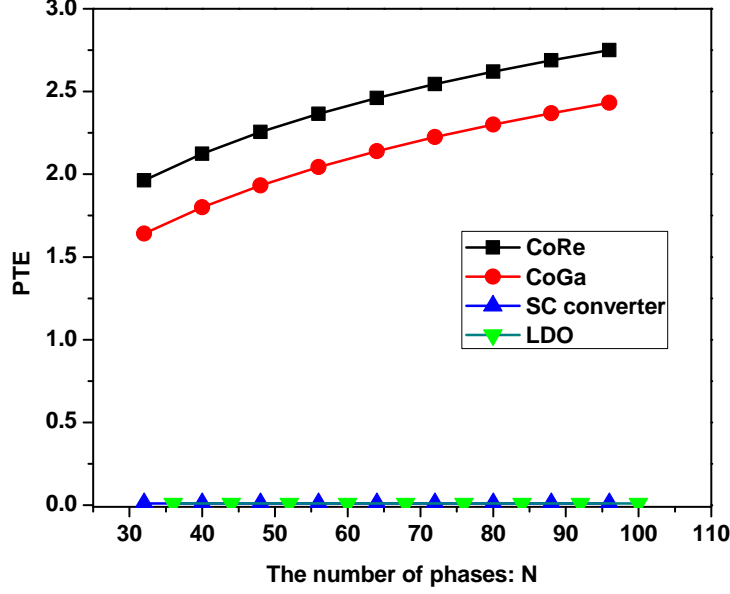


Figure 2.4 Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes without employing DVFS (DVFS in this work represents random DVFS).

where k_3 is the number of spikes in Region 5, as illustrated in Fig. 2.3. The PTE value for CoGa $PTE_{DPA}^{CoGa}(t)$ is therefore

$$PTE_{DPA}^{CoGa}(t) = - \sum_{i=A}^B \gamma_i(\theta, P(t)) \log_2(\gamma_i(\theta, P(t))). \quad (2.7)$$

Note that if $\theta = 0$, the probability $\gamma_i(0, P(t)) = 1$ and the PTE for CoGa becomes 0. However, in practice, the switching frequency f_s is not constant, but has a narrow frequency range. It is quite difficult for an attacker to keep the value of θ as 0 all the time. Therefore, in the rest of this Chapter, we assume $\theta \neq 0$.

For CoRe, the probability function $\lambda_j(\theta, P(t))$ for achieving different input powers is

$$\lambda_j(\theta, P(t)) = \frac{\binom{N}{j} \binom{N}{k_1+k_2-j}}{\binom{N}{k_1} \binom{N}{k_2}}, \quad (2.8)$$

$$j \in [C, D] = [\max\{0, k_1 + k_2 - N\}, \min\{N, k_1 + k_2\}], \quad (2.9)$$

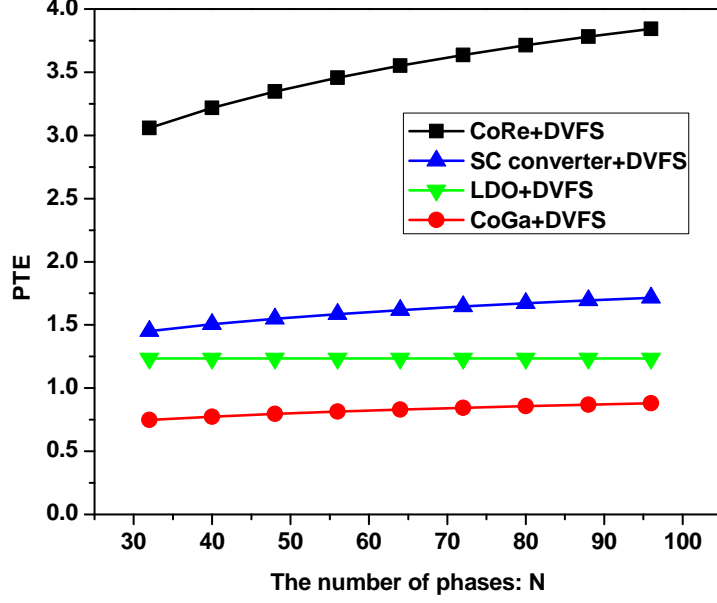


Figure 2.5 Relationship between the number of phases and the PTEs for four different kinds of voltage regulation schemes with DVFS enabled AES core.

when $\theta \neq 0$. In (2.8), $j = i_1 + i_2$ where i_1 and i_2 are the number of spikes, respectively, in Regions 3 and 4. The constraints for (i_1, i_2) are $(i_1 \leq k_1, i_2 \leq k_2)$. Accordingly, the PTE of CoRe $PTE_{DPA}^{CoRe}(t)$ becomes

$$PTE_{DPA}^{CoRe}(t) = - \sum_{j=C}^D \lambda_j(\theta, P(t)) \log_2^{(\lambda_j(\theta, P(t)))}. \quad (2.10)$$

The relationship between the number of phases and the PTE value for four different kinds of voltage regulation schemes is illustrated in Fig. 2.4 when load power demand varies from $(1/2)P_{max}$ to $(7/8)P_{max}$ where P_{max} is the maximum dynamic power consumption for AES core. As shown in Fig. 2.4, the PTE of CoRe is about 13% greater as compared to the PTE of CoGa and therefore CoRe provides better security than CoGa.

Dynamic voltage and frequency scaling (DVFS) is a popular technique which not only reduces power dissipation but also can improve the security level of AES core by increasing time trace entropy (TTE) [21]. Accordingly, the security implications of the proposed on-chip voltage regulation scheme is compared to the three other existing power delivery schemes in the presence of DVFS. When the AES core employs DVFS, we assume the random time delay between the input

data and power consumption variation caused by DVFS is T_0 . In other words, the input power would vary within 0 to T_0 after the input data completed. In the case of CoGa, the variations in the power consumption appear within the first switching period only after the input data has been processed. This can cause CoGa a non-zero PTE. The PTE for CoGa $PTE_{DVFS}^{CoGa}(t)$ with DVFS therefore becomes

$$PTE_{DVFS}^{CoGa}(t) = -\left(1 - \frac{T_s}{T_0}\right) \log_2 \left(1 - \frac{T_s}{T_0}\right) - \sum_{[\theta N]=1}^{N-1} \sum_{i=A}^B \frac{T_s}{NT_0} \gamma_i(\theta, P(t)) \log_2 \left(\sum_{[\theta N]=1}^{N-1} \frac{T_s}{NT_0} \gamma_i(\theta, P(t))\right). \quad (2.11)$$

The PTE for CoRe is, however, quite different in the presence of DVFS. The input power of CoRe keeps reshuffling regardless of the workload demand and therefore always has a non-zero PTE. As a result, the PTE of CoRe $PTE_{DVFS}^{CoRe}(t)$ is much greater than the PTE of CoGa and can be shown as

$$\begin{aligned} PTE_{DVFS}^{CoRe}(t) &= - \sum_{[\theta N]=1}^{N-1} \sum_{j=C}^D \frac{1}{N} \left(1 - \frac{T_s}{T_0}\right) \lambda_j^1(\theta, P(t)) \\ &\times \log_2 \left(\sum_{[\theta N]=1}^{N-1} \frac{1}{N} \left(1 - \frac{T_s}{T_0}\right) \lambda_j^1(\theta, P(t))\right) - \sum_{[\theta N]=1}^{N-1} \sum_{j=C}^D \lambda_j(\theta, P(t)) \\ &\times \frac{T_s}{NT_0} \log_2 \left(\sum_{[\theta N]=1}^{N-1} \frac{T_s}{NT_0} \lambda_j(\theta, P(t))\right). \end{aligned} \quad (2.12)$$

The probability function $\lambda_j^1(\theta, P(t))$ is the same as $\lambda_j(\theta, P(t))$ if $k_2 = k_1$. Similarly, the PTEs of a conventional SC voltage converter PTE_{DVFS}^{SC} and an LDO regulator PTE_{DVFS}^{LDO} with DVFS are

$$\begin{aligned} PTE_{DVFS}^{SC} &= -\left(1 - \frac{T_s}{T_0}\right) \log_2 \left(1 - \frac{T_s}{T_0}\right) \\ &- \frac{T_s}{T_0} \log_2 \left(\frac{T_s}{T_0} \frac{1}{\max\{k_1, k_2\}}\right), \end{aligned} \quad (2.13)$$

$$\begin{aligned} PTE_{DVFS}^{LDO} &= -\left(1 - \frac{T_s}{T_0}\right) \log_2 \left(1 - \frac{T_s}{T_0}\right) \\ &- \frac{T_s}{T_0} \log_2 \left(\frac{T_s}{T_0} \frac{f_s}{f_{clock}}\right), \end{aligned} \quad (2.14)$$

where f_{clock} is the clock frequency of the AES core.

The PTEs of the aforementioned four different voltage regulation schemes for different number of voltage converter stages are illustrated in Fig. 2.5 when DVFS is employed. In Fig. 2.5, the load power consumption varies from $(1/2)P_{max}$ to $(7/8)P_{max}$ where P_{max} denotes the maximum dynamic power consumption for AES core. The clock frequency is selected between 250 MHz and 450 MHz and the TTE value is 6.02 in [21]. The switching frequency for CoGa and CoRe is 30 MHz.

The PTE of CoRe increases $\sim 40\%$ when DVFS is activated. The primary reason for this enhancement is that the reshuffling behavior is workload-agnostic and DVFS further enhances the scrambling behavior. The PTE of SC voltage converter and LDO regulator also increases to a non-zero value with DVFS, but still much smaller than the PTE of CoRe. Alternatively, the PTE of CoGa reduces $\sim 64\%$ in the presence of DVFS. Therefore, CoRe technique provides significantly higher security as compared to other power delivery schemes when DVFS is activated.

2.6 Conclusion

A new on-chip power management technique, converter-reshuffling (CoRe), is proposed as a power efficient countermeasure against side channel attacks. A theoretical proof based on the power trace entropy (PTE) analysis is developed to compare CoRe with three other existing on-chip power delivery schemes. CoRe performs better than the other schemes with or without DVFS. The PTE of CoRe significantly increases when DVFS is activated whereas other techniques may have degraded PTE levels with DVFS.

CHAPTER 3: TIME-DELAYED CONVERTER-RESHUFFLING TECHNIQUE

3.1 Motivation

A workload-agnostic converter-reshuffling (CoRe) technique has been proposed in *Chapter 2* to randomly activate and deactivate converter stages to scramble the power consumption profile with a pseudo-random number generator (PRNG)¹. The main drawback of the conventional CoRe technique in *Chapter 2* is that the attacker can obtain switching frequency f_s and phase information with machine learning attacks. If the attacker can synchronize the attack with the switching frequency of the on-chip switched-capacitor (SC) converter, the average power within a switching period would leak critical information to the attacker that may annihilate the added security benefit of reshuffling the converter stages.

In this Chapter, a new technique, *time-delayed CoRe*, is introduced to cope with machine learning-based DPA attacks. In the proposed time-delayed CoRe technique, half of converter stages are delayed with a certain time-shift, eliminating possible synchronization of the attacker’s sampling frequency with the switching frequency of the converter. With this technique, the minimum power trace entropy (PTE) value is significantly increased as compared to the conventional CoRe technique in *Chapter 2* under machine learning attacks even when the attacker’s sampling frequency is in complete synchronization with the SC voltage converter.

3.2 Modeling

Entropy is commonly used in information theory to model the level of uncertainty (or randomness) in a given data set. In cryptography, entropy is used to evaluate the security performance

¹The content of this Chapter has been published in [54], the copyright permission can be found in Appendix F.

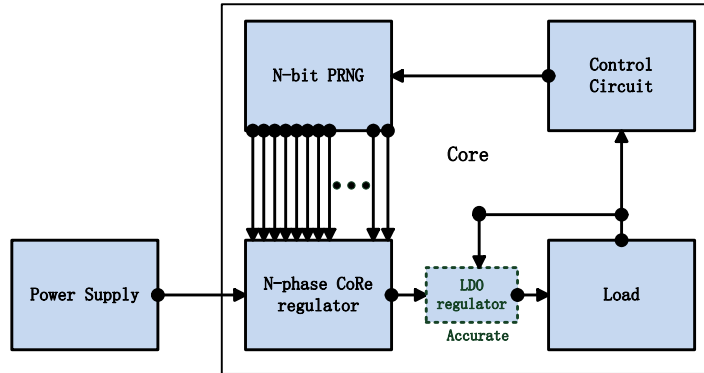


Figure 3.1 Schematic of the CoRe technique.

of integrated systems against side-channel attacks (SCA) [53, 55]. We will use entropy to quantify the security performance of different on-chip voltage converters. The input power of a voltage converter $H_i(t)$, ($i = 1, 2, \dots, k$) can have k different values while delivering the same output power $P_{out}(t)$ to the load circuits depending on the design parameters of the voltage converter and the phase and frequency of the input switching signal. Let's assume that the probability of having different input power values is $p_i(t)$, ($i = 1, 2, \dots, k$). The input power trace entropy $PTE(t)$ of a voltage converter can then be defined as

$$PTE(t) = - \sum_{i=1}^k p_i(t) \log_2^{p_i(t)}. \quad (3.1)$$

3.2.1 Converter-Reshuffling (CoRe) Technique

Primarily, two parameters of an on-chip SC converter can leak the load power information to attackers: switching frequency and number of active converter stages. The switching frequency f_s has a monotonic relationship with the output power P_{out} [52]. f_s is therefore fixed in this Chapter to eliminate possible leakage of the workload information. The number of active converter stages increases with the workload and therefore may leak the workload information to the attacker.

A system level architecture of the CoRe technique is illustrated in Fig. 3.1. The output power resolution N/P_{out} at the output of SC converter can be degraded while using a fixed-frequency

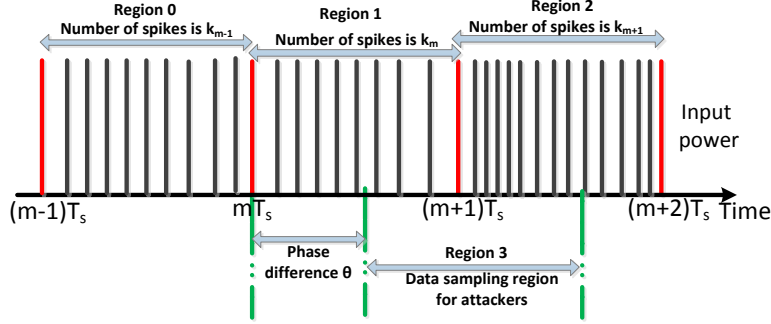


Figure 3.2 Input power profile of the CoRe technique.

modulation if the number of phases N is small. A low-dropout (LDO) regulator can be inserted at the output of the SC converter to mitigate the possible output DC shift. If the number of phases N is sufficiently large, the CoRe technique has a fine output power resolution and the LDO regulator can be removed.

The input power of the CoRe technique, which may be monitored by an attacker, is illustrated in Fig. 3.2. f_s and T_s are, respectively, the switching frequency and period. The number of spikes in regions 0, 1, and 2 are, respectively, k_{m-1} , k_m , and k_{m+1} . The phase difference between switching frequency and data sampling by the attacker is θ and the power consumption at each converter stage is P_0 . To represent the input power information between mT_s and $(m+2)T_s$, an array A_m is defined as

$$A_m = [a_{m,1}, \dots, a_{m,N}, a_{m,(N+1)}, \dots, a_{m,2N}]P_0, \quad (3.2)$$

where $\sum_{i=1}^N a_{m,i} = k_m$, $\sum_{i=N+1}^{2N} a_{m,i} = k_{m+1}$, and $a_{m,i} \in \{0, 1\}$, ($i = 1, 2, \dots, 2N$). We define another array $H_m = [h_1, h_2, \dots, h_{2N}]$ to represent the monitored power data by the attacker within a switching period with the values h_i as

$$h_i = \begin{cases} 0 & , i \leq [\theta/360 * N] \\ 1 & , [\theta/360 * N] < i \leq [\theta/360 * N] + N \\ 0 & , i > [\theta/360 * N] + N . \end{cases} \quad (3.3)$$

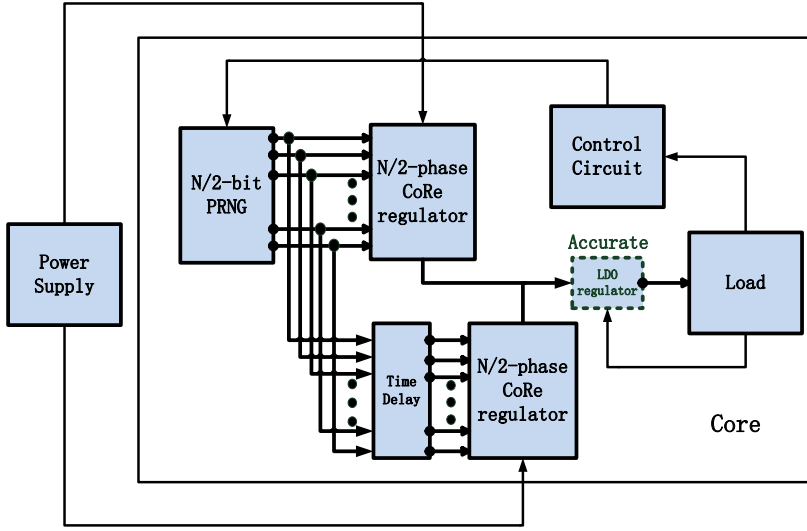


Figure 3.3 Schematic of the proposed time-delayed CoRe technique with an $N/2$ -bit PRNG.

The input power data $P_{s,m}$ sampled by an attacker within a switching period can then be written as

$$P_{s,m} = A_m H_m^T. \quad (3.4)$$

The next step is to enumerate all of the possible arrays A_m and count the number of each sampled power $P_{s,m}$. If the frequency for all the possible sampled power data $P_{s,m}$ is $g_j(\theta, k_m, k_{m+1})$, ($j = 1, 2, \dots, D$) where D is the total number of possible sampled input power data, the corresponding probability $\beta_j(\theta, k_m, k_{m+1})$, ($j = 1, 2, \dots, D$) is

$$\beta_j(\theta, k_m, k_{m+1}) = \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m} \binom{N}{k_{m+1}}}. \quad (3.5)$$

The PTE value of CoRe technique PTE_1 can be written as

$$PTE_1 = - \sum_{j=1}^D \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m} \binom{N}{k_{m+1}}} \log_2 \frac{g_j(\theta, k_m, k_{m+1})}{\binom{N}{k_m} \binom{N}{k_{m+1}}}. \quad (3.6)$$

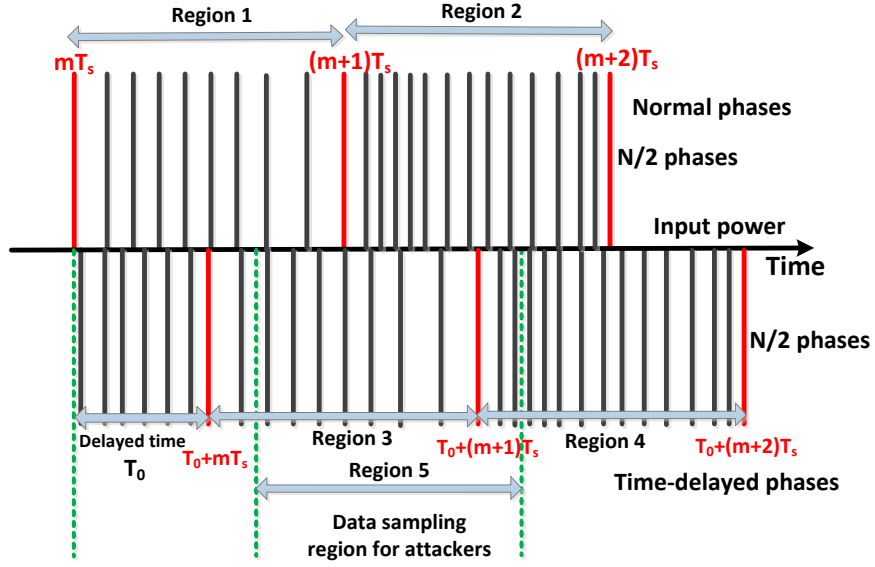


Figure 3.4 Input power of the time-delayed CoRe technique.

To synchronize the attack with the frequency of the voltage converter, an attacker can enter a constant input data to the circuit. Under a constant input sequence, the leakage power consumption within any switching cycle monitored at the input of the CoRe technique would be constant ($k_m = k_{m+1} = \dots$). By analyzing the power profile with machine learning attacks, the attacker can acquire the switching frequency f_s and synchronize the attack to have $\theta = 0^\circ$. PTE value of CoRe technique becomes zero when the phase difference $\theta = 0^\circ$ or 360° , as shown in Fig. 3.6. The proposed time-delayed CoRe technique provides an enhanced protection by maintaining high PTE under machine learning attacks.

3.2.2 Time-delayed Converter-Reshuffling (CoRe) Technique

A time-delayed CoRe technique is proposed to scramble the monitored power consumption so that an attacker will no longer extract meaningful information from the side-channel leakage. In this technique, half of the converter stages in the CoRe scheme will be activated and gated with a time delay, as shown in Fig. 3.3. An $N/2$ -bit PRNG is used to generate the gate signal.

An array B_m is defined to represent the input power information from $(m-1)T_s$ to $(m+2)T_s$, as shown in Fig. 3.4, as

$$B_m = [b_{(m-1),1}, \dots, b_{(m-1),N/2}, b_{(m-1),N/2+1}, \dots, b_{(m-1),N}, b_{(m-1),N+1}, \dots, b_{(m-1),3N/2}]P_0, \quad (3.7)$$

where $b_{(m-1),i} \in \{0, 1\}$, ($i = 1, 2, \dots, 3N/2$) and

$$\begin{aligned} & [\sum_{i=1}^{N/2} b_{(m-1),i}, \sum_{i=N/2+1}^N b_{(m-1),i}, \sum_{i=N+1}^{3N/2} b_{(m-1),i}] \\ & = [k_{m-1}/2, k_m/2, k_{m+1}/2]. \end{aligned} \quad (3.8)$$

In time-delayed CoRe, instead of H_m , there are two different arrays $Z_m = [z_1, z_2, \dots, z_{3N/2}]$ and $W_m = [w_1, w_2, \dots, w_{3N/2}]$ which represent, respectively, the power data monitored by an attacker from the conventional $N/2$ phases and time-delayed $N/2$ phases. z_i and w_i can be written as

$$z_i = \begin{cases} 0 & , i \leq [(\theta/360) * (N/2)] + N/2 \\ 1 & , [(\frac{\theta}{360} * \frac{N}{2}) + \frac{N}{2}] < i \leq [(\frac{\theta}{360} * \frac{N}{2})] + N \\ 0 & , i > [(\theta/360) * (N/2)] + N , \end{cases} \quad (3.9)$$

$$w_i = \begin{cases} 0 & , i \leq [((\theta - \alpha)/360) * (N/2)] + N/2 \\ 1 & , [(\frac{\theta - \alpha}{360} * \frac{N}{2}) + \frac{N}{2}] < i \leq [(\frac{\theta - \alpha}{360} * \frac{N}{2})] + N \\ 0 & , i > [((\theta - \alpha)/360) * (N/2)] + N , \end{cases} \quad (3.10)$$

where $\alpha = (T_0/T_s) * 360^\circ$ is the delayed phase angle and T_0 is the time delay. The input power data $P'_{s,m}$ of time-delayed CoRe that is monitored by an attacker within a switching period becomes

$$P'_{s,m} = B_m Z_m^T + B_m W_m^T. \quad (3.11)$$

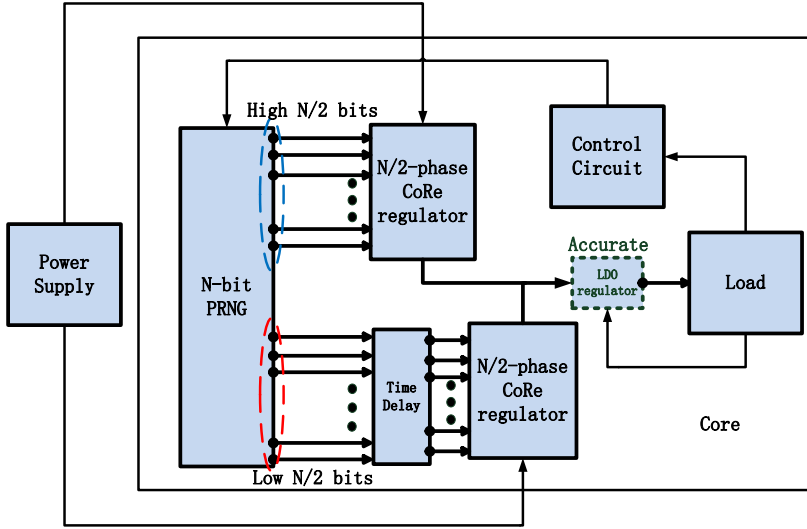


Figure 3.5 Schematic of the proposed time-delayed CoRe technique with an N -bit PRNG.

The next step is to execute all the possible arrays B_m and count the number of each sampled power $P'_{s,m}$. If the number of all possible sampled input power data is $x_j(\theta, k_{m-1}, k_m, k_{m+1})$, ($j = 1, 2, \dots, E$) where E is the total number of possible sampled input power data, then the probability $\gamma_j(\theta, k_{m-1}, k_m, k_{m+1})$, ($j = 1, 2, \dots, E$) for all the possible input power data $P'_{s,m}$ sampled by the attacker is

$$\gamma_j(\theta, k_{m-1}, k_m, k_{m+1}) = \frac{x_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N/2}{k_{m-1}/2} \binom{N/2}{k_m/2} \binom{N/2}{k_{m+1}/2}}. \quad (3.12)$$

The input power trace entropy PTE_2 for time-delayed CoRe technique with an $N/2$ -bit PRNG therefore becomes

$$PTE_2 = - \sum_{j=1}^E \gamma_j(\theta, k_{m-1}, k_m, k_{m+1}) \log_2 \gamma_j(\theta, k_{m-1}, k_m, k_{m+1}). \quad (3.13)$$

To investigate the effect of the PRNG bit length on the entropy level, an N -bit PRNG is used, as shown in Fig. 3.5, as compared to the $N/2$ -bit PRNG, as shown in Fig. 3.3. C'_m and C''_m arrays are defined to represent the input power information of normal phases and time-delayed

phases from $(m-1)T_s$ to $(m+2)T_s$, as shown in Fig. 3.4, and can be written as

$$\begin{aligned} C'_m &= [c'_{(m-1),1}, \dots, c'_{(m-1),N/2}, c'_{(m-1),N/2+1}, \\ &\dots, c'_{(m-1),N}, c'_{(m-1),N+1}, \dots, c'_{(m-1),3N/2}]P_0, \end{aligned} \quad (3.14)$$

$$\begin{aligned} C''_m &= [c''_{(m-1),1}, \dots, c''_{(m-1),N/2}, c''_{(m-1),N/2+1}, \\ &\dots, c''_{(m-1),N}, c''_{(m-1),N+1}, \dots, c''_{(m-1),3N/2}]P_0, \end{aligned} \quad (3.15)$$

where $c'_{(m-1),i}, c''_{(m-1),i} \in \{0, 1\}$, ($i = 1, 2, \dots, 3N/2$), and

$$\begin{aligned} &[\sum_{i=1}^{N/2} (c'_{(m-1),i} + c''_{(m-1),i}), \sum_{i=N/2+1}^N (c'_{(m-1),i} + c''_{(m-1),i}), \\ &\sum_{i=N+1}^{3N/2} (c'_{(m-1),i} + c''_{(m-1),i})] = [k_{m-1}, k_m, k_{m+1}]. \end{aligned} \quad (3.16)$$

The input power data $P''_{s,m}$ of time-delayed CoRe with N -bit PRNG monitored by an attacker within a switching period is

$$P''_{s,m} = C'_m Z_m^T + C''_m W_m^T. \quad (3.17)$$

When all possible values of C'_m and C''_m are listed, the frequency $y_j(\theta, k_{m-1}, k_m, k_{m+1})$, ($j = 1, 2, \dots, F$) for each sampled power $P''_{s,m}$ can be determined, where F is the total number of possible sampled input power data. So the corresponding probability $\lambda_j(\theta, k_{m-1}, k_m, k_{m+1})$, ($j = 1, 2, \dots, F$) is

$$\lambda_j(\theta, k_{m-1}, k_m, k_{m+1}) = \frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}} \binom{N}{k_m} \binom{N}{k_{m+1}}}. \quad (3.18)$$

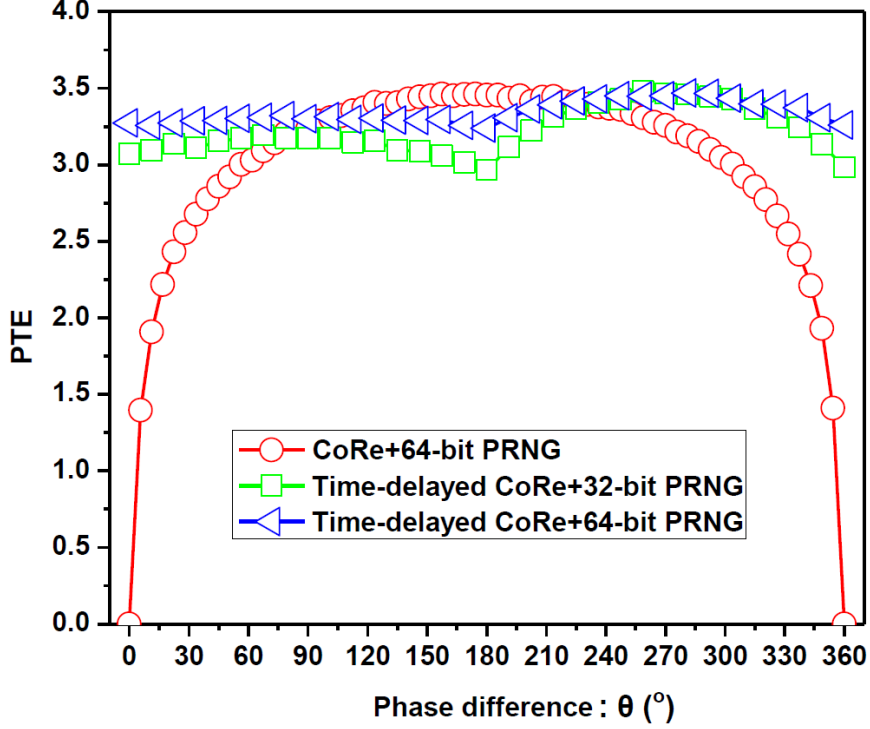


Figure 3.6 PTE value versus the phase difference between switching frequency and data sampling frequency (time delay $T_0 = T_s/2$).

The input power trace entropy PTE_3 for time-delayed CoRe technique with an N -bit PRNG is

$$PTE_3 = - \sum_{j=1}^F \frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}} \binom{N}{k_m} \binom{N}{k_{m+1}}} \log_2 \frac{y_j(\theta, k_{m-1}, k_m, k_{m+1})}{\binom{N}{k_{m-1}} \binom{N}{k_m} \binom{N}{k_{m+1}}}. \quad (3.19)$$

3.3 Results and Discussions

The PTE value for the CoRe technique with a 64 bit PRNG and for time-delayed CoRe technique with 32 and 64 bit PRNGs are shown in Fig. 3.6 when the output power dissipation changes from $(N/2) * \eta P_0$ to $(3N/4) * \eta P_0$. Here, $N=64$ and η is the power efficiency. The PTE value for CoRe technique becomes zero when the phase difference θ between switching frequency and data sampling frequency is 0° or 360° . In this case, the CoRe technique fails to provide any additional security against DPA attacks if machine learning attacks are applied. However, the

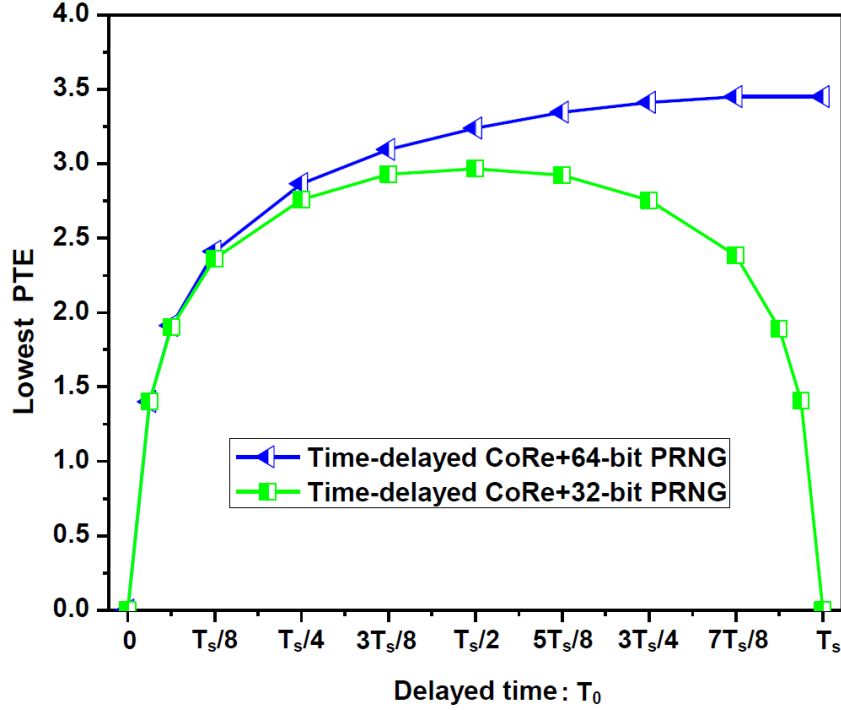


Figure 3.7 Lowest PTE value versus the time delay.

time-delayed CoRe technique continuously demonstrates high PTE values (above 3.2) all the time for $0^\circ < \theta < 360^\circ$. Even if the machine learning-based DPA attacks can determine the activation/deactivation pattern and synchronize the attack with the voltage converter, there still exists a high amount of uncertainty in the monitored data for an attacker to achieve a successful attack. This uncertainty is due to the withholding of charge in some of the converter stages independent of the activation/deactivation pattern. The number of spikes in each switching cycle therefore becomes independent of the workload information and the activation pattern in the proposed technique.

The optimum time delay for the proposed time-delayed CoRe with 32-bit PRNG is $\sim T_s/2$, as shown in Fig. 3.7. The PTE value of the time-delayed CoRe with a 32-bit PRNG, however, becomes zero when the time difference is either zero or a full period. As shown in Fig. 3.7, the PTE value for the time delayed CoRe with a 64-bit PRNG increases monotonically with the time delay since both of the $N/2$ converter stages are controlled by different bits of the PRNG. In a practical design, the selection of time delay T_0 also needs to satisfy $T_0 = n * (\frac{2T_s}{N})$, ($n = 1, 2, \dots, N/2$)

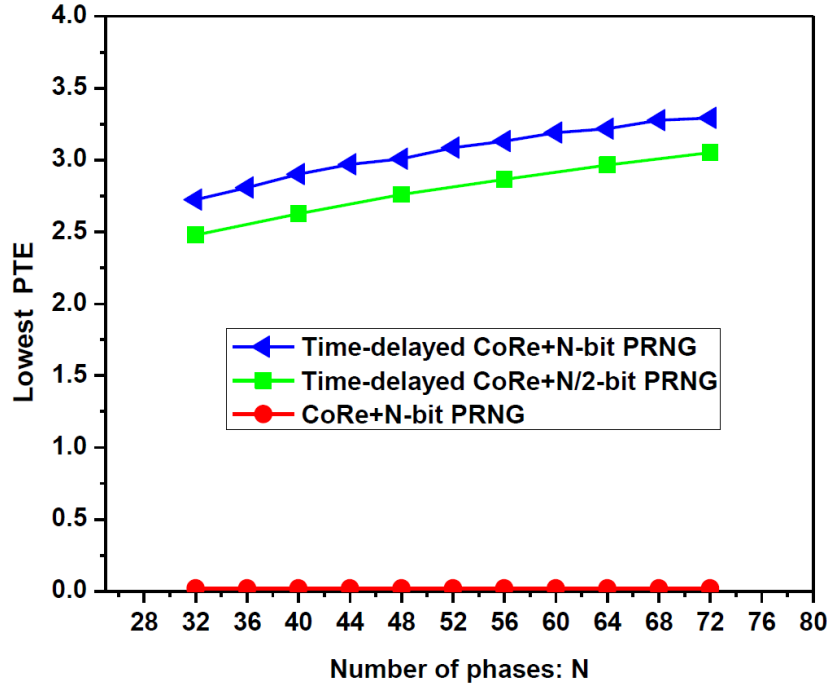


Figure 3.8 Lowest PTE value versus the number of phases ($T_0 = T_s/2$).

to prevent the attacker from splitting the power information of normal phases and time-delayed phases.

When the total number of phases N increases, the lowest PTE value of CoRe technique always maintains at zero while the lowest PTE value of the proposed time-delayed CoRe technique monotonically increases due to higher PRNG entropy, as shown in Fig. 3.8. Time-delayed CoRe technique therefore becomes a more effective countermeasure against machine learning-based DPA attacks with greater number of converter stages.

Please note that the proposed time-delayed CoRe technique only requires one additional circuitry that performs the time delay operation. The area overhead is therefore quite negligible (*i.e.*, less than 1%) as compared to the conventional CoRe technique.

3.4 Conclusion

The conventional CoRe technique is vulnerable under machine learning-based DPA attacks if the attacker synchronizes the attack with the switching frequency of the on-chip voltage converter.

Time-delayed CoRe technique delays half of the converter stages, making it infeasible to synchronize the attack with the switching frequency. An analytical expression for the PTE is developed to evaluate the security-performance of the conventional and time-delayed CoRe techniques. The lowest PTE value of the time-delayed CoRe technique is enhanced significantly even under machine learning-based DPA attacks.

CHAPTER 4: CHARGE-WITHHELD CONVERTER-RESHUFFLING TECHNIQUE

4.1 Motivation

Converter-reshuffling (CoRe) technique in *Chapter 2* utilizes a multi-phase switched capacitor (SC) voltage converter and is based on converter-gating (CoGa) [4] as a countermeasure against DPA attacks with negligible power overhead¹. The number of required converter stages is determined based on the workload information whereas the activation pattern of these stages is determined by a pseudo-random number generator (PRNG) to scramble the input power profile of the voltage converter. As a result, if an attacker is unable to synchronize the sampling frequency of the power data with the switching frequency of the on-chip voltage converter, a large amount of noise is inserted within the leakage data that is sampled by the attacker. Alternatively, if the attacker is able to synchronize the attack with the switching frequency of the on-chip voltage converter by using machine-learning attacks, the scrambled power data can be unscrambled by the attacker and the CoRe technique may effectively be neutralized. The reason is that the total number of activated phases within a switching period has a high correlation with the load power dissipation. A charge-withheld CoRe technique is proposed in this Chapter to prevent the attacker from acquiring accurate load power information even if the attacker can synchronize the data sampling.

The switching frequency f_s of an SC voltage converter is proportional to the output power P_{out} [52]. The fluctuations in f_s therefore can leak critical workload information to the attacker. In the proposed charge-withheld CoRe technique, f_s is kept constant under varying workload conditions (*i.e.*, f_s is workload-agnostic) to minimize the leakage of workload information. Instead, the number of activated phases is adaptively changed to satisfy the workload demand. As compared to

¹The content of this Chapter has been published in [56], the copyright permission can be found in Appendix F.

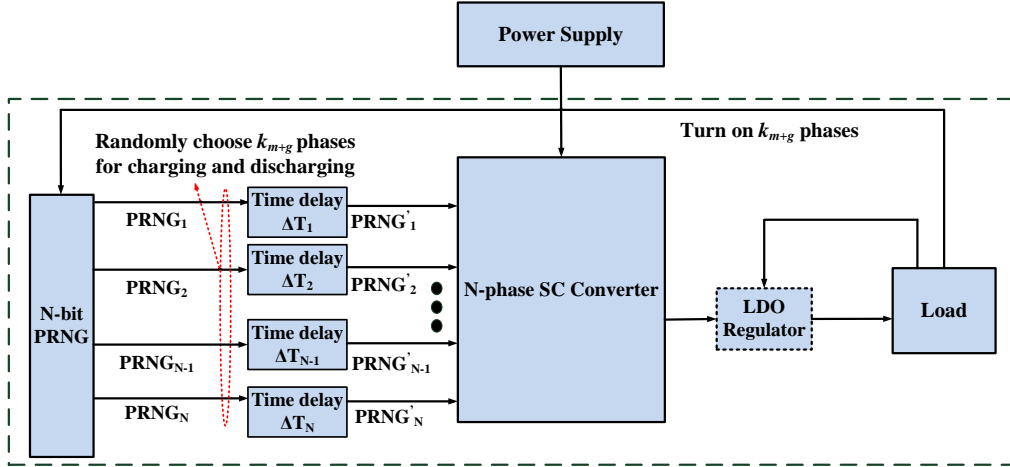


Figure 4.1 Architecture of the conventional CoRe technique.

the CoRe technique where only a single PRNG is utilized, as shown in Fig. 4.1, the charging and discharging states of the flying capacitors in the charge-withheld CoRe technique are controlled by two independent PRNGs ($PRNG_1$ and $PRNG_2$), as illustrated in Fig. 4.4. For instance, for an N -phase charge-withheld CoRe technique, if the load requires to activate k_{m+g} additional phases based on the workload, the $PRNG_1$ would randomly select V_{m+g} , ($k_{m+g} \leq V_{m+g} \leq N$) phases for charging. When the charging period ends, the $PRNG_2$ would choose k_{m+g} phases out of the selected V_{m+g} phases for discharging. As a result, the energy stored in the corresponding $(V_{m+g} - k_{m+g})$ phases is used for power delivery in the next couple of switch cycles. With this charge withhold- ing technique, the total number of activated phases within a switching period is no longer highly correlated with the actual load power consumption.

4.2 Architecture Design

4.2.1 Architecture of the Converter-Reshuffling (CoRe) Technique

In the conventional CoRe technique, the activation/deactivation pattern of a multi-phase SC voltage converter is controlled by an N -bit PRNG, as shown in Fig. 1.1. The PRNG produces an N -bit random sequence $PRNG_i$, ($i = 1, 2, \dots, N$) that is delayed by ΔT_i to get synchronized

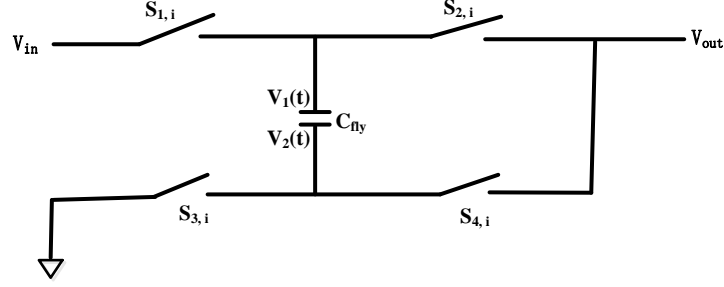


Figure 4.2 One of the identical 2:1 SC voltage converter stages in CoRe.

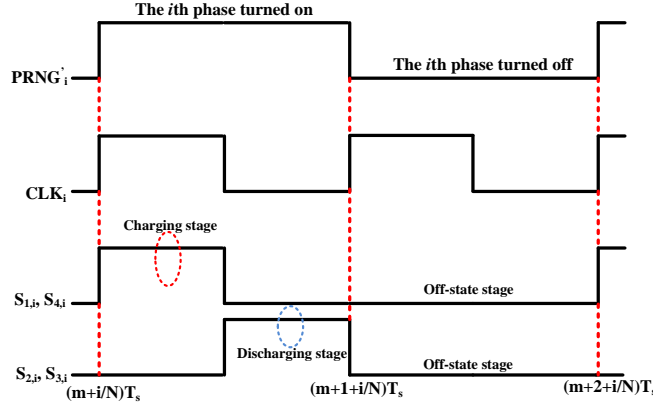


Figure 4.3 Logic level of the signals that control the switches ($S_{1,i}$, $S_{2,i}$, $S_{3,i}$, $S_{4,i}$) within the CoRe technique.

with the clock signal CLK_i generated by a phase shifter. The time delay ΔT_i is

$$\Delta T_i = \frac{i}{N} T_s, \quad (4.1)$$

where $T_s = 1/f_s$ is the switching period. An optional low-dropout (LDO) regulator can be utilized at the output of the CoRe technique if the number of phases N in the SC converter is not sufficient to meet the accuracy requirement of the load.

A high-level schematic of one of the identical phases within the multi-phase SC converter is shown in Fig. 4.2. The time delayed signal $PRNG'_i$, ($i = 1, 2, \dots, N$), as illustrated in Fig. 4.1, with the clock signal CLK_i controls the states of switches ($S_{1,i}$, $S_{2,i}$, $S_{3,i}$, $S_{4,i}$) in the i^{th} converter

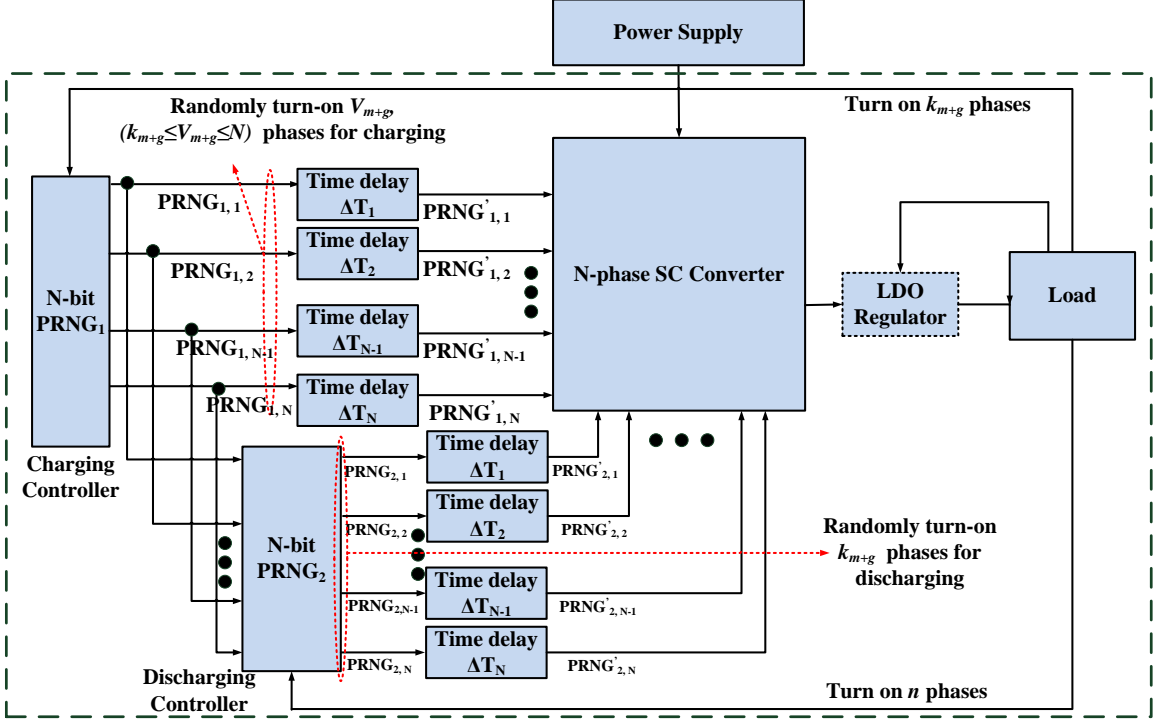


Figure 4.4 Architecture of the proposed charge-withheld CoRe technique.

stage as follows

$$\{S_{1,i}, S_{4,i}\} = PRNG'_i \otimes CLK_i, \quad (4.2)$$

$$\{S_{2,i}, S_{3,i}\} = PRNG'_i \otimes \overline{CLK}_i. \quad (4.3)$$

The corresponding signal waveforms controlling the switches ($S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i}$) are illustrated in Fig. 4.3. The signal $PRNG'_i$ is a binary variable and utilized to determine whether the i^{th} phase should be turned-on or turned-off within the next switching cycle. The circuit level implementation details of the CoRe technique can be found in [4] and [11].

4.2.2 Architecture of the Charge-Withheld Converter-Reshuffling (CoRe) Technique

Two PRNGs ($PRNG_1$ and $PRNG_2$) are utilized in the proposed charge-withheld CoRe technique, as shown in Fig. 4.4. When the load demand changes, a certain number of gated stages, let's say k_{m+g} stages, need to turn on. $PRNG_1$ randomly selects V_{m+g} , ($k_{m+g} \leq V_{m+g} \leq N$) stages

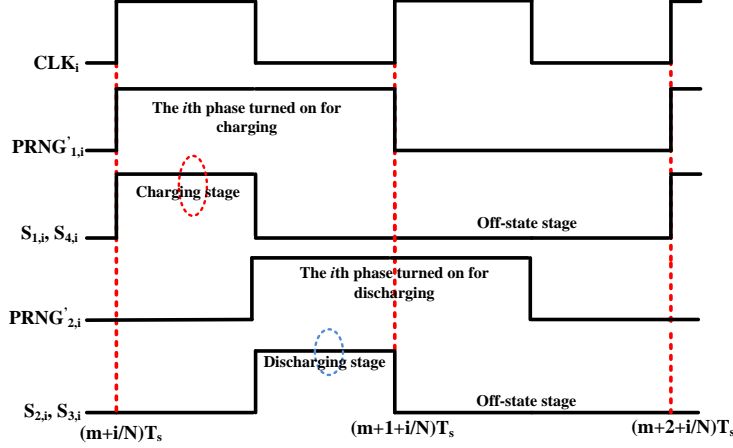


Figure 4.5 Logic level of the signals that control the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ within the charge-withheld CoRe technique.

and concurrently transmits the logic signal $PRNG_{1,i}$, $(i = 1, 2, \dots, N)$ both to the corresponding converter stages and to $PRNG_2$. The i^{th} converter stage turns-on if the corresponding $PRNG'_{1,i}$ value is 1. During the discharging stage, when $PRNG_2$ receives data generated by $PRNG_1$, after half a switching period, $PRNG_2$ sends out signal $PRNG_{2,i}$, $(i = 1, 2, \dots, N)$ to discharge k_{m+g} phases out of the selected V_{m+g} phases by $PRNG_1$. Under this condition, the stages that charge and discharge are independent and controlled, respectively, by $PRNG_1$ and $PRNG_2$. The state of the switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ in charge-withheld CoRe technique is

$$\{S_{1,i}, S_{4,i}\} = PRNG'_{1,i} \otimes CLK_i, \quad (4.4)$$

$$\{S_{2,i}, S_{3,i}\} = PRNG'_{2,i} \otimes \overline{CLK_i}, \quad (4.5)$$

where $PRNG'_{1,i}$ and $PRNG'_{2,i}$ are, respectively, the delayed output signal from $PRNG_1$ and $PRNG_2$. As compared to the conventional CoRe technique, the signal waveforms of switches $(S_{1,i}, S_{2,i}, S_{3,i}, S_{4,i})$ in charge-withheld CoRe are controlled by two different PRNGs, as shown in Fig. 4.5. $PRNG_1$ controls the switches $(S_{1,i}, S_{4,i})$ for charging while $PRNG_2$ controls the switches $(S_{2,i}, S_{3,i})$ for discharging.

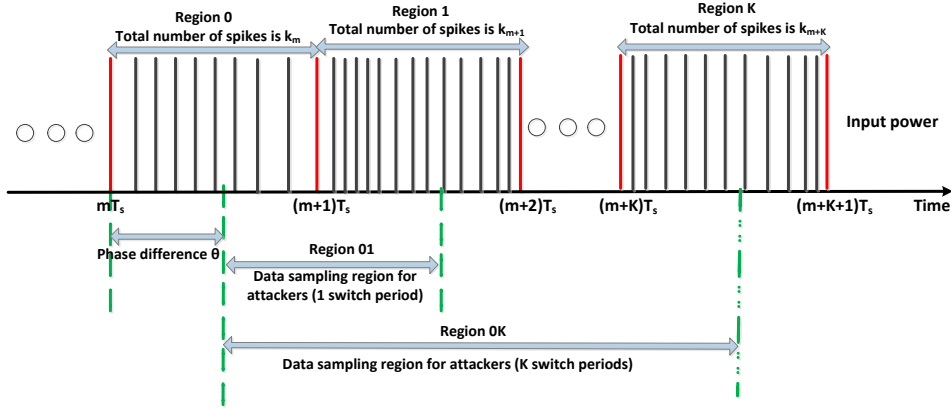


Figure 4.6 Input power profile of the CoRe technique.

4.3 Security Evaluation Model

4.3.1 Security Evaluation Against DPA Attacks

For a cryptographic device with an embedded CoRe technique, an attacker can sample the average input power within a switching period $\overline{P_{in,1}}, \overline{P_{in,2}}, \dots$, and exploit this input data to predict the average dynamic power within a switching period $\overline{P_{pr,1}}, \overline{P_{pr,2}}, \dots$. The attacker can then perform a correlation analysis between the monitored input power and the predicted power to estimate the correct key. Alternatively, the attacker can sample the average input power for a couple of switch cycles to strengthen the attack. For example, the attacker may sample K switch cycles to obtain the average input power where the average input power and predicted power are, respectively, $\sum_{j=1}^K (\overline{P_{in,j}}/K)$ and $\sum_{j=1}^K (\overline{P_{pr,j}}/K)$. The attacker can utilize these data to perform a correlation analysis.

Let's assume that the total number of SC converter phases in the CoRe technique is N and the attacker intends to sample the average input power within K switch cycles. Since there is a phase difference between the switching frequency and data sampling rate, we record the input power information in $(K + 1)$ switch cycles to obtain all of the possible power information of K switch cycles which may be sampled by the attacker. The input power distribution between mT_s

and $(m + K + 1)T_s$, as shown in Fig. 4.6, can be denoted by an array A_m as follows

$$A_m = [a_{m,1}, a_{m,2}, \dots, a_{m,N}, a_{m+1,1}, a_{m+1,2}, \dots, a_{m+1,N}, \dots, a_{m+K,1}, a_{m+K,2}, \dots, a_{m+K,N}]P_0, \quad (4.6)$$

where $a_{m+g,i} \in \{0, 1\}$, ($g = 0, 1, \dots, K$ and $i = 1, 2, \dots, N$) and $\sum_{i=1}^N a_{m+g,i} = k_{m+g}$. P_0 is the power consumed by each converter stage within the CoRe technique and k_{m+g} , ($g = 0, 1, \dots, K$) is the total number of active phases² within a switching period as shown in Fig. 4.6. Another array $W_m = [w_1, w_2, \dots, w_{(K+1)N}]$ is used to represent the position of the spikes which would be recorded by the attacker within K switching periods and the value of the elements w_q , ($q = 1, 2, \dots, (K+1)N$) in W_m becomes

$$w_q = \begin{cases} 0 & , q \leq [\theta/360 * N] \\ 1 & , [\theta/360 * N] < q \leq [\theta/360 * N] + K * N \\ 0 & , q > [\theta/360 * N] + K * N , \end{cases} \quad (4.7)$$

where θ is the phase difference, as illustrated in Fig. 4.6. The average input power within K switching periods $\overline{P_{m,K}}$ sampled by the attacker therefore becomes

$$\overline{P_{m,K}} = \frac{A_m W_m^T}{KN}. \quad (4.8)$$

When all of the possible A_m and W_m arrays are analyzed, the probability $\alpha_l(\theta, k_m, \dots, k_{m+K})$ of the average input power $\overline{P_{m,K}}$ can be written as

$$\alpha_l(\theta, k_m, \dots, k_{m+K}) = \frac{x_l(\theta, k_m, \dots, k_{m+K})}{\sum_{l=1}^G x_l(\theta, k_m, \dots, k_{m+K})}, \quad (4.9)$$

where $x_l(\theta, k_m, \dots, k_{m+K})$, ($l = 1, 2, \dots, G$) is the number of all possible values of $\overline{P_{m,K}}$ induced by different A_m and W_m arrays, and G represents the total number of possible values of $\overline{P_{m,K}}$. The

²Note that the number of active phases is equal to the number of spikes in a switching period.

power trace entropy (PTE) of CoRe technique $PTE_{CR}(\theta)$ then becomes

$$PTE_{CR}(\theta) = - \sum_{l=1}^G H_l \log_2^{H_l}, \quad (4.10)$$

$$H_l = \alpha_l(\theta, k_m, \dots, k_{m+K}), \quad (4.11)$$

and the average PTE value of the CoRe technique $\overline{PTE_{CR}}$ is

$$\overline{PTE_{CR}} = \frac{\int_0^{360} PTE_{CR}(\theta) d\theta}{360}. \quad (4.12)$$

For the charge-withheld CoRe technique, we define a matrix $B_m(K+1, N)$ to denote the phase sequences that are selected for charging within $(K+1)$ consecutive switch cycles by PRNG₁. $B_m(K+1, N)$ can be written as

$$B_m(K+1, N) = \begin{pmatrix} b_{m,1} & \cdot & \cdot & \cdot & b_{m,N} \\ b_{m+1,1} & \cdot & \cdot & \cdot & b_{m+1,N} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ b_{m+K,1} & \cdot & \cdot & \cdot & b_{m+K,N} \end{pmatrix}, \quad (4.13)$$

where $b_{m+g,i} \in \{0, 1\}$, ($g = 0, 1, \dots, K$ and $i = 1, 2, \dots, N$) and $k_{m+g} \leq V_{m+g} = \sum_{i=1}^N b_{m+g,i} \leq N$. Another matrix $C_m(K+1, N)$ is defined to record whether the flying capacitor in the corresponding converter stage has already withheld charge or not before being selected by PRNG₁ for charging. Note the elements $c_{m+g,i}$ in matrix $C_m(K+1, N)$ are also binary. Accordingly, only the i^{th} converter stage which is selected for charging and does not have withheld charge from the previous cycles can exhibit the related power spike in the input power profile. Additionally, we define a matrix $D_m(K+1, N)$ to reflect the input power information within the $(K+1)$ consecutive switching

periods. Note that the elements $d_{m+g,i}$ in $D_m(K+1, N)$ satisfy the following expression

$$d_{m+g,i} = (b_{m+g,i} \otimes 1) \otimes (\overline{c_{m+g,i}} \otimes 1). \quad (4.14)$$

Another binary $(K+1) \times N$ matrix $E_m(K+1, N)$ is used to record the phases which are chosen by PRNG₂ for discharging. The relationship between the elements $e_{m+g,i}$ in $E_m(K+1, N)$ and $b_{m+g,i}$ is

$$b_{m+g,i} - e_{m+g,i} \geq 0, \quad (4.15)$$

$$\sum_{i=1}^N (b_{m+g,i} \otimes e_{m+g,i}) = k_{m+g}. \quad (4.16)$$

Finally, in the voltage conversion system, the number of charged phases needs to be equal to the number of discharged phases plus the number of charge-withheld phases all the time. This constraint is satisfied as

$$c_{m+g+1,i} = c_{m+g,i} + d_{m+g,i} - e_{m+g,i}. \quad (4.17)$$

After all of the elements $d_{m+g,i}$ in $D_m(K+1, N)$ have been obtained, the matrix $D_m(K+1, N)$ can be converted into a $1 \times (K+1)N$ array A'_m which is similar to the array A_m as

$$\begin{aligned} A'_m = & [d_{m,1}, d_{m,2}, \dots, d_{m,N}, d_{m+1,1}, d_{m+1,2}, \dots, d_{m+1,N}, \\ & \dots, d_{m+K,1}, d_{m+K,2}, \dots, d_{m+K,N}] P_0. \end{aligned} \quad (4.18)$$

After satisfying all of the aforementioned constraints, the PTE value of the proposed charge-withheld CoRe technique can be determined with (4.10).

4.3.2 Security Evaluation Against Machine Learning (ML)-Based DPA Attacks

To perform a successful ML based DPA attack, two steps are required. The first step is to determine the switching period and phase difference (T_s, θ) with machine-learning attacks. The

second step is to synchronize the data sampling rate with the switching frequency. To estimate the switching period T_s , the attacker can apply a number of random input data to determine the minimum time gap ΔT_s between the two adjacent spikes in the input power profile. For an N -phase SC converter, the switching period T_s is equal to $N\Delta T_s$, therefore the attacker only needs to determine the number of phases N to acquire the correct T_s .

Assume that the attacker estimates the switching period as $T_s = F\Delta T_s$, ($F = 1, 2, \dots$) and sequentially applies two different input data ($data_1$ and $data_2$) with the frequency $f_0 = 1/(F\Delta T_s)$. The attacker then estimates $\theta = [0 : 360/F : 360]$ as all of the possible phase difference scenarios between the attack and switching frequency to synchronize the attack. If the estimation of (F, θ) is correct, the total number of spikes k_{m+g} , as illustrated in Fig. 4.6, can be written as

$$k_{m+g} = k', (g = 0, 2, 4, \dots) \quad (4.19)$$

$$k_{m+g} = k'', (g = 1, 3, 5, \dots), \quad (4.20)$$

where k' and k'' are, respectively, the total number of input power spikes due to inputs $data_1$ and $data_2$. In this case, the total number of input power spikes within two consecutive switching periods is $(k' + k'')$, which is a constant value. If the attacker can synchronize the attack such that a constant average power profile in any two consecutive switching periods is obtained, the correct switching period and phase difference (T_s, θ) are successfully determined. Once the correct (T_s, θ) are obtained, the attacker can eliminate all of the noise inserted by the CoRe technique and perform a successful DPA attack.

ML based DPA attacks are rather difficult to implement for the charge-withheld CoRe technique as the total number of spikes within a switching period is variable. Even if the attacker can obtain the information about (T_s, θ) and synchronize the attack with the switching frequency, the attacker can only eliminate the noise data induced by the CoRe technique. However, the noise data due to the charge-withholding operation cannot be eliminated with ML based DPA attacks.

4.4 Efficiency Analysis

During the charge-withholding operation, a number of flying capacitors within a multi-stage SC voltage converter are charged. Some of these capacitors maintain the charge for a random number of cycles, instead of discharging after each charging phase. The power dissipation in the form of leakage from the flying capacitors is investigated in this section.

For a multi-phase 2:1 SC converter, as shown in Fig. 4.2, the top plate voltage $V_1(t)$ and the bottom plate voltage $V_2(t)$ of the flying capacitor in a charge-withheld phase can be denoted as follows

$$V_1(t) = (V_{in} - V_{out})e^{(-t/R_{off}C_{fly,top})} + V_{out}, \quad (4.21)$$

$$V_2(t) = V_{out}e^{(-t/R_{off}\alpha C_{fly,top})}, \quad (4.22)$$

where V_{in} and V_{out} are, respectively, the input and output voltages. t is the discharging time, R_{off} is the off-state resistance of the MOSFET switch, $C_{fly,top}$ is the top plate flying capacitance and α is the bottom plate capacitance ratio. The total dissipated energy ratio $\mu(t)$ of the flying capacitor due to the charge leakage can be written as

$$\mu(t) = 1 - \frac{\frac{1}{2}C_{fly,top}V_1^2(t) + \frac{1}{2}\alpha C_{fly,top}V_2^2(t)}{\frac{1}{2}C_{fly,top}V_{in}^2 + \frac{1}{2}\alpha C_{fly,top}V_{out}^2}. \quad (4.23)$$

By substituting (4.21) and (4.22) into (4.23), the number of switch cycles M ($M = t/T_s$) required to deplete the corresponding energy in a flying capacitor can be obtained.

The number of switch cycles M required to dissipate 1% of the total stored energy in the flying capacitor through leakage is about 101 cycles assuming a flying capacitor $C_{fly,top}=1$ pF, the bottom plate capacitance ratio $\alpha = 6.5\%$ [57], input voltage $V_{in}=1.2$ V [58], switching frequency $f_s=60$ MHz [58], and off-state resistance of a MOSFET in 90 nm [58] $R_{off}=240$ M Ω . The proposed charge-withholding technique therefore practically does not cause any efficiency degradation due to the charge leakage from the flying capacitors during the withholding operation.

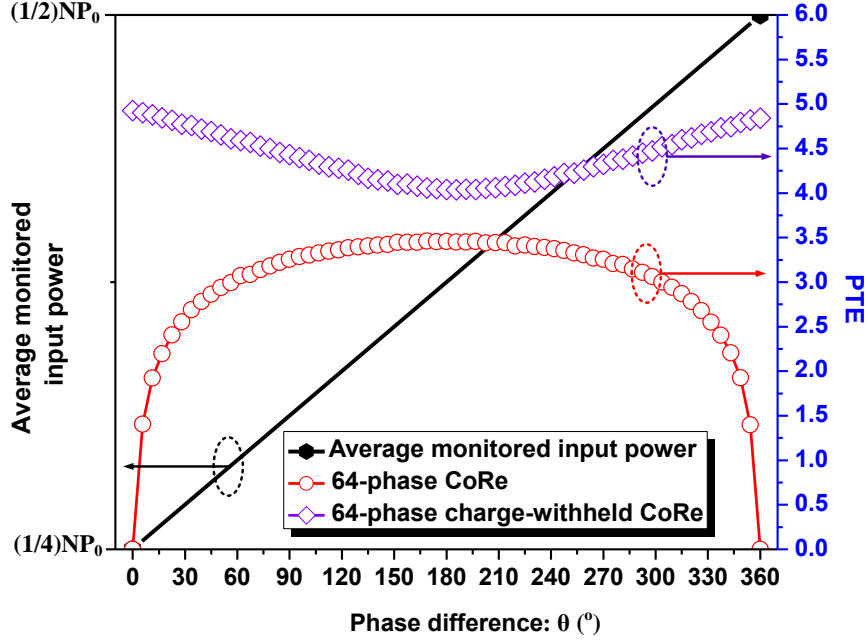


Figure 4.7 PTE value versus the phase difference θ between the switching frequency and data sampling frequency for CoRe and charge-withheld CoRe techniques.

4.5 Results and Discussions

The input PTE versus the phase difference θ for the 64-phase CoRe and the 64-phase charge-withheld CoRe techniques are shown in Fig. 4.7 when the load power varies from $(1/4)\eta NP_0$ to $(1/2)\eta NP_0$. Here η is the power efficiency and the number of switch cycles K sampled by the attackers is 1. As compared to the conventional CoRe technique, the charge-withheld CoRe has two advantages. The proposed technique eliminates the possibility of having zero PTE even when the phase difference θ is 0° or 360° . Additionally, the average PTE value of the proposed charge-withheld CoRe technique is enhanced by about 46.1% as compared to the conventional CoRe technique.

The effect of the sampling period KT_s on the average PTE value is also investigated. The average PTE value of the conventional CoRe technique slightly decreases when KT_s increases (as shown in Fig. 4.8). Alternatively, the average PTE value of the proposed charge-withheld CoRe technique increases more than 20% when KT_s increases three-fold. Further increasing KT_s does not result in a significant change in PTE as PTE converges to a certain value. The primary reason

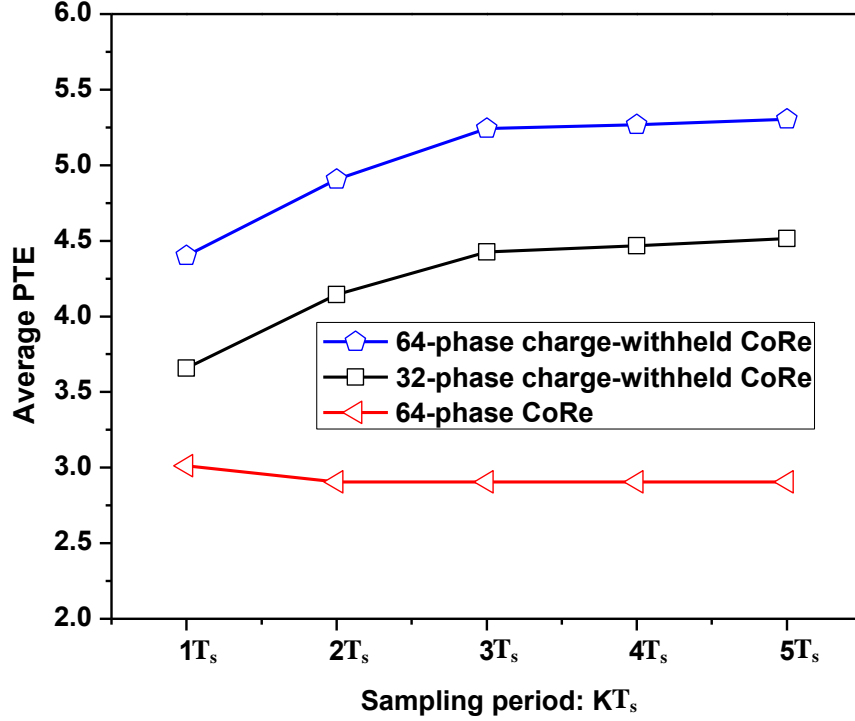


Figure 4.8 Average PTE value versus the number of switch cycles sampled by the attacker for CoRe and charge-withheld CoRe techniques.

for the convergence of PTE is that as the attacker increases the sampling period, the probability for the withheld charge to be delivered to the power grid within the same sampling period increases. Since the effective number of charge withholding from one sampling cycle to another sampling cycle reduces by increasing the attacker's sampling period, the PTE value converges to a constant value. Lastly, the impact of the number of stages within the SC voltage converter on the average PTE value is investigated, as shown in Fig. 4.9. The average PTE value increases with a larger number of phases N for both conventional and charge-withheld CoRe techniques. The average PTE value of the proposed charge-withheld CoRe technique, however, has a steeper slope, indicating better security-performance against DPA attacks with a larger number of converter phases.

The flying capacitors that withhold charge in the charge-withheld CoRe technique cannot be utilized as a filter capacitor as these capacitors are not connected to the output node during the charge-withholding operation. This would slightly increase the output voltage ripple. For example, the amplitude of the output ripple voltage increases less than 2.5 mV for a 32 phase SC voltage

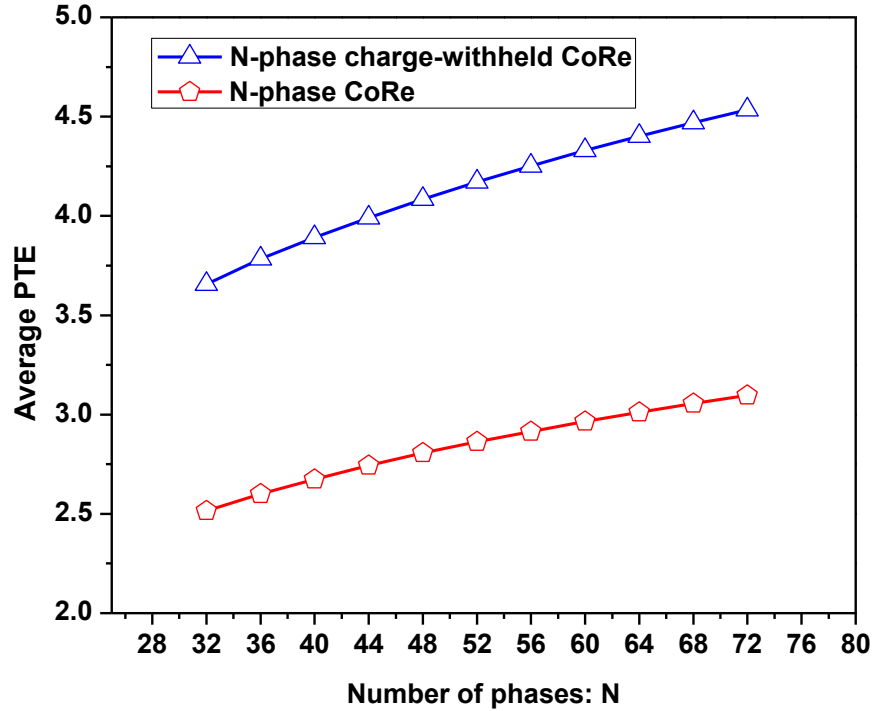


Figure 4.9 Average PTE value versus the number of SC voltage converter phases N for CoRe and charge-withheld CoRe techniques.

converter when only eight of the stages are active. Alternatively, the ripple amplitude increases less than 1 mV when more than half of the stages are active. The increase in the ripple voltage can be mitigated by increasing the number of SC converter stages. If the number of stages is increased from 32 to 48, the ripple amplitude would be reduced by 40%.

4.6 Conclusion

The proposed charge-withheld CoRe technique withholds a random portion of input charge and delivers this charge to the power network after a random time period. This proposed technique is more effective than the conventional CoRe technique against DPA attacks and ML based DPA attacks. The possibility of having zero PTE under certain conditions is successfully eliminated and the average PTE value is increased more than 46% with negligible power loss due to the leakage of flying capacitors. Since the charge that is withheld for a random amount of time is eventually delivered to the power grid, there is no additional power overhead.

CHAPTER 5: CO-DESIGNING CORE TECHNIQUE WITH AES ENGINE

5.1 Introduction

DPA attacks are high efficiency and low cost power attacks, which are widely utilized by attackers to leak the critical information of cryptographic circuit¹. Various countermeasures have been proposed against DPA attacks [7, 60–64]. Although certain countermeasures are quite effective to increase the trustworthiness of modern integrated circuits (ICs), the corresponding power, area, and performance overheads of existing countermeasures are typically quite large to be widely utilized.

There is a growing trend to integrate voltage regulators (VRs) fully on-chip in modern ICs to reduce the power noise, improve transient response time and increase power efficiency [65–68]. A one-to-one relationship exists between the input current I_{in} and load current I_{load} , as shown in Fig. 5.1, when a conventional on-chip VR (such as a low-dropout (LDO) regulator, a buck converter, and a switched-capacitor (SC) converter) is utilized. Therefore, an attacker can determine *what is going on inside a CC* by monitoring the input power profile of a conventional on-chip VR [54]. To break the one-to-one relationship between the input current and load current, converter-gating (CoGa) technique is proposed in [4] to achieve a non-injective relationship between the input current and output current. A multi-phase SC converter is utilized in the CoGa technique where the total number of active converter phases is adaptively altered based on the load power requirement to achieve a high power conversion efficiency [4]. A pseudo-random number generator (PRNG) is also inserted to randomize the sequence of the activated phases when the load current changes. However, if the variation in the load current is small, as shown in Fig. 5.2, CoGa technique is not

¹The content of this Chapter has been published in [59], the copyright permission can be found in Appendix F.

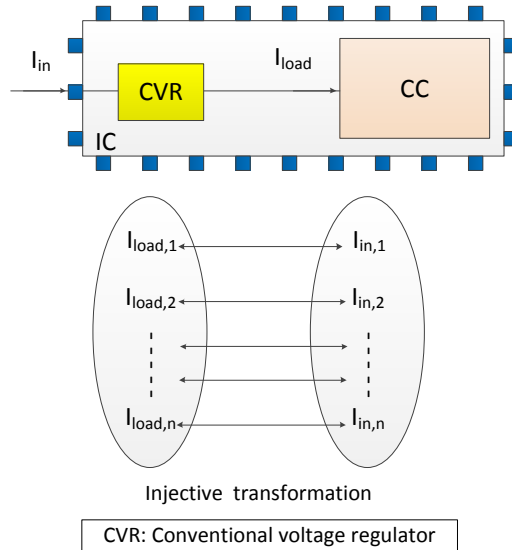


Figure 5.1 One-to-one relationship between the input current and load current in conventional voltage regulator.

activated. To increase the variance of injected random power noise by the on-chip VR, converter-reshuffling (CoRe) technique is proposed to randomly reshuffle the sequence of active and gated stages in every switching cycle even when the change in the load current is small. The primary difference between the CoGa and CoRe techniques is the design of the PRNG. As compared to the CoGa regulator, the correlation coefficient between the input power and load power of the CoRe regulator is significantly reduced due to the larger variance of the inserted random power noise by reshuffling the active and gated stages. Multiphase on-chip VRs can be distributed across the die or implemented at a centralized location [69–71]. Therefore, the security implications of the centralized and distributed on-chip voltage regulation with the proposed CoRe technique are investigated based on the correlation coefficient between the input power and side-channel power².

A pipelined advanced encryption standard (AES) engine is a widely used CC due to the low path delay [72–74]. In a typical 128-bit pipelined AES engine, 16 substitution-boxes (S-boxes) are required in the 1st round encryption (each S-box is 8-bit), where each of the 16 S-boxes works independently. In a practical attack, if the attacker intends to attack one of those 16 S-boxes during the 1st encryption round, the attacker can dynamically alter the 8-bit input plaintext that

²Side-channel power represents the power consumption induced by the S-box under attack.

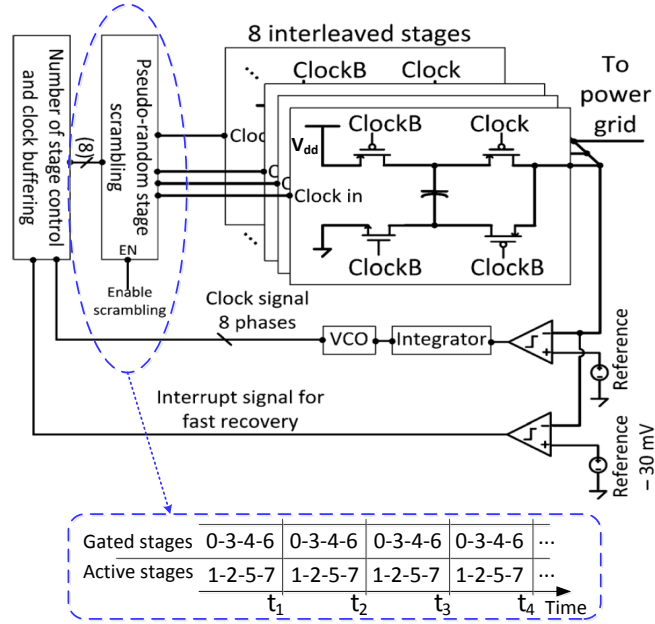


Figure 5.2 CoGa regulator in [4] (8-phase) exhibits a constant sequence of active stages if the variation in load current is small.

corresponds to the input of the S-box under attack. The other plaintexts that are applied to the other 15 S-boxes which are not under attack are kept constant. As a result, the transient power noise generated by these 15 S-boxes which are not under attack would be greatly reduced and only a small amount of leakage power is dissipated within these S-boxes.

If the 15 S-boxes which are not under attack can exhibit a high dynamic power consumption even when the attacker applies a constant input plaintext, this dynamic power consumption can be randomized with the CoRe technique to further decrease the correlation between the input power and side-channel power. Therefore, an improved pipelined AES engine is proposed where invert boxes are added at the inputs of the S-boxes with a negligible area and power overhead. A clock signal with half of the frequency of the input plaintext is utilized to control all of the added invert boxes to ensure that all of the S-boxes would always have a high dynamic power consumption even if their input plaintexts are constant.

We introduce the CoRe technique in *Chapter 2* where we demonstrate the working principle without providing a detailed analytic model. In *Chapter 3*, a certain time delay is inserted in the CoRe technique while activating the phases to eliminate the possibility of having zero entropy

under machine learning attacks. A finite amount of charge is withheld in the flying capacitor for a random amount of time in *Chapter 4* to increase the entropy of the input power profile. The key contributions of this Chapter are to lay the mathematical foundations of the CoRe technique through a detailed analysis of the correlation between the input and output power of both conventional and proposed voltage regulation techniques. The correlation coefficient and measurement to disclose (MTD) are used as the security metric in this Chapter instead of the power trace entropy used in [11, 54, 56]. The implications of the physical placement of the VRs on the correlation coefficient are investigated with centralized and distributed implementations of the CoRe regulators. We have recently noticed that the CoRe technique with an improved pipelined AES engine inserts both additive and multiplicative noise to the input power profile. An improved lightweight AES engine is accordingly proposed to further scramble the input power even if the attacker applies a constant plaintext to the S-boxes that are not under attack. The security implications of the proposed techniques are analytically proven using the correlation coefficient and MTD.

5.2 Security of a Switching Converter against Power Analysis Attacks

The correlation coefficient between the input data and actual dynamic power dissipation of a cryptographic circuit (CC) γ is [75]

$$\gamma \simeq \sqrt{\frac{m_0}{m_1}} \quad (5.1)$$

and the corresponding MTD value is [75]

$$MTD \propto \frac{1}{\gamma^2}, \quad (5.2)$$

where m_1 is the total number of bits of the input data and m_0 is the number of bits which strongly correlates with the actual dynamic power consumption in the input data. The correlation coefficient γ between the input data and actual dynamic power consumption is determined by the architecture of a CC. If the architecture of a CC is not modified at runtime γ and MTD would not have a significant variation.

A switching converter has two phases in each switching period: charging phase and discharging phase. The average input power within a switching period strongly correlates with the load power within that switching period. Let us assume that the switching frequency of the converter is f_s and the clock frequency of the CC is f_c . In modern ICs, f_c is typically greater than f_s [71, 76] (we assume $f_c = M_1 f_s$). To obtain accurate power data generated by a CC from the input side of the switching converter, the attacker needs to sample the average input power within a switching period as one sample of the power data. However, from a CC without a switching converter, the attacker can obtain M_1 different power data samples within that switching period. As a result, if a CC is powered with a switching converter, the MTD is inherently enhanced M_1 times, as compared to the MTD of a CC without a switching converter. Decreasing the switching frequency is therefore an effective way to enhance the MTD value, but lower switching frequency may increase the area of output capacitance of the voltage converter. So there is a trade-off between the area and security of switching converters.

5.3 Correlation Analysis of On-Chip Voltage Regulators

In this section, the correlation coefficient models are presented for the CoGa and CoRe techniques as well as for the conventional on-chip VRs.

5.3.1 Modeling Correlation Coefficient of Converter-Gating (CoGa) and Converter-Reshuffling (CoRe) Regulators

The CoGa regulator [4] consists of two types of modulations: frequency modulation and number of activated phases modulation. The switching frequency f_s in CoGa regulator has a narrow variation range $[f_{s,pk} - \Delta f_s/2, f_{s,pk} + \Delta f_s/2]$, where $f_{s,pk}$ is the corresponding switching frequency to achieve the peak power conversion efficiency and Δf_s is the amplitude of the variation in the switching frequency f_s . If f_s is higher than $f_{s,pk} + \Delta f_s/2$, an additional phase is activated to provide more power to the load. When an additional phase is activated, f_s is reduced to a nominal value. If f_s is lower than $f_{s,pk} - \Delta f_s/2$, an active phase is gated to reduce the output power while f_s is increased to a nominal value.

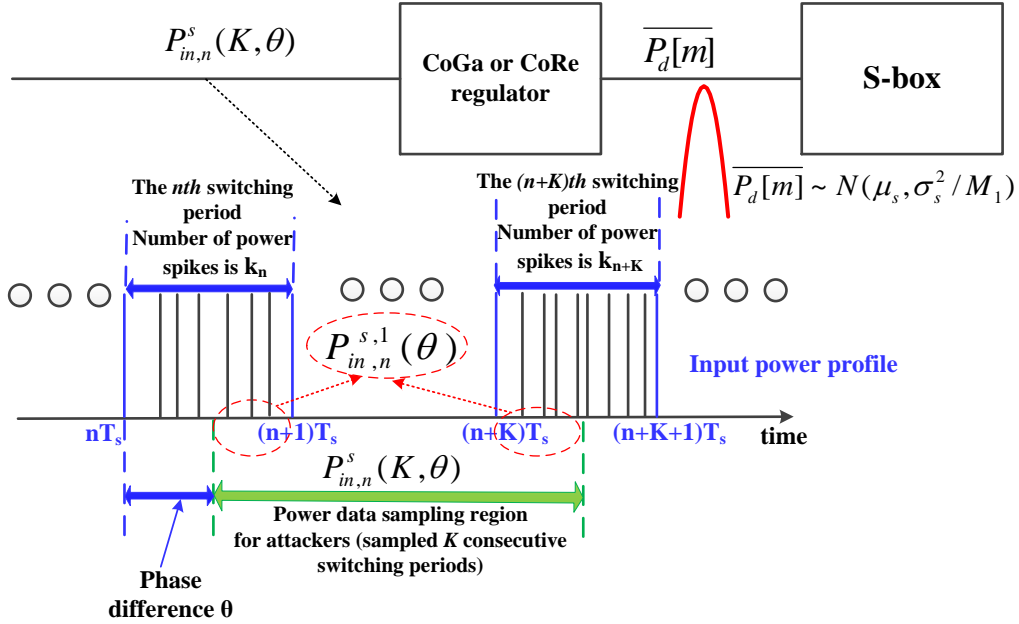


Figure 5.3 Input power data sampling for the attacker within K consecutive switching periods when the CoGa or CoRe techniques are enabled (T_s is the switching period of the CoGa or CoRe regulator).

To investigate the security implications of CoGa or CoRe regulator, the type of power noise generated by CoGa and CoRe regulators needs to be determined. Two different types of noise can be inserted into a system: additive noise and multiplicative noise. The input power of CoGa or CoRe regulator P_{in} can be defined as

$$P_{in} = a_o \times P_{load} + b_o, \quad (5.3)$$

where P_{load} is the load power dissipation of CoGa or CoRe regulator. a_o and b_o , respectively, represent multiplicative and additive noise. If the load power P_{load} is zero, the input power P_{in} is also equal to zero. Therefore, $b_o = 0$ and only the multiplicative noise exists in CoGa or CoRe regulator. Since signal-to-noise ratio (SNR) is not a convenient metric for modeling multiplicative noise, correlation coefficient between the input power and load power is used as the metric to evaluate the security of on-chip VR [7, 8].

The dynamic power consumption $P_d[m]$ of a single S-box in an AES engine induced by the m^{th} , ($m = 1, 2, \dots$) input plaintext conforms to a normal distribution [75], where the mean and variance of $P_d[m]$ are, respectively, μ_s and σ_s^2 . Assuming that the clock frequency of the AES engine is M_1 times greater than the switching frequency of the CoGa or CoRe regulator (*i.e.*, $f_c = M_1 f_s$), the average dynamic power consumption of a single S-box within a switching period $\overline{P_d[m]}$ can be written as

$$\overline{P_d[m]} = \sum_{p=0}^{M_1-1} \frac{P_d[m+p]}{M_1}. \quad (5.4)$$

When $P_d[m], P_d[m+1], \dots, P_d[m+M_1-1]$ are mutually independent, the average dynamic power consumption of a single S-box within a switching period $\overline{P_d[m]}$ also conforms to a normal distribution with mean $\overline{\mu_s}$ and variance $\overline{\sigma_s^2}$ as

$$\overline{\mu_s} = \sum_{p=0}^{M_1-1} \frac{\mu_s}{M_1} = \mu_s, \quad (5.5)$$

$$\overline{\sigma_s^2} = \sum_{p=0}^{M_1-1} \left(\frac{\sigma_s}{M_1} \right)^2 = \frac{\sigma_s^2}{M_1}. \quad (5.6)$$

The minimum and maximum average dynamic power dissipation of a single S-box within a single switching period are, respectively, $j_{min}P_0$ and $j_{max}P_0$ where P_0 is the power resolution. Assuming P_0 is sufficiently small, the following approximated equation can be written as

$$\sum_{j=j_{min}}^{j_{max}} \frac{P_0 \sqrt{M_1}}{\sigma_s \sqrt{2\pi}} \exp\left(-\frac{(j \times P_0 - \mu_s)^2}{2\sigma_s^2/M_1}\right) \approx 1. \quad (5.7)$$

If the total number of input plaintexts applied by the attacker is W , the number W_j which corresponds to the average dynamic power of a single S-box jP_0 , ($j \in [j_{min}, j_{max}]$) within a switching

period can be approximated as

$$W_j \approx W \frac{P_0 \sqrt{M_1}}{\sigma_s \sqrt{2\pi}} \exp\left(-\frac{(j \times P_0 - \mu_s)^2}{2\sigma_s^2 / M_1}\right). \quad (5.8)$$

If the attacker intends to sample $K, (K = 1, 2, \dots)$ consecutive switching periods as one sample of power data, as shown in Fig. 5.3, the input power distribution among the $(n + u)T_s$ and $(n + u + 1)T_s, (n = 0, 1, \dots, u = 0, 1, 2, \dots)$ period can be denoted by array A_{n+u} as

$$A_{n+u} = [a_{n+u,1}, a_{n+u,2}, \dots, a_{n+u,N}]P, \quad (5.9)$$

where P is the power consumed by each phase, N is the total number of phases of CoGa or CoRe regulator, and $a_{n+u,i} \in \{0, 1\}, (i = 1, 2, \dots, N)$. Another array $G(\theta) = [g_1(\theta), g_2(\theta), \dots, g_N(\theta)]$ is used to store the range of sampled input power spikes within the n^{th} switching period where θ is the phase difference between the switching frequency and frequency of data sampling. The elements $g_i(\theta)$ in $G(\theta)$ array are

$$g_i(\theta) = \begin{cases} 0 & , i \leq [\theta/2\pi \times N] \\ 1 & , [\theta/2\pi \times N] < i \leq N. \end{cases} \quad (5.10)$$

The total sampled input power by the attacker within K consecutive switching periods $P_{in,n}^s(K, \theta)$, as shown in Fig. 5.3, is

$$\begin{aligned} P_{in,n}^s(K, \theta) &= A_n G(\theta)^T + A_{n+K} \overline{G(\theta)}^T + \sum_{u=1}^{K-1} \frac{j_{n+u} P_0}{\eta_0} \\ &= P_{in,n}^{s,1}(\theta) + \sum_{u=1}^{K-1} \frac{j_{n+u} P_0}{\eta_0}, \end{aligned} \quad (5.11)$$

where a complementary array $\overline{G(\theta)} = [\overline{g_1(\theta)}, \overline{g_2(\theta)}, \dots, \overline{g_N(\theta)}]$ is used to represent the range of input power sampling within the $(n + K)^{th}$ switching period, where η_0 is the power efficiency of CoGa or CoRe regulator and $j_{n+u} \in [j_{min}, j_{max}]$.

For the CoRe regulator, the total number of power spikes k_{n+u} within the $(n+u)^{th}$ switching period can be determined as

$$k_{n+u} = \lceil \frac{j_{n+u} \times P_0}{\eta_0 \times P} \rceil. \quad (5.12)$$

Additionally, the element $a_{n+u,i}$ in A_{n+u} needs to satisfy $\sum_{i=1}^N a_{n+u,i} = k_{n+u}$.

In the CoRe regulator, the total sampled input power within the n^{th} switching period and the $(n+K)^{th}$ switching period is $P_{in,n}^{s,1}(\theta) = lP$, ($l = 0, 1, 2, \dots, N$). The number of the corresponding input power samples can be counted as $x_{l,j_n,j_{n+K}}(\theta)$ after all of the possible A_n and A_{n+K} are enumerated. When W input plaintexts are applied by the attacker, the number of total input power samples $x_l(\theta)$ for the corresponding sampled input power $P_{in,n}^{s,1}(\theta)$ can be calculated as

$$x_l(\theta) = \sum_{j_{n+K}=j_{min}}^{j_{max}} \sum_{j_n=j_{min}}^{j_{max}} W_{j_n} W_{j_{n+K}} x_{l,j_n,j_{n+K}}(\theta). \quad (5.13)$$

The mean value of the total sampled input power within K consecutive switching periods $\mu_{in}(K, \theta)$ becomes³

$$\begin{aligned} \mu_{in}(K, \theta) &= E(P_{in,n}^s(K, \theta)) \\ &= E(P_{in,n}^{s,1}(\theta)) + E\left(\sum_{u=1}^{K-1} \frac{j_{n+u} P_0}{\eta_0}\right) \\ &= \frac{\sum_{l=0}^N lP \times x_l(\theta)}{\sum_{l=0}^N x_l(\theta)} + (K-1)\mu'_s, \end{aligned} \quad (5.14)$$

where μ'_s is

$$\mu'_s \approx \sum_{j=j_{min}}^{j_{max}} \frac{jP_0\sqrt{M_1}}{\eta_0\sigma_s\sqrt{2\pi}} \exp\left(-\frac{(j \times P_0 - \mu_s)^2}{2\sigma_s^2/M_1}\right). \quad (5.15)$$

³ E represents the sign for the calculation of the mean value.

The variance of total sampled input power within K consecutive switching periods $\sigma_{in}^2(K, \theta)$ can be written as⁴

$$\begin{aligned}
\sigma_{in}^2(K, \theta) &= Var(P_{in,n}^s(K, \theta)) \\
&= Var(P_{in,n}^{s,1}(\theta)) + Var\left(\sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0}\right) \\
&= \frac{\sum_{l=0}^N (x_l(\theta) \times (lP - \mu_{in}(\theta))^2)}{\sum_{l=0}^N x_l(\theta)} + (K-1)(\sigma'_s)^2,
\end{aligned} \tag{5.16}$$

where $(\sigma'_s)^2$ is

$$(\sigma'_s)^2 = \frac{1}{j_{max} - j_{min} + 1} \sum_{j=j_{min}}^{j_{max}} (jP_0/\eta_0 - \mu'_s)^2. \tag{5.17}$$

The load power of the CoRe regulator $P_{load,n}(K, \theta)$ that corresponds to the sampled input power $P_{in,n}^s(K, \theta)$ can be written as

$$P_{load,n}(K, \theta) = \left(1 - \frac{\theta}{2\pi}\right)j_{n+1}P_0 + \frac{\theta}{2\pi}j_{n+K+1}P_0 + \sum_{u=2}^K j_{n+u}P_0. \tag{5.18}$$

The mean value of the load power $\mu_L(K, \theta)$ and variance of the load power $\sigma_L^2(K, \theta)$, respectively, are

$$\mu_L(K, \theta) = \left(1 - \frac{\theta}{2\pi}\right)\mu_s + \frac{\theta}{2\pi}\mu_s + (K-1)\mu_s = K\mu_s, \tag{5.19}$$

$$\sigma_L^2(K, \theta) = \left(1 - \frac{\theta}{2\pi}\right)\frac{\sigma_s^2}{M_1} + \frac{\theta}{2\pi}\frac{\sigma_s^2}{M_1} + (K-1)\frac{\sigma_s^2}{M_1} = \frac{K\sigma_s^2}{M_1}. \tag{5.20}$$

⁴*Var* represents the sign for the calculation of the variance.

The correlation coefficient of the on-chip CoRe regulator $\gamma(K, \theta)$ is determined as⁵

$$\gamma(K, \theta) = \frac{E(P_{in,n}^s(K, \theta) \times P_{load,n}(K, \theta))}{\sigma_{in}(K, \theta) \times \sqrt{K/M_1}\sigma_s} - \frac{\mu_{in}(K, \theta) \times K\mu_s}{\sigma_{in}(K, \theta) \times \sqrt{K/M_1}\sigma_s}, \quad (5.21)$$

where $E(P_{in,n}^s(K, \theta) \times P_{load,n}(K, \theta))$ is

$$\begin{aligned} E(P_{in,n}^s(K, \theta) \times P_{load,n}(K, \theta)) &= \frac{1}{(j_{max} - j_{min} + 1)^{K+2}} \times \\ &\left(\sum_{j_{n+K+1}=j_{min}}^{j_{max}} \dots \sum_{j_n=j_{min}}^{j_{max}} \left((P_{in,n}^{s,1}(\theta) + \sum_{u=1}^{K-1} \frac{j_{n+u}P_0}{\eta_0}) \times \right. \right. \\ &\left. \left. \left(\left(1 - \frac{\theta}{2\pi}\right)j_{n+1}P_0 + \frac{\theta}{2\pi}j_{n+K+1}P_0 + \sum_{u=2}^K j_{n+u}P_0 \right) \right) \right). \end{aligned} \quad (5.22)$$

The average correlation coefficient of the CoRe regulator $\overline{\gamma(K)}$ can be denoted as

$$\overline{\gamma(K)} = \frac{1}{2\pi} \int_0^{2\pi} \gamma(K, \theta) d\theta. \quad (5.23)$$

The correlation coefficient modeling of the CoGa regulator is quite similar to the modeling of the CoRe regulator with one extra condition that needs to be added to the element $a_{n+u,i}$ in A_{n+u} as

$$\begin{cases} a_{n+u+1,i} - a_{n+u,i} \geq 0 & , \text{ if } k_{n+u+1} \geq k_{n+u} \\ a_{n+u,i} - a_{n+u+1,i} \geq 0 & , \text{ if } k_{n+u} < k_{n+u+1} . \end{cases} \quad (5.24)$$

5.3.2 Modeling Correlation Coefficient of Conventional On-Chip Voltage Regulators

Conventional on-chip (COC) VRs such as LDO regulator/buck converter/SC converter typically do not insert any randomness in the input or output power profile unless their architectures are tailored to scramble the input and output impedance characteristics. The relationship between

⁵The attacker sampled the total input power within K consecutive switching periods as one sample of the power data.

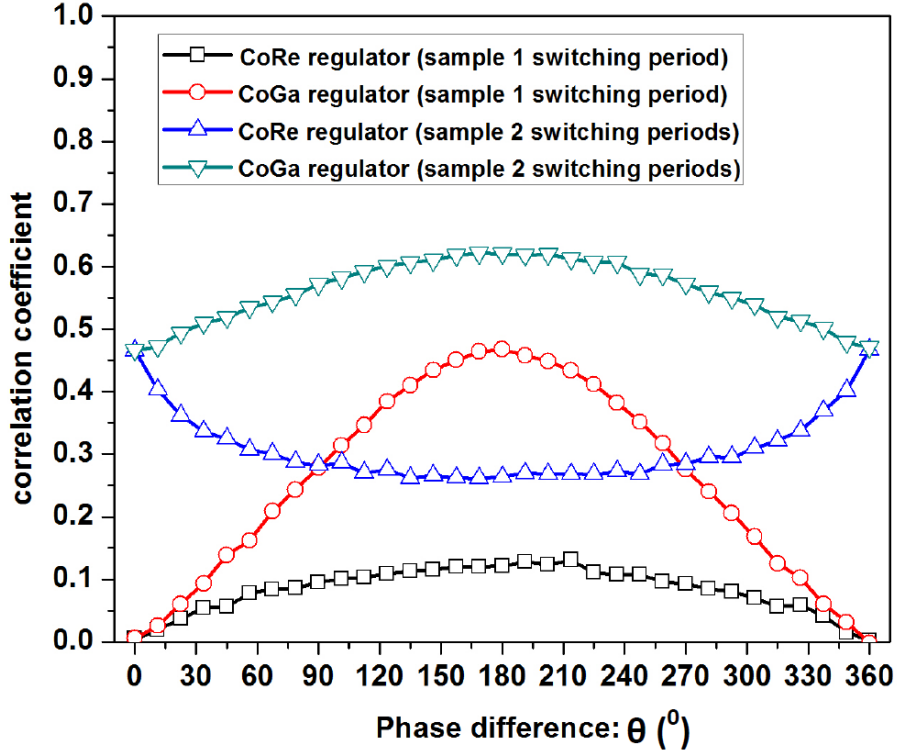


Figure 5.4 Phase difference versus correlation coefficient of CoGa and CoRe techniques.

the input power and load power of a COC VR can be modeled as

$$P'_{in}(t + \Delta t) = \frac{1}{\eta_1} \times P_{load}(t), \quad (5.25)$$

where Δt is the time delay between the input power and load power, η_1 is the power efficiency, $P'_{in}(t + \Delta t)$ is the transient input power, and $P_{load}(t)$ is the load power of a COC VR.

The detailed correlation coefficient derivation of COC VRs can be found in Appendix A.

5.3.3 Validation of the Proposed Correlation Coefficient Models with Practical Parameters

Substitution-box (S-box) is a circuit which is widely used in cryptography to mask the relationship between the secret key and ciphertext [77–79]. Since an S-box can perform a non-linear transformation, for an S-box with m_1 bits of input data, the output data can be m_2 bits that are masked through the non-linear transformations. An S-box with a clock frequency f_c of 200 MHz

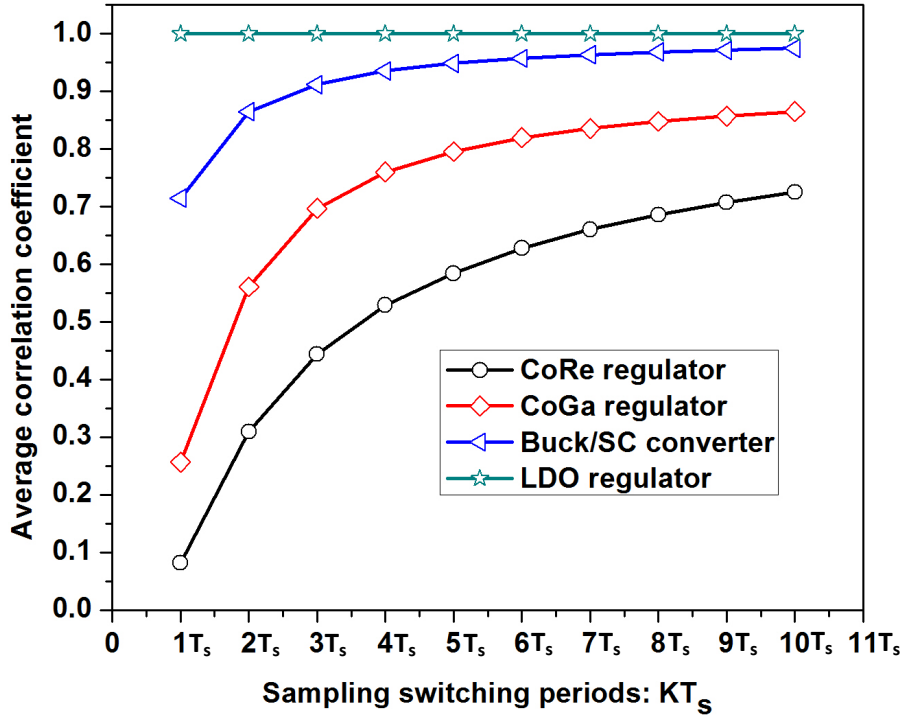


Figure 5.5 Sampling switching periods versus average correlation coefficient.

is designed [80] with 130nm CMOS and simulated in Cadence. The dynamic power dissipation of the S-box $P_d[m]$ conforms to a normal distribution with a mean value μ_s of 264 uW and a standard deviation σ_s of 26.8 uW. The total number of phases N in the CoGa and CoRe regulators is 32. As shown in Fig. 5.4, the correlation coefficient between the input power and load power of CoGa and CoRe regulators is not constant when the phase difference between the switching frequency and data sampling frequency changes. Unlike CoGa, CoRe regulator has a lower correlation coefficient due to the increased randomness with the reshuffling operation.

The relationship between the sampling switching period and average correlation coefficient is shown in Fig. 5.5. The correlation coefficient of an LDO regulator is around 1 due to the negligible time delay between the input power and load power. CoRe regulator exhibits the lowest correlation coefficient among the existing on-chip VRs due to the high randomness obtained with phase reshuffling. When the attacker increases the number of sampling switching periods, the average correlation coefficient of the CoRe regulator increases. The reason is that a certain portion of the noise inserted by the CoRe regulator can be filtered by the attacker by increasing the

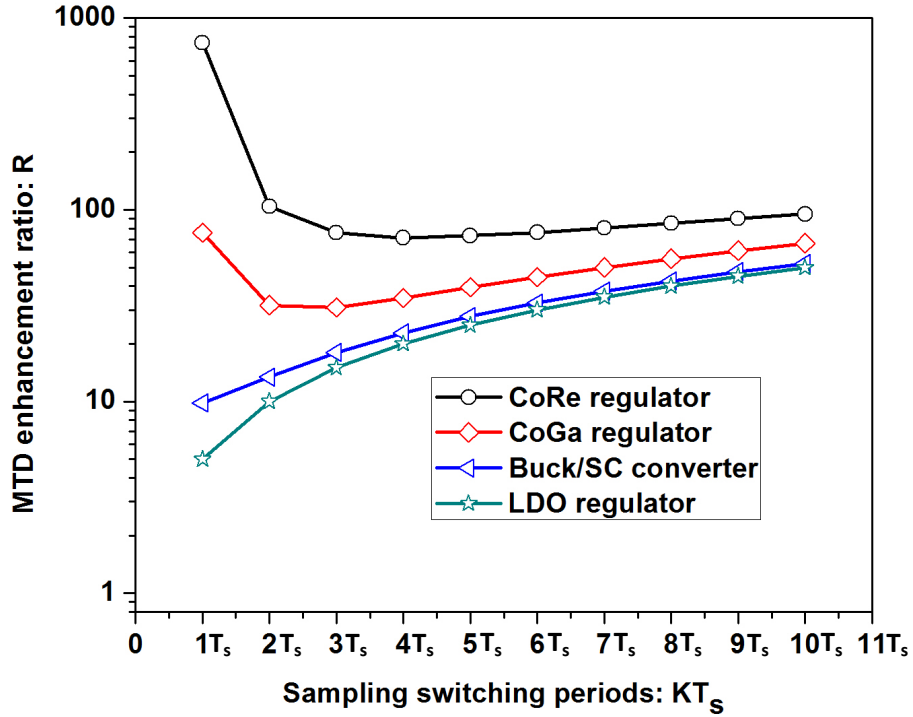


Figure 5.6 Sampling switching periods versus MTD enhancement ratio ($M_1 \approx 5$).

number of switching periods for each sampling. The cost is that more measurements are required for a successful attack, potentially increasing the MTD.

Let's assume that the correlation coefficient between the predicted and actual dynamic power consumption of an S-box is γ_1 and the correlation coefficient between the actual dynamic power consumption of an S-box and input power of an on-chip VR is γ_2 . Since the operations that occur in the S-box are independent of the operations of the on-chip VR, the correlation coefficient between the input data and input power of an on-chip VR γ_3 can be denoted as [75]

$$\gamma_3 = \gamma_1 \times \gamma_2. \quad (5.26)$$

For a single S-box, the relationship between MTD value MTD_0 and correlation coefficient γ_1 is [75]

$$MTD_0 \simeq C/\gamma_1^2. \quad (5.27)$$

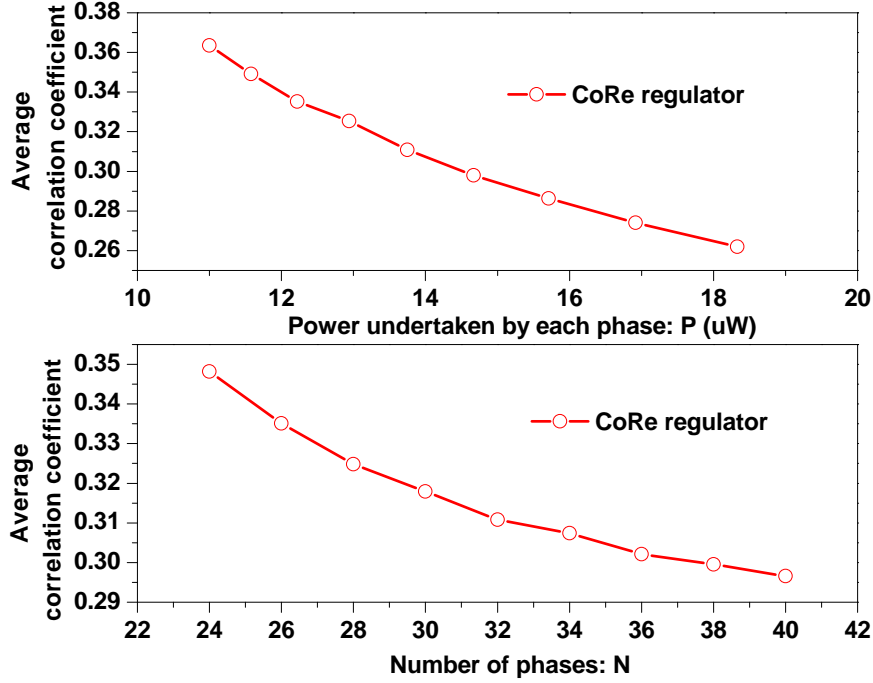


Figure 5.7 Number of phases and power undertaken by each phase versus average correlation coefficient.

where C is the success rate dependent constant [75]. Accordingly, for a single S-box powered by an on-chip VR, the measurement to disclose MTD_1 becomes

$$MTD_1 \simeq \frac{M_1 K}{\gamma_2^2} \times MTD_0 = R \times MTD_0, \quad (5.28)$$

where R is the MTD enhancement ratio of a single S-box powered by an on-chip VR. As compared to an S-box without an on-chip VR, as shown in Fig. 5.6, a single S-box with the CoRe regulator has the highest MTD enhancement ratio. The lowest MTD enhancement ratio of the CoRe regulator with S-box is 71.4 when the attacker optimizes the sampling duration of the attack and selects the total input power within 4 consecutive switching periods as a single sample of the power data.

The average correlation coefficient of the CoRe regulator decreases when the total number of phases N increases, as shown in Fig. 5.7. The reason is that when N increases, more number of gated phases are utilized to increase the randomness of the CoRe regulator. Additionally, if the power P consumed by each phase increases, the average correlation coefficient of the CoRe

regulator reduces due to the larger variance of the random noise caused by the phase reshuffling within every switching cycle.

5.4 Conventional Pipelined (CP) AES Engine with Converter-Reshuffling

In this section, the security concerns of a conventional pipelined AES engine are presented. Additionally, the implications of centralized and distributed on-chip voltage regulations with the CoRe technique on the security of the AES engine are investigated.

5.4.1 Practical Power Attacks on a Pipelined AES Engine without On-Chip Voltage Regulation

For a conventional 128-bit pipelined AES Engine, 16 S-boxes need to be placed in the 1st round encryption block, as shown in Fig. 5.8. If an attacker intends to implement a DPA attack on one of the 16 S-boxes in the 1st encryption round, the attacker can apply a suitable input plaintext combination to simplify the attack. For example, when S-box₁ is being targeted with a DPA attack, the attacker can input a different 8-bit *plaintext*₁ to combine the 8-bit cipher *key*₁ with the input side of S-box₁ sequentially while also maintaining the rest of the input plaintexts (*plaintext*₂, *plaintext*₃, ..., *plaintext*₁₆) as constant. As a result, S-box₁ would exhibit a high dynamic power consumption while the other 15 S-boxes would show a low leakage power dissipation. The leakage power generated by the other 15 S-boxes with a constant input plaintext can be treated as an additive power noise to the S-box₁ that is under attack.

5.4.2 Conventional Pipelined (CP) AES Engine with a Distributed CoRe Technique

Since 16 S-boxes exist in the 1st round encryption block of the CP AES engine, if a distributed CoRe technique is employed, 16 CoRe regulators are needed to power all of the S-boxes, as shown in Fig. 5.9. Let us assume that the total number of phases in the distributed CoRe regulators is N and the number of phases in each distributed CoRe regulator is $N/16$. In this case, the phase

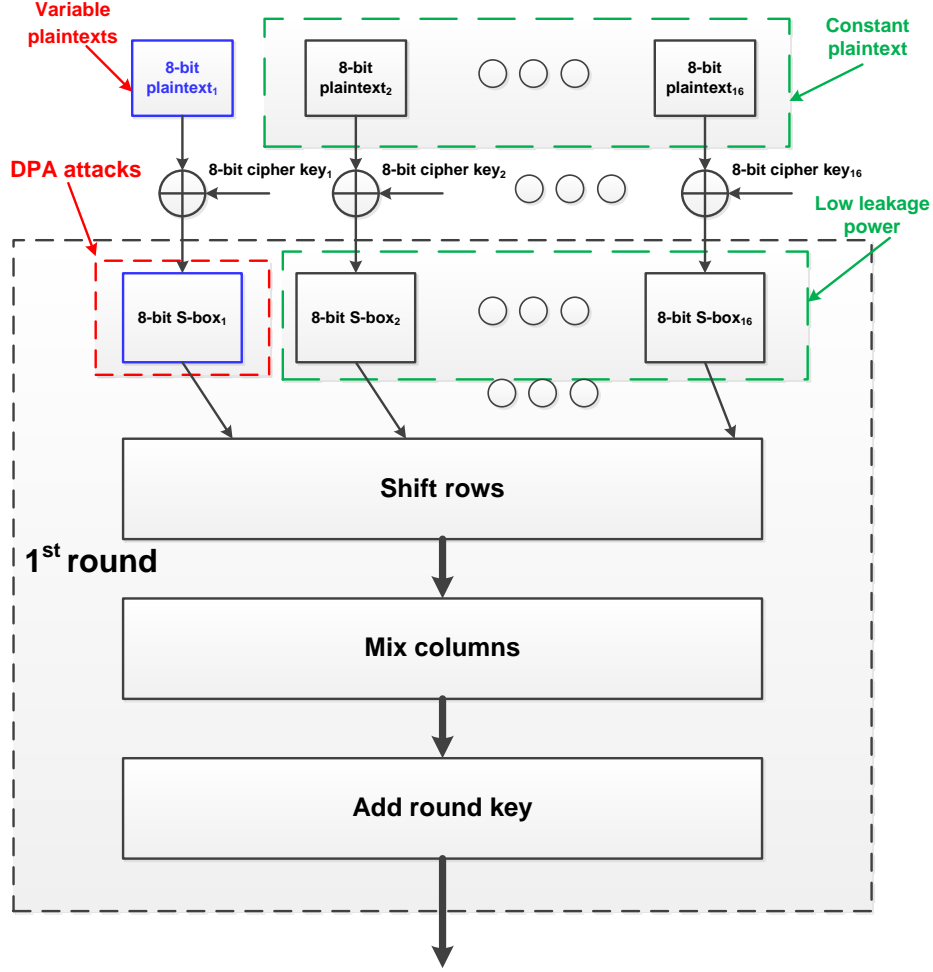


Figure 5.8 1st encryption round of a typical 128-bit pipelined AES engine.

shift $\beta_{y,z}$ in each distributed CoRe regulator can be written as

$$\beta_{y,z} = \frac{2\pi}{N}(y + 16 \times (z - 1)), \quad (5.29)$$

where y represents the y^{th} ($y = 1, 2, \dots, 16$) CoRe regulator and z is the z^{th} ($z = 1, 2, \dots, N/16$) phase in the y^{th} CoRe regulator. The total sampled input power $P_{in,n}^{s,d}(K, \theta)$ of a CP AES engine with 16

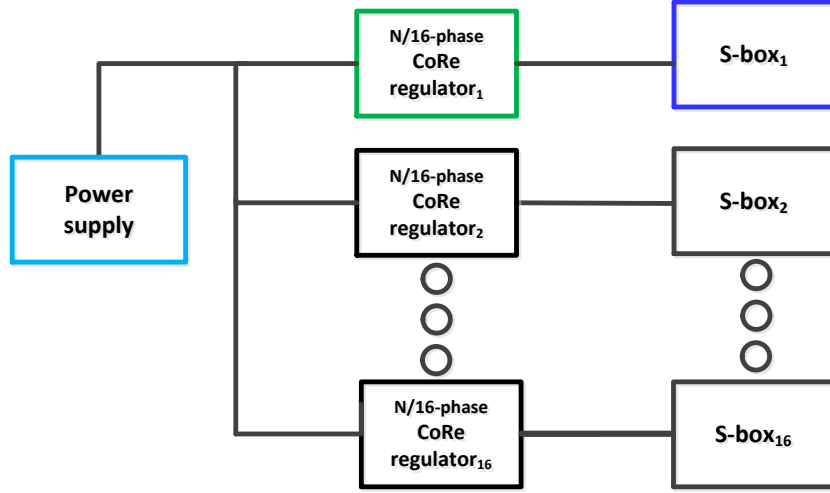


Figure 5.9 A conventional pipelined AES engine with a distributed on-chip CoRe technique.

distributed CoRe regulators within K consecutive switching periods can be expressed as⁶

$$P_{in,n}^{s,d}(K, \theta) = \sum_{y=2}^{16} A_y^d(K, \theta) \left(\frac{P_{leak,y}}{\eta_0} + A_1^d(K, \theta) \left(\frac{(1 - \frac{\theta}{2\pi})j_n P_0 + \frac{\theta}{2\pi}j_{n+K} P_0 + \sum_{u=1}^{K-1} j_{n+u} P_0}{\eta_0} \right) \right), \quad (5.30)$$

where $A_y^d(K, \theta)$ is the y^{th} multiplicative noise inserted by the y^{th} CoRe regulator and $P_{leak,y}$ is the leakage power dissipation of the y^{th} S-box. For a 128-bit CP AES engine with a distributed CoRe architecture, the total number of phases can be utilized to scramble the side-channel power is $16/N$. However, if a centralized CoRe architecture is used to power a CP AES engine, all of the phases can be utilized to scramble the input power consumption. The variance of noise in a CP AES engine with a distributed CoRe architecture may therefore not be high, which can be enhanced by utilizing a centralized CoRe technique in the following section.

5.4.3 Conventional Pipelined (CP) AES Engine with a Centralized CoRe Technique

When all of the 16 S-boxes use a centralized on-chip VR, as shown in Fig. 5.10, a common on-chip CoRe regulator is utilized to deliver power to all S-boxes. In this case, the total sampled

⁶Assuming S-box₁ is under DPA attacks.

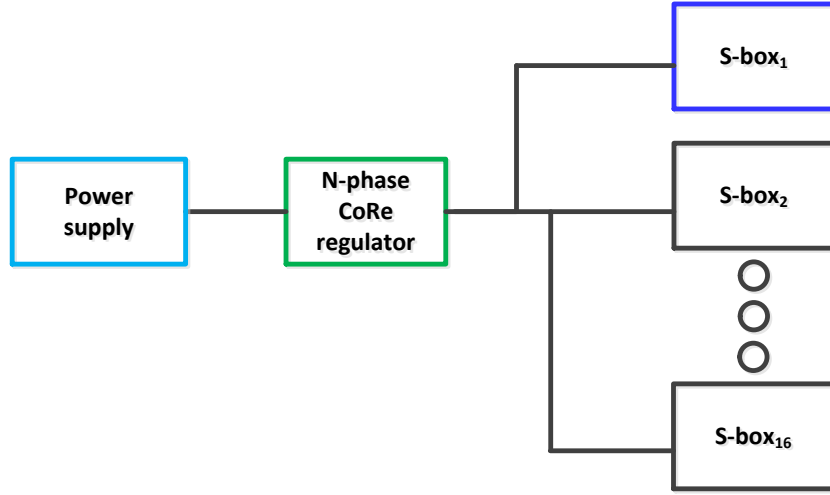


Figure 5.10 A conventional pipelined AES engine with a centralized on-chip CoRe technique.

input power $P_{in,n}^{s,c}(K, \theta)$ within K consecutive switching cycles can be denoted as

$$P_{in,n}^{s,c}(K, \theta) = A^c(K, \theta) \left(\frac{(1 - \frac{\theta}{2\pi})j_n P_0 + \frac{\theta}{2\pi} j_{n+K} P_0}{\eta_0} + \frac{\sum_{u=1}^{K-1} j_{n+u} P_0 + P_{leak}}{\eta_0} \right), \quad (5.31)$$

where $A^c(K, \theta)$ is the multiplicative noise generated by randomly reshuffling the active and gated phases in a CP AES engine with a centralized CoRe regulator. P_{leak} is the total leakage power generated by the 15 S-boxes with constant input plaintext where $\sum_{y=2}^{16} P_{leak,y} = P_{leak}$.

Assuming that the correlation coefficient of a centralized CoRe regulator within a CP AES engine is γ_0 , the signal-to-noise ratio (SNR) of the centralized CoRe regulator within a CP AES engine SNR_0 is [75]

$$SNR_0 = \frac{\sigma_f^2}{\sigma_q^2} = \frac{1}{\frac{1}{\gamma_0^2} - 1}, \quad (5.32)$$

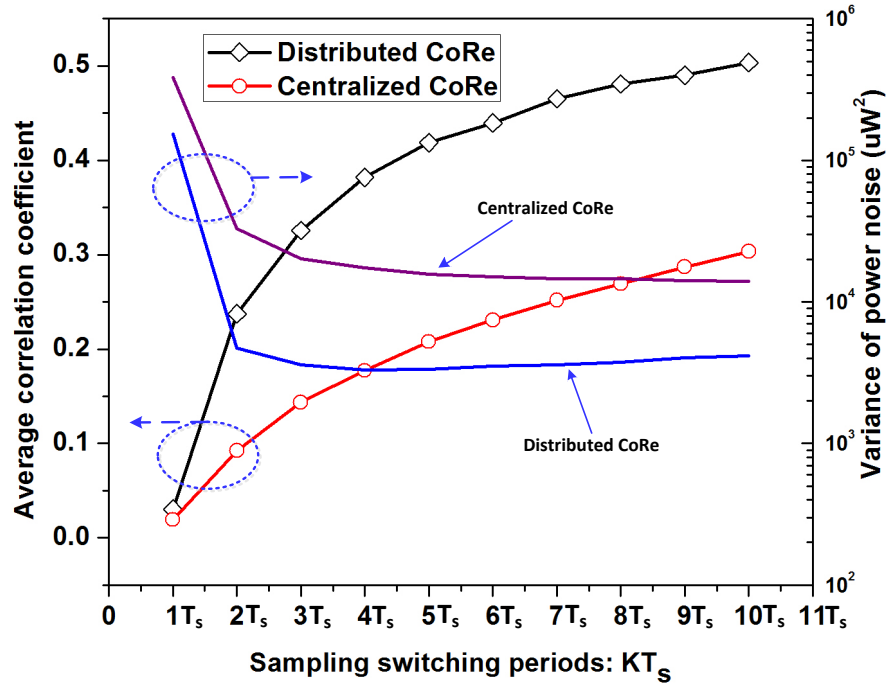


Figure 5.11 Sampling switching periods versus average correlation coefficient and variance of power noise of the distributed and centralized CoRe architectures.

where σ_f^2 and σ_q^2 are, respectively, the variance of the signal and noise. Accordingly, the variance of the noise of the centralized CoRe regulator within a CP AES engine can be denoted as

$$\sigma_q^2 = \left(\frac{1}{\gamma_0^2} - 1\right)\sigma_f^2. \quad (5.33)$$

As shown in Fig. 5.11, the average correlation coefficient of a centralized CoRe technique is lower than the average correlation coefficient of a distributed CoRe technique. The reason is that an increased number of gated phases are utilized during the reshuffling operation. As a result, the variance of the power noise inserted by the phase reshuffling operation in every switching cycle in a centralized CoRe architecture is enhanced significantly as compared to the total variance of power noise in a distributed CoRe architecture. As shown in Fig. 5.12, the minimum MTD enhancement ratio of a CP AES engine with a centralized CoRe architecture is around 544 when the attacker samples 10 consecutive switching cycles. Alternatively, the minimum MTD enhancement ratio of a CP AES engine with a distributed CoRe architecture is about 137.1 when the attacker samples 4

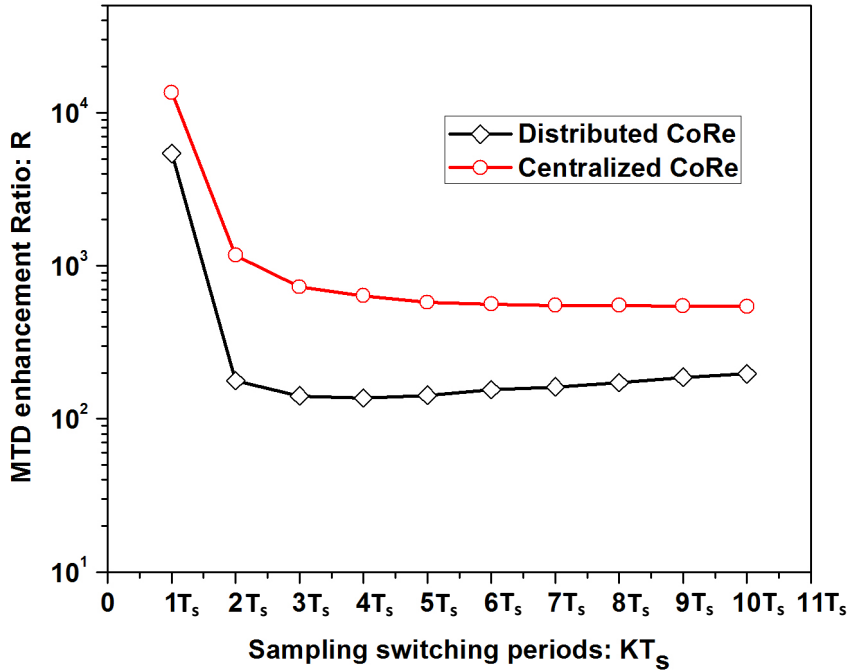


Figure 5.12 Sampling switching periods versus MTD enhancement ratios of the distributed and centralized CoRe architectures ($M_1 \approx 5$).

consecutive switching cycles. After adopting the centralized CoRe technique, the minimum MTD enhancement ratio is also significantly increased.

5.5 Improved Pipelined (IP) AES Engine with Centralized CoRe Technique

In a CP AES engine, the S-boxes which are fed with a constant input plaintext would generate a low leakage power dissipation. If those S-boxes that are not under attack can exhibit a high dynamic power dissipation all the time even when constant input plaintext is applied, this high dynamic power dissipation may act as a power noise to scramble the dynamic power generated by the S-box under attack.

An improved pipelined (IP) AES engine is proposed to ensure that all of the S-boxes have high dynamic power dissipation at all times. As shown in Fig. 5.13, 16 invert boxes (the internal logic circuits of each invert box are shown in Fig. 5.14) are inserted at the inputs of the S-boxes. After the 11th round of CP AES engine, a mask removal operation is performed, sim-

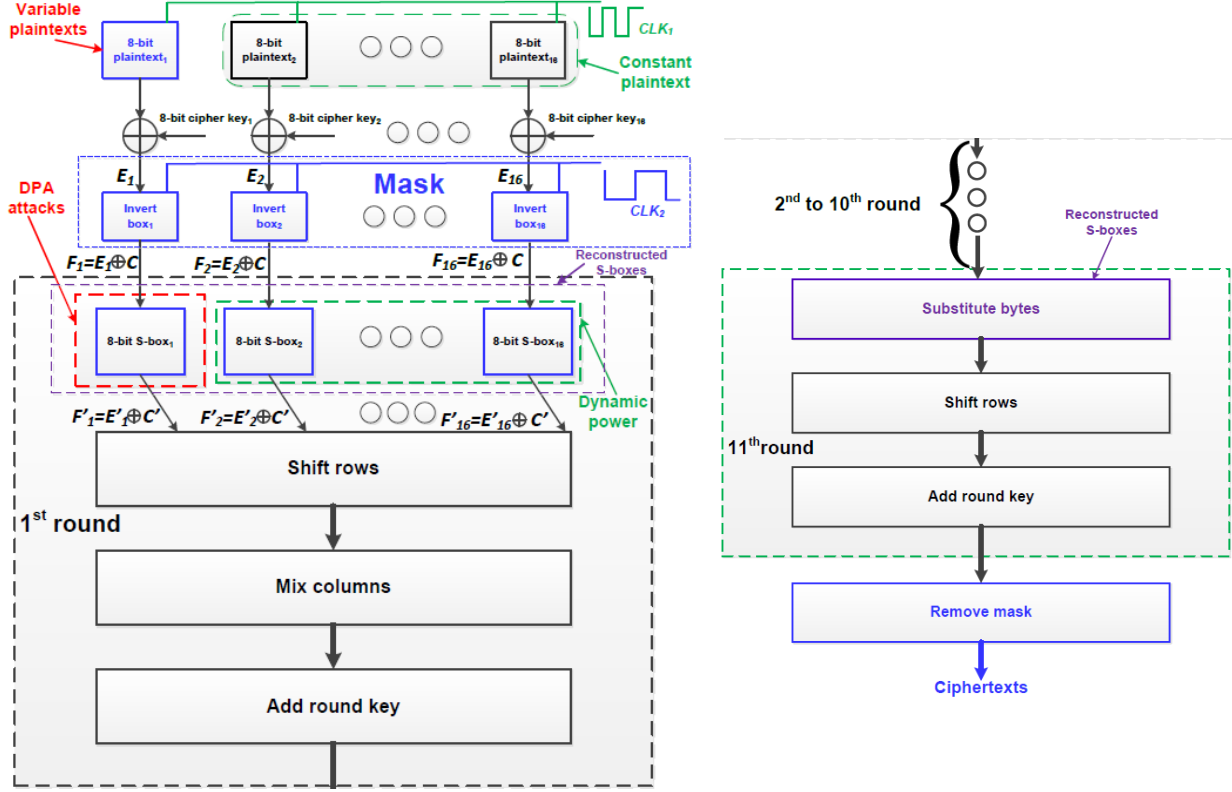


Figure 5.13 Full encryption rounds of an 128-bit improved pipelined (IP) AES engine, please note that invert boxes are added before the 1st round and the mask removal operation is performed after the 11th round (the architecture of the reconstructed S-box can be founded in [5, 6]).

ilar to [5]. CLK_1 is the clock signal for controlling the frequency of the input plaintext (CLK_1 also represents the clock frequency f_c as mentioned before). CLK_2 is the clock signal to control the frequency of the invert operations in each invert box. When the frequency of CLK_1 f_c is two times of the frequency of CLK_2 f_I , ($f_c = 2f_I$), the input data of each S-box can be inverted with a frequency of f_c if constant input plaintext is enabled. As shown in Fig. 5.14, if $E_y = (10010100)_2, (10010100)_2, \dots$, after adding the corresponding invert box, the output data of invert box becomes $F_y = (10010100)_2, (01101011)_2, (10010100)_2, (01101011)_2, \dots$. All of the S-boxes can therefore exhibit a high dynamic power consumption even if a constant input plaintext is applied by the attacker.

For the IP AES engine with constant input plaintext, if the output data of the y^{th} invert box is $F_y = (f_{y,1}, f_{y,2}, \dots, f_{y,8})_2$, and F_y makes a transition from $(f_{y,1}, f_{y,2}, \dots, f_{y,8})_2$ to $(\overline{f_{y,1}}, \overline{f_{y,2}}, \dots, \overline{f_{y,8}})_2$,

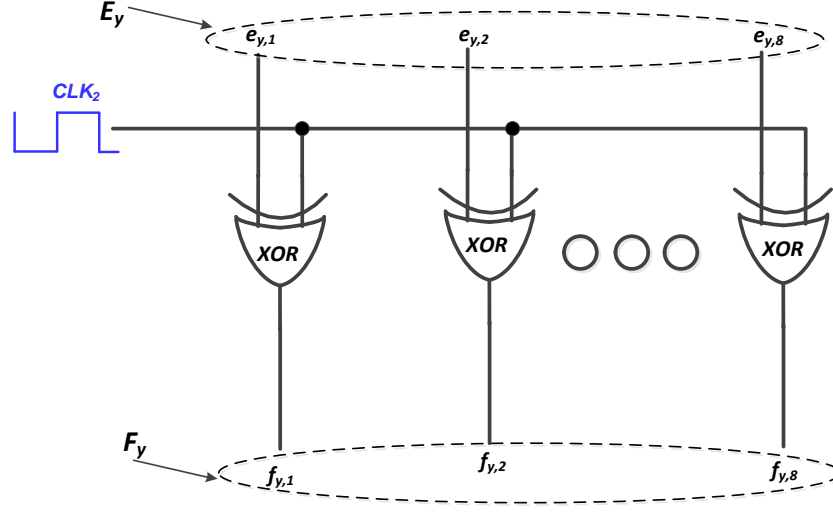


Figure 5.14 Internal logic circuits of the y^{th} invert box.

the dynamic power consumption of the y^{th} S-box is $P_{d,y,1}$. When F_y makes a transition from $(\overline{f_{y,1}}, \overline{f_{y,2}}, \dots, \overline{f_{y,8}})_2$ to $(f_{y,1}, f_{y,2}, \dots, f_{y,8})_2$, the dynamic power consumption of the y^{th} S-box is $P_{d,y,2}$. The total dynamic power dissipation $\overline{P_{d,y}}$ of the y^{th} S-box within a switching period can be denoted as

$$\overline{P_{d,y}} = \frac{M_1 \times (P_{d,y,1} + P_{d,y,2})}{2}. \quad (5.34)$$

The mean value $\mu_{I,y}$ and variance $\sigma_{I,y}^2$ of the dynamic power dissipation of the y^{th} S-box within a switching period respectively, are

$$\mu_{I,y} = \frac{(\mu_s + \mu_s) \times \frac{M_1}{2}}{M_1} = \mu_s, \quad (5.35)$$

$$\sigma_{I,y}^2 = \frac{(\sigma_s^2 + \sigma_s^2) \times (\frac{M_1}{2})^2}{M_1^2} = \frac{\sigma_s^2}{2}. \quad (5.36)$$

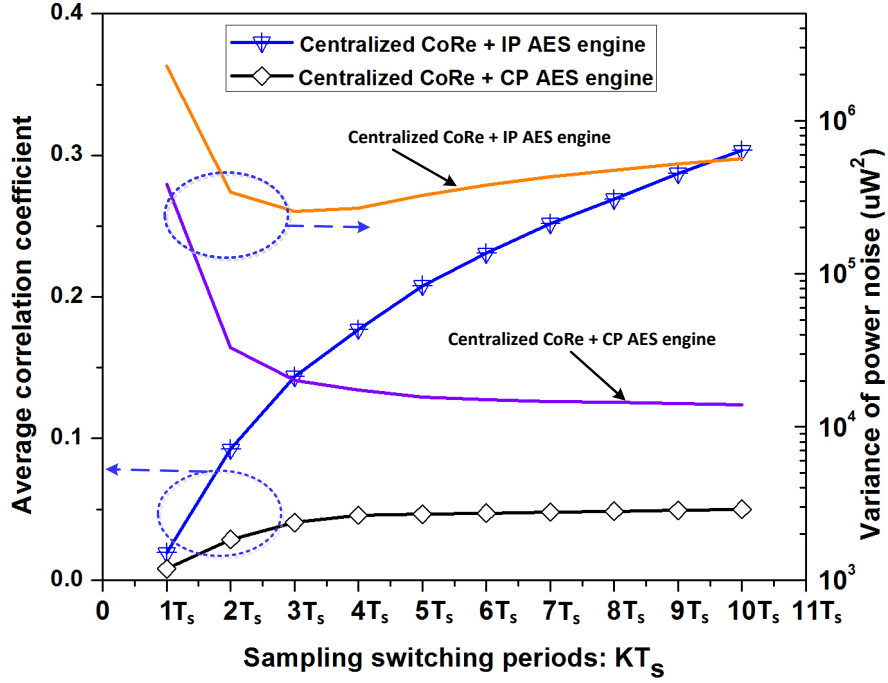


Figure 5.15 Sampling switching periods versus average correlation coefficient and variance of power noise of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator.

Accordingly, the mean value μ_I and variance σ_I^2 of the total dynamic power consumption generated by the other 15 S-boxes with constant input plaintext within a switching period become

$$\mu_I = 15\mu_s, \quad (5.37)$$

$$\sigma_I^2 = 15 \times \frac{\sigma_s^2}{2} = 7.5\sigma_s^2. \quad (5.38)$$

If a centralized CoRe regulator is utilized to deliver power to an IP AES engine, the total sampled input power within K consecutive switching periods $P_{in,n}^{s,I,c}(K, \theta)$ can be obtained as⁷

$$P_{in,n}^{s,I,c}(K, \theta) = A^{I,c}(K, \theta) \left(\frac{\sum_{y=2}^{16} \overline{P_{d,y}}}{\eta_0} \right) + A^{I,c}(K, \theta) \left(\frac{(1 - \frac{\theta}{2\pi})j_n P_0 + \frac{\theta}{2\pi} j_{n+K} P_0 + \sum_{u=1}^{K-1} j_{n+u} P_0}{\eta_0} \right), \quad (5.39)$$

⁷Assuming S-box₁ is under DPA attacks.

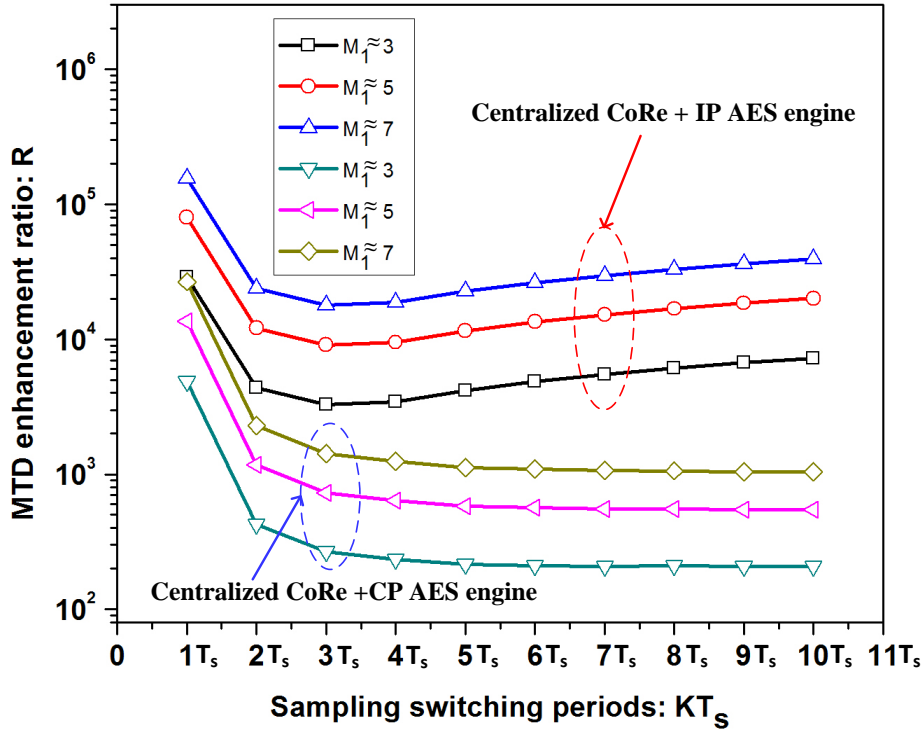


Figure 5.16 Sampling switching periods versus MTD enhancement ratio of the CP AES engine with a centralized CoRe regulator and the IP AES engine with a centralized CoRe regulator ($M_1 \approx 3, 5$, and 7).

where $A^{I,c}(K, \theta)$ is the multiplicative noise. The total dynamic power consumption within a switching period induced by the 15 S-boxes with constant input plaintext is $\sum_{y=2}^{16} \overline{P_{d,y}} \sim N(15\mu_s, 7.5\sigma_s^2)$. With phase reshuffling operation, the multiplicative noise $A^{I,c}(K, \theta)$ would convert the high dynamic power $\sum_{y=2}^{16} \overline{P_{d,y}}$ into a large additive power noise in the input power profile. As a result, the large additive noise $A^{I,c}(K, \theta)(\sum_{y=2}^{16} \overline{P_{d,y}}/\eta_0)$ can successfully scramble the correlation between the input power and side-channel power in an IP AES engine with a centralized CoRe regulator.

As shown in Fig. 5.15, as compared to the CP AES engine with a centralized CoRe regulator, the IP AES engine with a centralized CoRe regulator has lower correlation coefficient due to the larger variance of the power noise in the IP AES engine with a centralized CoRe regulator. The large power noise arises from the high dynamic power consumption caused by the 15 S-boxes with constant input plaintext. In Fig. 5.16, the lowest MTD enhancement ratio of the IP AES engine with a centralized CoRe regulator is 9,100 when $M_1 \approx 5$ (if $M_1 \approx 3, 7$, the lowest MTD enhancement

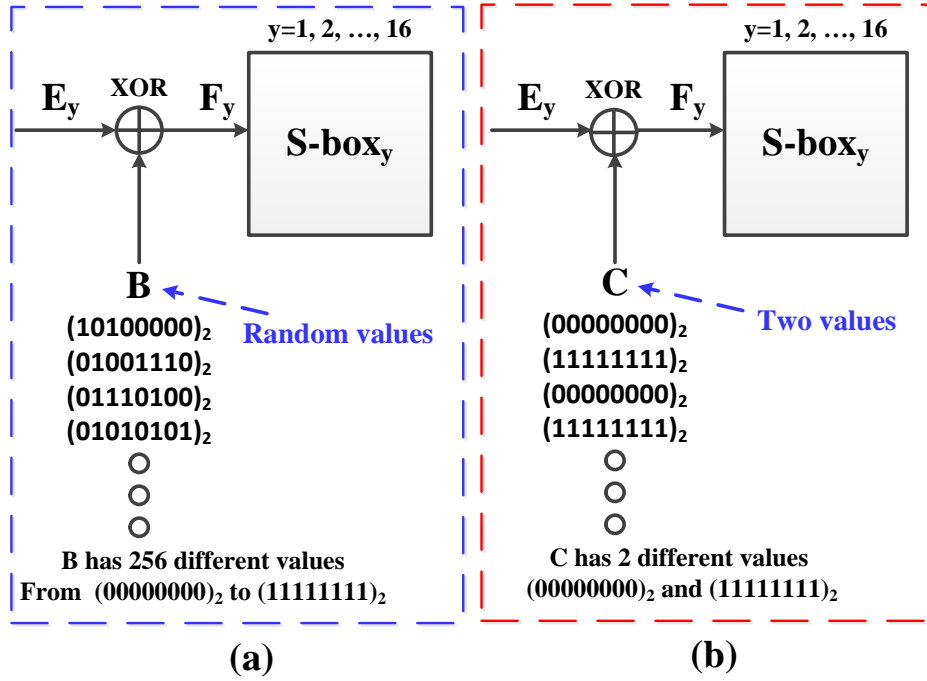


Figure 5.17 (a) Masking operation in conventional masked AES engine and (b) Masking operation in the IP AES engine that we proposed.

ratios are 3290, 17850, respectively) when the attacker samples 3 consecutive switching cycles as one sample of the power data. This value is about 15.7 times higher than the minimum MTD enhancement ratio of the CP AES engine with a centralized CoRe regulator.

The power overhead of the proposed IP AES engine can be justified as follows. When a CP AES engine is working during regular operation (not under attack), all of the 16 S-boxes would show high dynamic power consumption due to the variable input plaintexts. Henceforth, adding invert boxes in the IP AES engine would actually not bring extra power overhead to the S-boxes. The proposed IP AES engine can be considered as a voltage regulator-assisted masked AES engine, which can recover the correct output data by using the same way as a conventional masked AES engine. For the conventional masked AES engine, as shown in Fig. 5.17(a), the masking random data B is added at the beginning of encryption. The corresponding masking component would be removed at the end of encryption [5, 6]. For the conventional masked AES engine, the input data of S-box $F_y = E_y \oplus B$. However, for the IP AES engine, the input data of S-box is $F_y = E_y \oplus C$ where the masking data C is also added at the beginning of encryption and the corresponding masking

component can be removed at the end of encryption by using the same way as the conventional masked AES engine, as shown in Fig. 5.13 and Fig. 5.17(b).

The primary difference between the conventional masked AES engine and IP AES engine we proposed is the masking data. For the conventional AES engine, the masking data B is an 8-bit random value, so B can have $2^8 = 256$ different values. 256 masking values would increase the size of look-up table (LUT) and computational complexity of the AES engine significantly [6]. As a result, the area and performance overhead of the conventional masked AES engine is quite large [6]. For an implemented masked AES engine based on field-programmable gate array (FPGA) [81], the area overhead is 60.1% and the frequency decreases about 11% [81].

However, for the proposed IP AES engine, the masking data C can only have two values: $(00000000)_2$ and $(11111111)_2$ ($E_y \oplus (00000000)_2 = E_y$ and $E_y \oplus (11111111)_2 = \overline{E_y}$). As compared to the conventional masked AES engine, the overhead of IP AES engine would therefore be reduced to $2/256 = 1/128$. The approximate area overhead of the proposed IP AES engine would be around $60.1\% * (1/128) = 0.47\%$ and the frequency reduction of the IP AES engine would be around $11\% * (1/128) = 0.09\%$.

5.6 Circuit Level Simulation

The CoGa and CoRe techniques are designed with 130nm IBM CMOS technology and simulated in Cadence where the switching frequency is swept between 30 and 60 MHz. As shown in Fig. 5.18, when the load current I_{load} is constant, the CoGa regulator is not triggered, and the active and gated phases do not change as long as the variations in the load current demand are small. However, the sequence of active and passive stages continuously alters over time in the CoRe regulator regardless of the variations in the workload demand. Therefore, as compared to CoGa, input power consumption of the CoRe regulator shows an uncertain sequence of active stages even if the load current demand does not change, increasing the variance of multiplicative power noise in input power profile.

As shown in Fig. 5.19(a), the dynamic power consumption of an IP AES engine is much higher than the dynamic power consumption of a CP AES engine. The reason is that all 16 S-

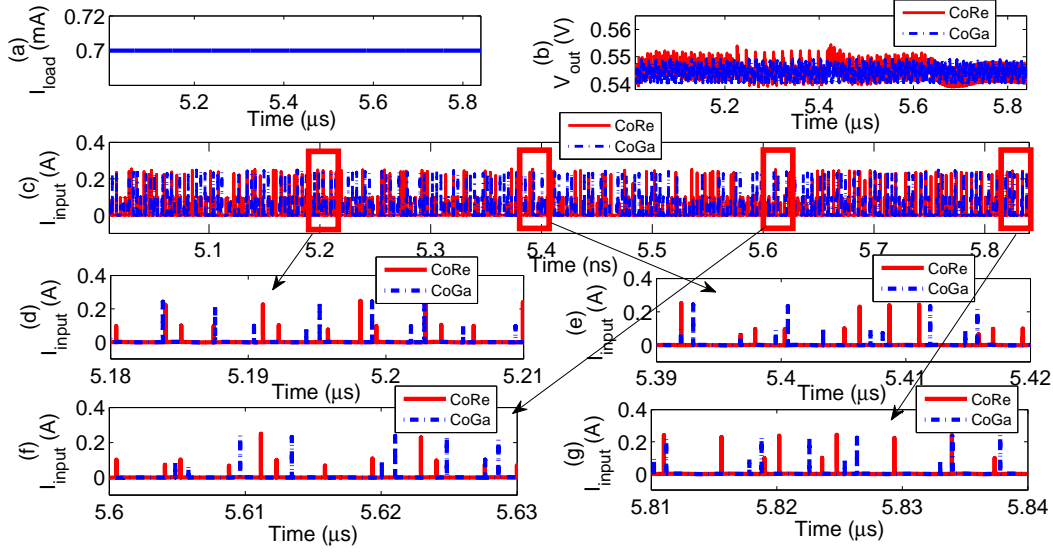
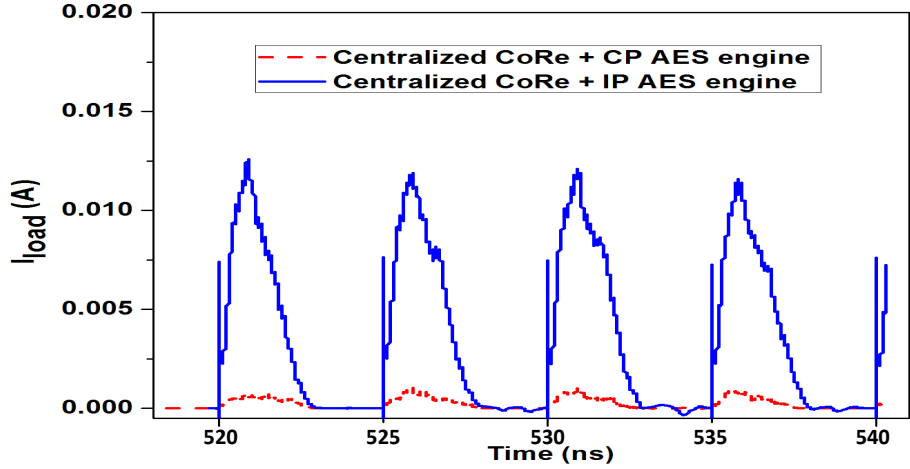


Figure 5.18 8-phase CoGa regulator and 8-phase CoRe regulator are simulated: a) Distribution of load current, b) transient output voltage profile, and c) input current profile of CoGa regulator and CoRe regulator, sequence of active stages in CoRe regulator is variable while sequence of active stages in CoGa regulator is invariable if a constant load current is enabled, as shown in d), e), f), and g).

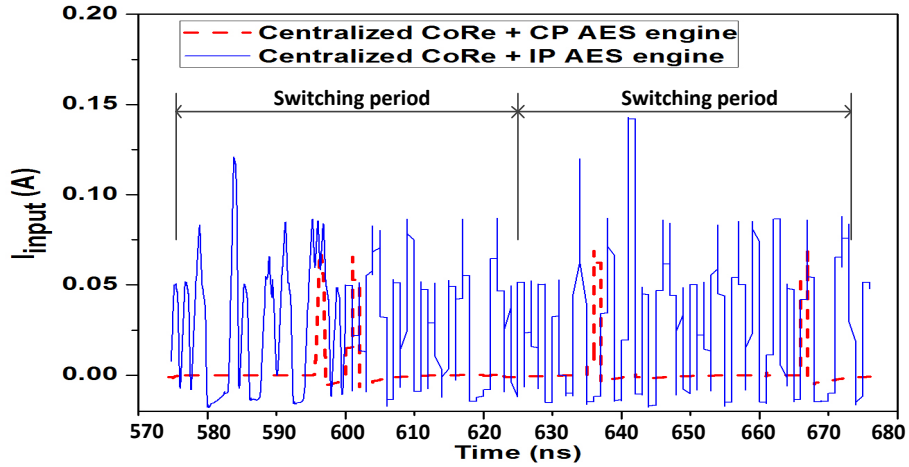
boxes have high dynamic power dissipation in an IP AES engine while only the S-box under attack contributes to the dynamic power dissipation in a CP AES engine. As shown in Fig. 5.19(b), only 2 stages are activated in the CP AES engine with a centralized CoRe regulator in a switching cycle while a greater number of stages are turned-on in the centralized CoRe regulator. Hence, the power noise generated by those 15 S-boxes which are not under attack are reshuffled in the input power profile, further reducing the correlation between the input power and side-channel power in the IP AES engine with a centralized CoRe regulator.

5.7 Conclusion

An on-chip CoRe technique is utilized to reinforce a lightweight AES engine as an efficient countermeasure against power analysis attacks due to the high multiplicative power noise induced by reshuffling active and gated converter stages. A detailed analytical analysis of the correlation between the input and output power of both conventional and proposed voltage regulation techniques is presented. The security implications of the physical placement of the voltage regulators



(a)



(b)

Figure 5.19 (a) Load current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator, (b) Input current profile of a CP AES engine with a centralized CoRe regulator and an IP AES engine with a centralized CoRe regulator (The total number of phases of the centralized CoRe regulator is 64).

are investigated with centralized and distributed implementations of the CoRe regulators. An improved AES engine is proposed to further scramble the input power even when the attacker applies a constant plaintext to the S-boxes that are not under attack. The security implications of the proposed techniques are analytically proven using the correlation coefficient. When a centralized CoRe regulator is combined with the proposed improved pipelined AES engine, the MTD value is enhanced over 9,100 times as compared to an unprotected AES engine.

CHAPTER 6: SECURITY-ADAPTIVE VOLTAGE CONVERSION TECHNIQUE

6.1 Introduction

DPA attacks are one of the most widely studied SCAs that exploit the switching activities within the cryptographic circuits while processing different input data¹. Recently leakage power analysis (LPA) attacks have been proposed by M. Alioto *et al.* [3] to obtain the critical information by analyzing the correlation between the input data and leakage power dissipation of the cryptographic circuit. LPA attacks exploit the fact that the leakage current signature of NMOS and PMOS transistors is different [3]. The amplitude of the leakage power is orders of magnitude smaller than the amplitude of dynamic power consumption. To perform a successful LPA attack, the attacker must mitigate the measurement noise that can make the analysis quite difficult due to the small signal-to-noise ratio (SNR) of the monitored leakage power. An effective technique to mitigate the measurement noise is to lower the operating frequency of the cryptographic circuit [83].

Since the leakage mechanisms in DPA and LPA attacks are quite different, DPA-resistant cryptographic circuits may still be vulnerable against LPA attacks [84]. There is therefore a strong need for effective countermeasures against LPA attacks. Converter-reshuffling (CoRe) technique has been proposed in [11, 59] as a countermeasure against DPA attacks with low overhead. CoRe technique utilizes a multi-phase switched-capacitor (SC) voltage converter where each phase delivers a portion of the required power to the cryptographic circuit with a different time delay. A pseudo-random number generator (PRNG) is used to scramble the sequence of activate phases to insert a varying amount of uncertain power noise in each switching period against DPA attacks. However, if the attacker implements an LPA attack on a cryptographic circuit with a CoRe voltage converter,

¹The content of this Chapter has been published in [82], the copyright permission can be found in Appendix F.

the low leakage power dissipation generated by the cryptographic circuit would only activate a small number of converter phases. The small number of active phases would significantly reduce the entropy of the PRNG in the CoRe voltage converter, making the CoRe technique also vulnerable against LPA attacks.

To increase security against LPA attacks with negligible overhead, in this Chapter, the voltage regulator is designed in a security-adaptive fashion. The security-adaptive (SA) voltage converter is designed based on the CoRe voltage converter [11, 59] but modified to sense LPA attacks and insert noise through a discharging resistor only when the device is under an LPA attack. When the SA voltage converter is utilized as the supply voltage of the cryptographic circuit, during the normal² and idle³ modes of operation, no redundant current is being consumed and the SA voltage converter operates conventionally as the CoRe voltage converter. The SA voltage converter is triggered to provide redundant current when the operating clock frequency f_c is within a certain range which is explained in detail in Section 6.2. The activity of the discharging resistor is then reshuffled by the PRNG to scramble the inserted noise profile. Since the proposed SA converter operates conventionally and is only triggered to sink redundant current when the device is under an LPA attack, the power overhead of this countermeasure is negligible.

6.2 Architecture Design

The proposed SA voltage converter consists of a CoRe voltage converter, two clock frequency sensors, and a discharging resistor as shown in Fig. 6.1. When the cryptographic circuit is in a normal working mode, the cryptographic circuit exhibits a high dynamic power consumption (*i.e.*, the clock frequency f_c is high), M_1 transistor would be in off-state to let the SA voltage converter operate similar to the CoRe voltage converter. Under an LPA attack, however, the attacker would lower the clock frequency f_c to mitigate the measurement noise [83]. If the clock frequency f_c is lower than the active critical frequency F_{ac} and higher than the idle critical frequency F_{ic} , both

²In a normal working mode, clock frequency f_c of the cryptographic circuit is high, therefore, power consumption is high.

³In the idle mode, the clock frequency f_c of the cryptographic circuit is quite low, therefore, overall power consumption is low.

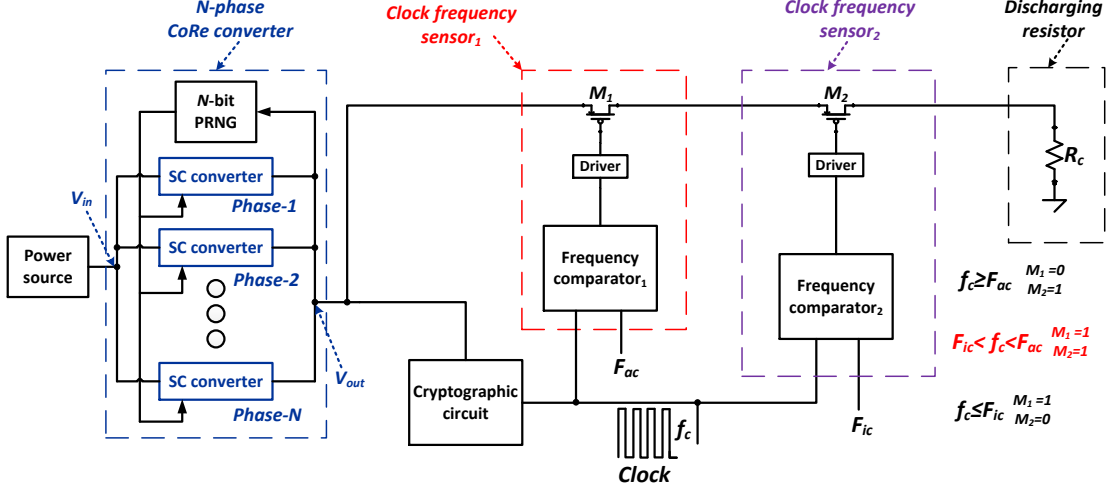


Figure 6.1 Architecture of the proposed security-adaptive (SA) voltage converter (N is the total number of phases (N is an even), switch $M_{i_1} = 1$, ($i_1 = 1, 2$) represents that it is in on-state and *vice versa*).

M_1 transistor and M_2 transistor would be in on-state, letting some amount of redundant current flow through the discharging resistor R_c . The redundant power dissipation induced by R_c is then reshuffled by the N -phase CoRe converter to scramble the inserted power noise.

When the clock frequency f_c of the cryptographic circuit is lower than the idle critical frequency F_{ic} , the M_2 transistor would be turned-off, deactivating the discharging resistor R_c as shown in Fig. 6.1. When the cryptographic circuit is in an idle mode ($f_c \ll F_{ic}$), the discharging resistor R_c is therefore inactive to avoid power overhead. The design guidelines on the selection of suitable F_{ic} and F_{ac} to maximize security are provided in Section 6.4 and Appendix B, respectively.

6.3 Parameter Design

To maximize the entropy of the N -bit PRNG that resides within the SA voltage converter, the number of active phases of an SA voltage converter in each switching period should be around $N/2$ (the entropy of the N -bit PRNG reaches the maximum value $-\binom{N}{N/2} \times \frac{1}{\binom{N}{N/2}} \log_2 \binom{N}{N/2} = \log_2 \binom{N}{N/2}$). Let's assume the mean value of leakage power dissipation of the cryptographic circuit within a switching period under LPA attacks is μ_c and the output voltage of an N -phase CoRe converter within the SA voltage converter is V_{out} . When the cryptographic circuit employs an SA

voltage converter, if the discharging resistor R_c is activated, the power dissipation P_c consumed by the discharging resistor R_c can be denoted as $P_c = V_{out}^2/R_c$. The mean value μ_t of the total load power dissipation of the SA voltage converter within a switching period can be approximated as

$$\mu_t \approx \mu_c + \frac{V_{out}^2}{R_c}. \quad (6.1)$$

The output current I_{out} delivered by a single SC converter phase is [52]

$$I_{out} = 2C_f(V_{in} - 2V_{out})kf_s, \quad (6.2)$$

where C_f is the flying capacitance within each phase, V_{in} is the input voltage from the power source, f_s is the switching frequency of the SC converter, and k is the f_s and C_f dependent parameter which can be found in [52].

Since around half of the total phases should be active in each switching period to maximize the entropy of the N -bit PRNG, the following approximated equation should be satisfied

$$V_{out} \times \frac{N}{2} \times I_{out} \approx \mu_c + \frac{V_{out}^2}{R'_c}, \quad (6.3)$$

where R'_c is the optimized resistance value of the discharging resistor R_c that maximizes the security of the cryptographic circuit. R'_c therefore, can be determined as

$$R'_c \approx \frac{V_{out}^2}{V_{out}NC_f(V_{in} - 2V_{out})kf_s - \mu_c}. \quad (6.4)$$

6.4 Security Evaluation Against LPA Attacks

To quantify the security of a cryptographic circuit that employs the proposed SA voltage converter against LPA attacks, the correlation coefficient between the input and load power profiles of the SA voltage converter needs to be modeled. The correlation coefficient γ of a voltage converter

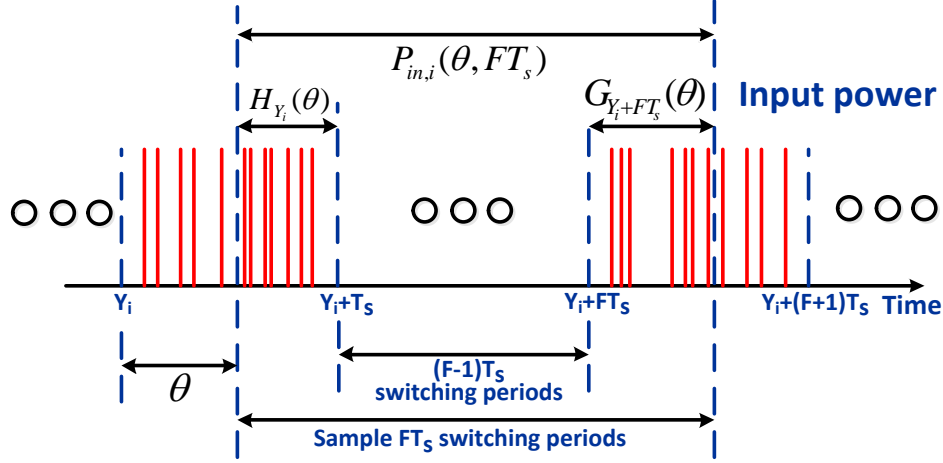


Figure 6.2 Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a single clock period as one sample of input power data (T_s is the switching period of the SA voltage converter, Y_i is the starting time point of the 1st switching period for sampling the i^{th} input power data, and θ is the phase difference between the switching period and input power data sampling).

is

$$\gamma = \frac{\sum_{i=1}^n (P_{l,i} - \overline{P_l})(P_{in,i} - \overline{P_{in}})}{\sqrt{\sum_{i=1}^n (P_{l,i} - \overline{P_l})^2 \sum_{i=1}^n (P_{in,i} - \overline{P_{in}})^2}}, \quad (6.5)$$

where n is the total number of the input or load power data samples, $P_{l,i}$ ($P_{in,i}$) is the i^{th} , ($i = 1, 2, \dots, n$) load (input) power of the voltage converter, and $\overline{P_l}$ ($\overline{P_{in}}$) is the corresponding total average load (input) power.

6.4.1 Sampling a Single Clock Period as One Sample of Input Power Data

In LPA attacks, in order to filter the measurement noise, the clock frequency f_c of the cryptographic circuit needs to be sufficiently reduced [83] (*i.e.*, $f_c \approx \frac{1}{F_0} f_s$ where F_0 is an integer that can reasonably filter out the measurement noise). However, when a cryptographic circuit implemented with a CoRe or an SA voltage converter is under LPA attacks, in addition to filtering the measurement noise, the reshuffling noise induced by PRNG can also be filtered if the clock frequency f_c is further reduced. For example, the clock frequency f_c can be further reduced to $f_c \approx \frac{1}{F} f_s$ (F is an integer and $F > F_0$) to also filter the reshuffling noise.

If the attacker selects a single clock period (F number of switching periods) as one sample of the input power data as shown in Fig. 6.2, the sampled input power $P_{in,i}(\theta, FT_s)$ is

$$P_{in,i}(\theta, FT_s) = (H_{Y_i}(\theta) + G_{Y_i+FT_s}(\theta))P_0 + \frac{(F-1)(P_i + \frac{V_{out}^2}{R_c})}{\eta_c}, \quad (6.6)$$

where η_c is the power efficiency of the N -phase CoRe converter in the SA voltage converter, P_0 is the power consumed by a single active phase in the SA voltage converter, and P_i is the leakage power dissipation of the cryptographic circuit induced by the i^{th} input data. $H_{Y_i}(\theta)$ and $G_{Y_i+FT_s}(\theta)$ are the corresponding number of active phases, as illustrated in Fig. 6.2. The corresponding load power $P_{l,i}(\theta, FT_s)$ of the SA voltage converter (which is correlated with $P_{in,i}(\theta, FT_s)$) can be written as

$$P_{l,i}(\theta, FT_s) = (1 - \frac{\theta}{2\pi})P_i + (F-1)P_i + \frac{\theta}{2\pi}P_i = FP_i. \quad (6.7)$$

As compared to a conventional cryptographic circuit (*i.e.*, without any countermeasure), the MTD enhancement ratio $R(FT_s)$ of a cryptographic circuit that employs a voltage converter is [59]

$$R(FT_s) \propto \frac{1}{(\frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta, FT_s) d\theta)^2}, \quad (6.8)$$

where $\frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta, FT_s) d\theta$ is the average correlation coefficient between the input and output power profiles of the voltage converter.

As compared to an LPA attack on a conventional cryptographic circuit with clock frequency $f_c \approx \frac{1}{F_0} f_s$, the MTD value would be enhanced by F/F_0 times if the attacker implements an LPA attack on a cryptographic circuit which employs a voltage converter with a slower clock frequency $f_c \approx \frac{1}{F} f_s$. As a result, the MTD enhancement ratio $R_1(FT_s)$ of a cryptographic circuit that employs

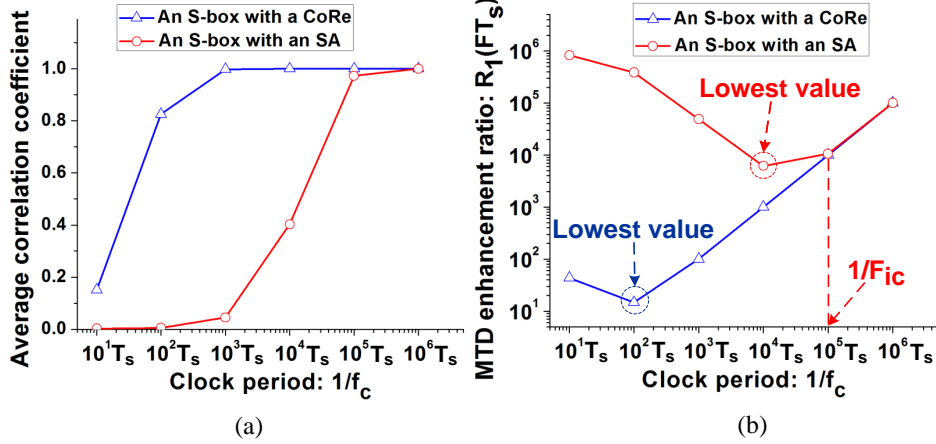


Figure 6.3 (a) Average correlation coefficient versus clock period $1/f_c$ and (b) MTD enhancement ratio $R_1(FT_s)$ versus clock period $1/f_c$.

a voltage converter with a variable clock frequency can be written as

$$R_1(FT_s) \simeq \frac{F}{F_0} \frac{1}{\left(\frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta, FT_s) d\theta\right)^2}. \quad (6.9)$$

Substitution-box (S-box) is a commonly component of modern cryptographic algorithms such as advanced encryption standard (AES) which utilizes multiple S-Boxes to perform non-linear mathematical transformations to mask the relationship between the ciphertext and the secret key [3, 85, 86]. To validate the mathematical analysis, a 130 nm CMOS S-box [80] is used as the cryptographic circuit that is powered, respectively, by a CoRe voltage converter and by an SA voltage converter. Both circuits are simulated in Cadence. $\{F_0=10\}$ ⁴ and $N=32$. The average correlation coefficient of the SA voltage converter is quite lower than the average correlation coefficient of the CoRe voltage converter when the attacker selects a fast clock frequency to perform the LPA attack, as shown in Fig. 6.3(a). The lowest MTD enhancement ratio of an S-box that employs an SA voltage converter under LPA attacks is $\sim 6,145$ when clock period is about $10^4 T_s$ while the lowest MTD enhancement ratio of an S-box that employs a CoRe voltage converter under LPA attacks is about 14.7 when clock period is about $10^2 T_s$, as shown in Fig. 6.3(b).

⁴From the experimental results in [83], the measurement noise can be reasonably filtered if the clock frequency f_c is lowered 100 times. In the simulation, the clock frequency in a normal working mode is about 10 times of the switching frequency and 100 times of the clock frequency in the idle mode, therefore, F_0 is selected as 10.

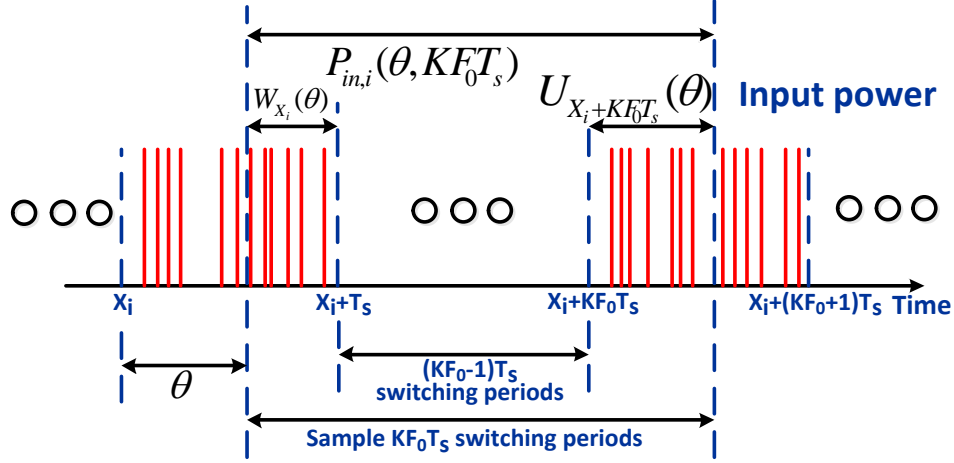


Figure 6.4 Input power profile of a cryptographic circuit that employs an SA voltage converter under LPA attacks when the attacker selects a variable number of clock periods as one sample of input power data (X_i is the starting time point of the 1st switching period for sampling the i^{th} input power data).

6.4.2 Sampling Multiple Clock Periods as One Sample of Input Power Data

The technique of sampling multiple clock/switching periods as one sample of input power data is quite efficient for filtering the power noise generated from reshuffling-based voltage converters in DPA attacks [59]. When an attacker implements an LPA attack on a cryptographic circuit that houses a CoRe voltage converter or an SA voltage converter, the attacker can also filter the reshuffling noise by sampling K , ($K \geq 2$) number of clock periods as one sample of input power data instead of lowering the clock frequency ($f_c \approx \frac{1}{F_0} f_s$) further, as shown in Fig. 6.4. The corresponding input power $P_{in,i}(\theta, KF_0 T_s)$ and load power $P_{l,i}(\theta, KF_0 T_s)$ of the SA voltage converter can be, respectively, written as

$$P_{in,i}(\theta, KF_0 T_s) = (W_{X_i}(\theta) + U_{X_i + KF_0 T_s}(\theta))P_0 + \frac{(F_0 - 1)(P_{(i-1)K+1} + \frac{V_{out}^2}{R_c})}{\eta_c} + F_0 \sum_{j=2}^K \frac{(P_{(i-1)K+j} + \frac{V_{out}^2}{R_c})}{\eta_c}, \quad (6.10)$$

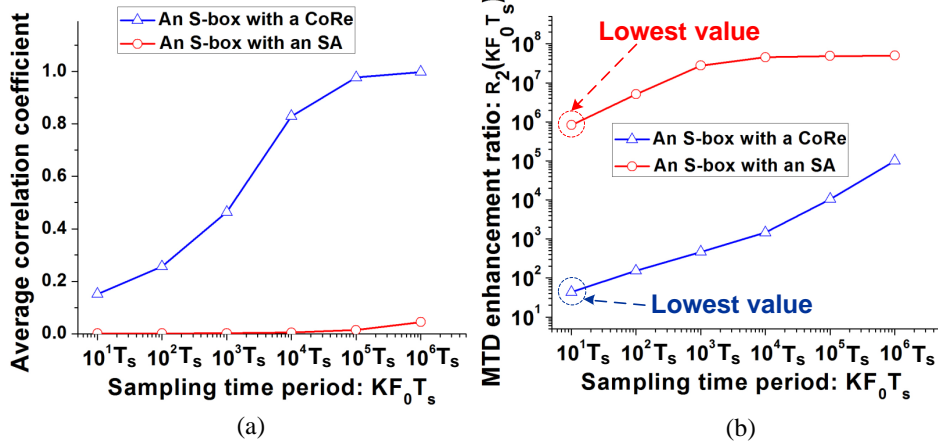


Figure 6.5 (a) Average correlation coefficient versus sampling time period KF_0T_s and (b) MTD enhancement ratio $R_2(KF_0T_s)$ versus sampling time period KF_0T_s ($F_0=10$ and $N=32$).

$$\begin{aligned}
P_{l,i}(\theta, KF_0T_s) &= (1 - \frac{\theta}{2\pi})P_{(i-1)K+1} + (F_0 - 1)P_{(i-1)K+1} \\
&+ F_0 \sum_{j=2}^K P_{(i-1)K+j} + \frac{\theta}{2\pi}P_{(i-1)K+K+1},
\end{aligned} \tag{6.11}$$

where $P_{(i-1)K+j}$, ($j = 1, 2, \dots$) is the leakage power dissipation of the cryptographic circuit induced by the $((i-1)K + j)^{th}$ input data. $W_{X_i}(\theta)$ and $U_{X_i+KF_0T_s}(\theta)$ are the corresponding number of active phases, as illustrated in Fig. 6.4.

As compared to sampling a single clock period as one sample of input power data, sampling K number of clock periods as one sample of input power data would enhance the MTD value to K times [59]. Therefore, the MTD enhancement ratio $R_2(KF_0T_s)$ of a cryptographic circuit that employs a voltage converter is

$$R_2(KF_0T_s) \simeq K \frac{1}{(\frac{1}{2\pi} \int_0^{2\pi} \gamma(\theta, KF_0T_s) d\theta)^2}, \tag{6.12}$$

when utilizing K number of clock periods as one sample of input power data.

When the attacker increases the sampling time period to KF_0T_s , the average correlation coefficient of the SA voltage converter has a marginal enhancement, as shown in Fig. 6.5(a). This indicates that sampling multiple clock periods as one sample of input power data to mitigate noise is not sufficiently effective. The lowest MTD enhancement ratio of an S-box with an SA (CoRe)

voltage converter is 826446 (43) (shown in Fig. 6.5(b)), which is much higher than the lowest MTD enhancement ratio 6,145 (14.7) (shown in Fig. 6.3(b)). That means further reducing the clock frequency f_c is more effective than sampling multiple clock periods as one sample of input power data to enhance the power of LPA attacks on an S-box with a voltage converter. The primary reason is that under the same sampling time period ($FT_s = KF_0T_s$), the variance of the load power of a voltage converter with a variable clock frequency $D(P_{l,i}(\theta, FT_s))$ is

$$D(P_{l,i}(\theta, FT_s)) = D(FP_i) = D(KF_0P_i) = K^2F_0^2\sigma_s^2, \quad (6.13)$$

where σ_s^2 is the variance of the leakage power dissipation of the cryptographic circuit. However, the variance of load power of a voltage converter while sampling K number of clock periods as one sample of input power data $D(P_{l,i}(\theta, KF_0T_s))$ is ($F_0 > 1$)

$$\begin{aligned} D(P_{l,i}(\theta, KF_0T_s)) &= \\ D\left(\left(1 - \frac{\theta}{2\pi}\right)P_{(i-1)K+1} + (F_0 - 1)P_{(i-1)K+1}\right) &+ \\ + D\left(F_0 \sum_{j=2}^K P_{(i-1)K+j}\right) + D\left(\frac{\theta}{2\pi}P_{(i-1)K+K+1}\right) &= \\ = \left(F_0 - \frac{\theta}{2\pi}\right)^2\sigma_s^2 + F_0^2(K-1)\sigma_s^2 + \left(\frac{\theta}{2\pi}\right)^2\sigma_s^2 &= \\ = KF_0^2\sigma_s^2 - \frac{\theta}{\pi}F_0\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 < KF_0^2\sigma_s^2 - \frac{\theta}{\pi}\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 & \\ \leq KF_0^2\sigma_s^2 - \frac{\theta}{\pi} \frac{\theta}{2\pi}\sigma_s^2 + \frac{\theta^2}{2\pi^2}\sigma_s^2 = KF_0^2\sigma_s^2. & \end{aligned} \quad (6.14)$$

As compared to sampling K number of clock periods as one sample of input power data, further lowering clock frequency f_c can therefore enhance the variance of the load power of the voltage converter over K times. A larger variance of the load power enhances the SNR of the voltage converter and decreases the lowest MTD enhancement ratio.

Lowering clock frequency f_c further is more efficient than sampling multiple clock periods as one sample of input power data to enhance the power of LPA attacks. When the attacker further lowers clock frequency f_c , as shown in Fig. 6.3(b), the idle critical frequency F_{ic} can be selected

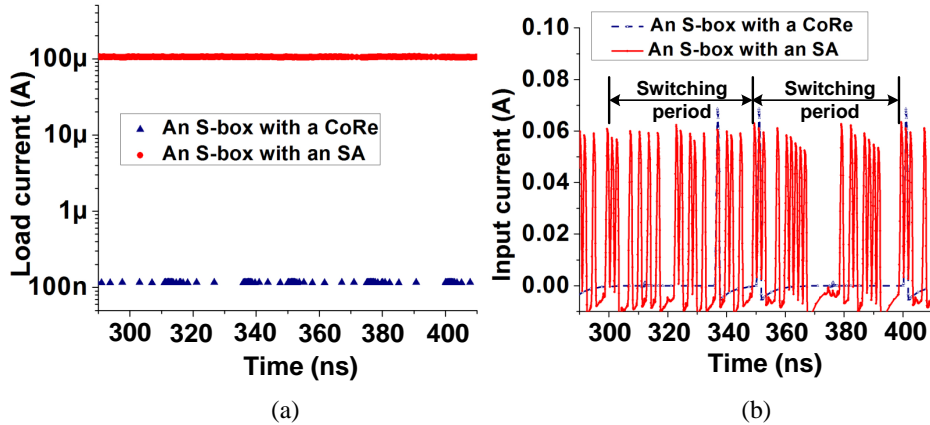


Figure 6.6 (a) Load current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter, (b) Input current profile of an S-box that employs a CoRe voltage converter and an S-box that employs an SA voltage converter.

as $1/(10^5 T_s)$. The intuitive explanation is that when the clock frequency f_c is lower than the idle critical frequency $F_{ic} = 1/(10^5 T_s)$, the M_2 transistor would be turned-off to make the SA voltage converter behave as a CoRe voltage converter. The MTD enhancement ratio of an S-box with an SA voltage converter is almost the same as the MTD enhancement ratio of an S-box with a CoRe voltage converter when the clock frequency f_c is lower than $1/(10^5 T_s)$, as shown in Fig. 6.3(b). The security of an S-box with an SA voltage converter against LPA attacks therefore would not be compromised when $F_{ic} = 1/(10^5 T_s)$.

6.5 Circuit Level Verification

To validate the proposed countermeasure with circuit level simulations, a 130 nm CMOS S-box [80] is used as the load to simulate the correlations between the input and load power profiles of different voltage converters. A 32-phase 2:1 CoRe voltage converter and a 32-phase 2:1 SA voltage converter are used in the simulations. The detailed architecture and control algorithm of the CoRe voltage converter can be found in [59]. The input voltage V_{in} and output voltage V_{out} of the voltage converters used in the simulations are, respectively, 2.4 V and 1.2 V. Additionally, the clock frequency f_c of the S-box to perform an LPA attack is reduced to 2 MHz and the variation range of the switching frequency f_s of the voltage converter is $f_s \in [19 \text{ MHz}, 21 \text{ MHz}]$.

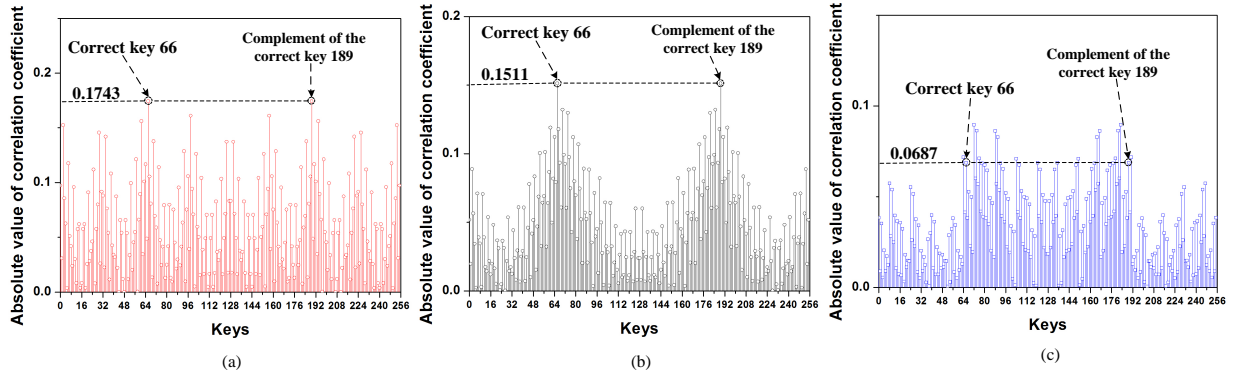


Figure 6.7 LPA attacks simulation: (a) All of the possible keys versus absolute value of the correlation coefficient for an S-box without countermeasure after analyzing 500 leakage power traces, (b) All of the possible keys versus absolute value of correlation coefficient for an S-box that employs a CoRe voltage converter after analyzing 2 million leakage power traces, and (c) All of the possible keys versus absolute value of the correlation coefficient for an S-box that employs an SA voltage converter after analyzing 2 million leakage power traces.

The load current of the SA voltage converter is significantly higher than the CoRe voltage converter when the S-box is under LPA attacks, as shown in Fig. 6.6(a). The high load power dissipation of the SA voltage converter from the discharging resistor R_c is reshuffled in the input power profile to generate high power noise against LPA attacks. As demonstrated in Fig. 6.6(b), only a single phase is active in a switching period in an S-box that employs a CoRe voltage converter while 16 phases are activated in a switching period in an S-box that employs an SA voltage converter. The large number of active phases in each switching period would significantly enhance the entropy of the PRNG from $\log_2^{(32)}_1$ to $\log_2^{(32)}_{16}$, generating a large amount of uncertain power noise in input power profile against LPA attacks.

6.6 LPA Attacks Simulation

When LPA attacks are implemented (simulated) on an S-box [80] that does not house any countermeasure, the correct key (which is $(66)_{10}$ in this example) is leaked to the attacker after analyzing 500 leakage power traces, as shown in Fig. 6.7(a). When the attacker implements an LPA attack on an S-box that employs an SA voltage converter and lowers the clock frequency f_c to $1/(10^4 T_s)$ (clock frequency with lowest MTD enhancement ratio as shown in Fig. 6.3(b)), the

correct key cannot be obtained by the attacker even after analyzing two million leakage power traces, as shown in Fig. 6.7(c). By contrast, when the attacker lowers the clock frequency f_c to $1/(10^4 T_s)$ and implements an LPA attack on an S-box which employs a CoRe voltage converter, after analyzing 2 million leakage power traces, the correct key is leaked to the attacker, as shown in Fig. 6.7(b). Therefore, as compared to an S-box that employs a CoRe voltage converter, the reshuffled redundant load power dissipation in the SA voltage converter can successfully act as noise to enhance the MTD value.

6.7 Conclusion

A security-adaptive (SA) voltage converter is utilized as a lightweight countermeasure against LPA attacks. The discharging resistor in the SA voltage converter can significantly increase the amount of noise insertion in the input power profile when LPA attacks are sensed by the proposed technique. Through scrambling the redundant load power dissipation in the input power profile, the MTD value of a cryptographic circuit that employs the SA voltage converter is enhanced over 6,145 times as compared to the MTD value of a conventional cryptographic circuit that has no countermeasure.

CHAPTER 7: ON-CHIP VOLTAGE REGULATION WITH VFS

7.1 Introduction

Dynamic power consumption of a cryptographic circuit is $P_{dyn} = \alpha f_c V_{dd}^2$ where f_c , V_{dd} , and α are, respectively, the clock frequency, supply voltage, and activity factor¹. Activity factor α is determined by the number of $0 \rightarrow 1$ transitions that occur in the cryptographic circuit under different input data [75]. To hide the actual dynamic power consumption P_{dyn} of a cryptographic circuit, different logic families are proposed to make the dynamic power consumption constant under different input data values. The wave dynamic differential logic (WDDL), which is a type of balanced logic gate, is proposed in [85, 88] to make the activity factor α constant regardless of the input data values. A switched-capacitor current equalizer-based countermeasure is proposed in [61] to achieve a constant P_{dyn} through discharging the residual charge in every switching cycle. However, DPA attacks countermeasures that hide the dynamic power dissipation of a cryptographic circuit by maintaining constant dynamic power consumption typically cause significant power/area/performance overhead [2, 61]. Alternatively, masking technique [5, 6] is an effective DPA attacks countermeasure that uses random intermediate data values to be inserted among the actual side channel leakage data to reduce the correlation between the input data and α . However, masking technique may also induce significant area overhead due to the large look-up table (LUT) when a large amount of random data is inserted [5, 6]. Please note that the effectiveness of masking-based countermeasures is directly correlated with the number of inserted data values. There is therefore a tradeoff between the LUT size and the effectiveness of the masking operation.

¹The content of this Chapter has been published in [87], the copyright permission can be found in Appendix F.

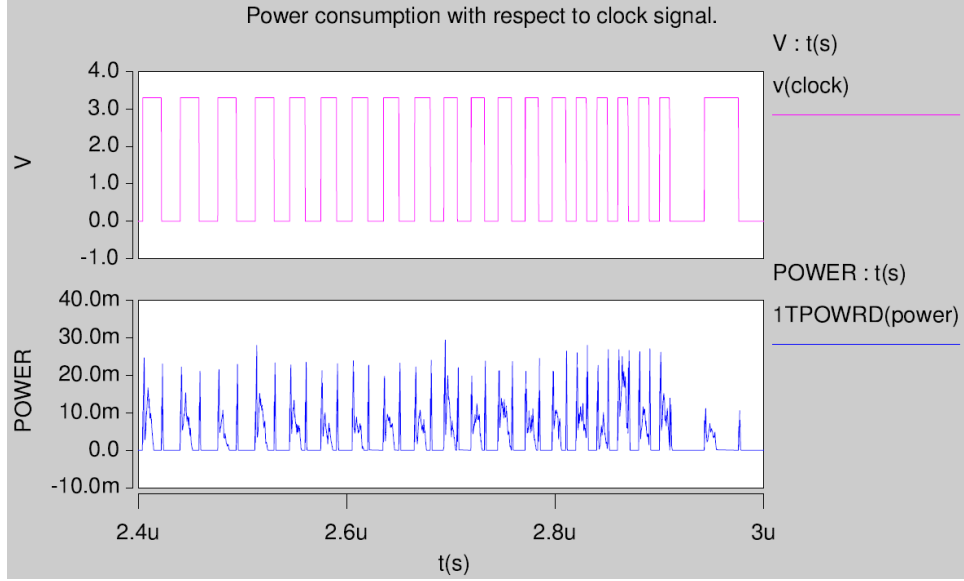


Figure 7.1 Relationship between the clock pulse and power consumption of a cryptographic circuit [7].

To minimize the information leakage through the power consumption profile, existing power management techniques that scale voltage and/or frequency at runtime have been tailored as a countermeasure against DPA attacks [7, 8, 21]. These voltage/frequency scaling (VFS) based countermeasures typically randomize the supply voltage and/or the frequency to break the one-to-one relationship between these parameters and the actual workload. Random dynamic voltage and frequency scaling (RDVFS) technique is one of the first VFS-based countermeasures against DPA attacks that reduces the power consumption while also increasing the security [21]. The working principle of the RDVFS technique is to randomly vary f_c and V_{dd} to mask the dynamic power variations from an attacker. RDVFS technique, however, has major security flaws since the clock frequency f_c can be leaked in the input power profile, as demonstrated in Fig. 7.1 [7]. In other words, in a cryptographic circuit that utilizes conventional RDVFS, f_c becomes a linear function of V_{dd} , ($f_c = K_1.V_{dd} + B$ where K and B are the linear parameters) [7].

An attacker can therefore unriddle the fluctuations in the f_c and V_{dd} by solely monitoring the width of the spikes in the power consumption profile. After analyzing the pulse width of the monitored power consumption of the cryptographic circuit concurrently with the input data, a

cryptographic circuit that houses the RDVFS technique can therefore be breached with negligible effort [7]. Another VFS-based countermeasure, random dynamic voltage scaling (RDVS) technique, is proposed in [7] to disrupt the linear relationship between f_c and V_{dd} . Unfortunately, this technique introduces significant power overhead to disrupt the relationship between f_c and V_{dd} where the security increases with higher power overhead. In order to minimize the power overhead while utilizing VFS as a countermeasure to secure a cryptographic circuit, Avirneni *et al.* [8] proposed the aggressive voltage and frequency scaling (AVFS) technique. In the AVFS technique, f_c and V_{dd} are independent so that an attacker can no longer estimate the changes in V_{dd} by solely monitoring the pulse width of the spikes in the monitored power dissipation profile. AVFS technique, however, increases the total chip area by about 3% due to redundant register duplication to minimize the circuit contamination delay [8].

Leakage power dissipation primarily has two components: subthreshold power leakage and gate-oxide power leakage [89]. These two power leakage components increase significantly with the continuous scaling of the silicon technology and the reduced supply voltage levels. Conventional LPA attacks are quite sensitive to measurement noise [90] and therefore have attracted relatively less attention as compared to DPA attacks. LPA attacks can still be quite effective if the clock frequency of the cryptographic circuit is lowered by the attacker and the analysis is reinforced with average sampling analysis [83]. Although there are no VFS-based countermeasures specifically tailored against LPA attacks, the leakage power dissipation is naturally affected by the voltage scaling techniques and the aforementioned VFS-based countermeasures are also partly effective against LPA attacks. Moreover, on-chip voltage regulation is becoming an essential part of cryptographic circuits, enabling faster and more power efficient voltage/frequency scaling (VFS) [71] with less than 1% area overhead [91]. In this Chapter, we investigate the security implications of three different on-chip voltage regulator topologies: low-dropout (LDO) regulator, buck converter, and switched-capacitor (SC) converter that can be implemented with countermeasures such as RDVFS, RDVS, and AVFS against both DPA and LPA attacks.

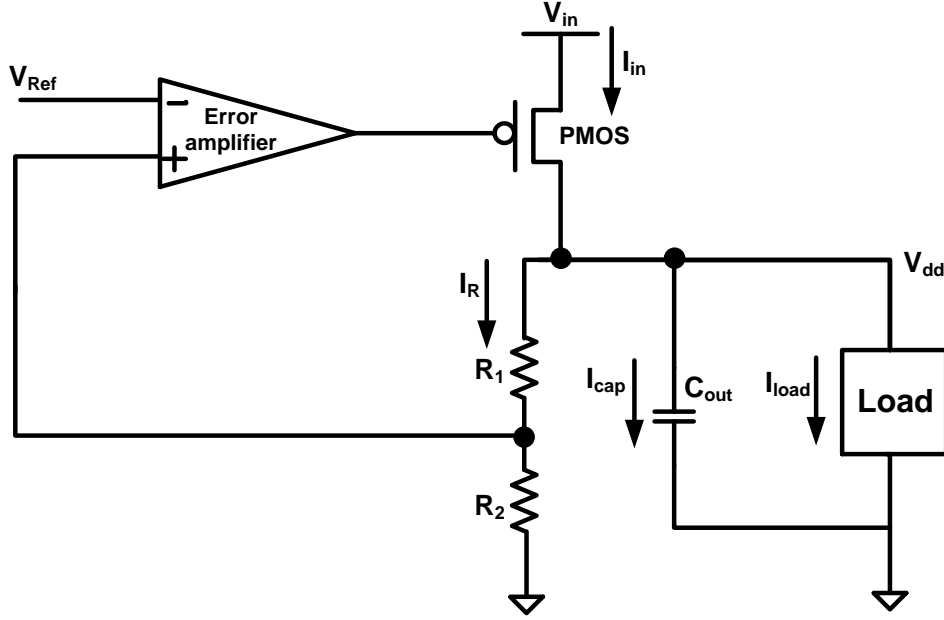


Figure 7.2 Schematic of a conventional LDO voltage regulator.

7.2 On-Chip Voltage Regulation with VFS Load

Each voltage regulator topology has different input and output voltage/current characteristics. These differences change the way how different voltage regulators may leak critical information. In this section, the side-channel leakage mechanisms of three widely used on-chip voltage regulator topologies are investigated.

7.2.1 Low-Dropout (LDO) Regulator with VFS Load

The relationship between the input current I_{in} and the load current I_{load} of an LDO regulator, as shown in Fig. 7.2, is

$$I_{in} = I_R + I_{cap} + I_{load}, \quad (7.1)$$

where I_R and I_{cap} are, respectively, the resistor and capacitor current. To minimize the power conversion loss, the resistances of R_1 and R_2 are typically quite large, making the resistor current I_R negligible. Recently, output-capacitorless LDO voltage regulators have proliferated to reduce the area of LDO regulators [65, 92]. As a result, the capacitor current I_{cap} can also be ignored in

our derivations without loss of generality. The relationship between I_{in} and I_{load} can therefore be approximated as

$$I_{in} \approx I_{load}. \quad (7.2)$$

Similarly, the relationship between the input power P_{in} and load current I_{load} can be denoted as

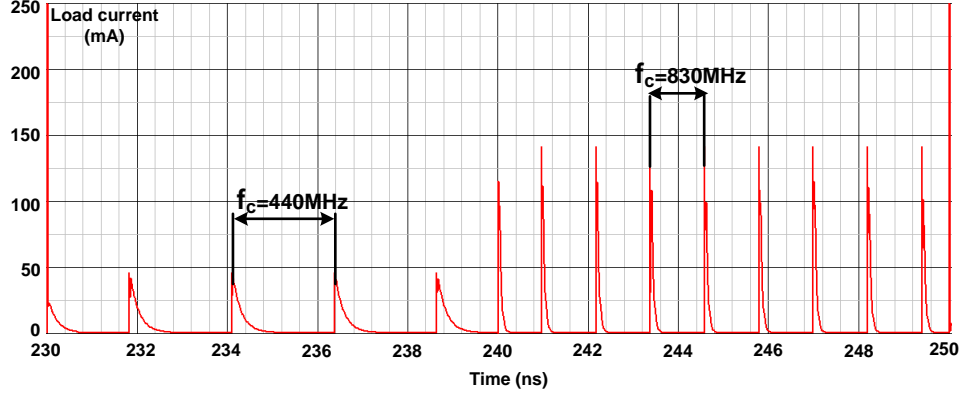
$$P_{in} \approx V_{in}I_{load}, \quad (7.3)$$

where V_{in} is the input voltage. Since there is an approximated linear relationship between P_{in} and I_{load} , certain characteristics of the clock frequency f_c can be estimated by an attacker by monitoring the input power profile.

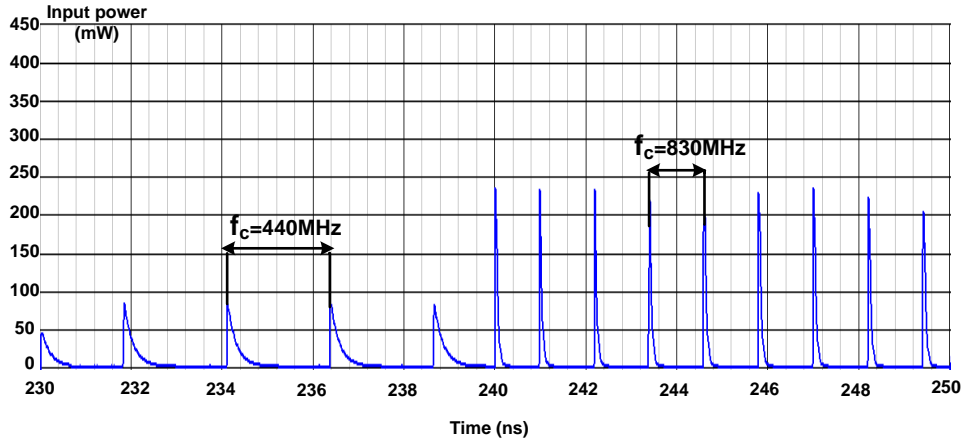
The relationship between the load current and input power of an LDO voltage regulator is analyzed under a switching load where the clock frequency and supply voltage (f_c, V_{dd}) pair varies between (440 MHz, 0.8 V) and (830 MHz, 1.2 V) [8]. As shown in Figs. 7.3(a) and 7.3(b), a linear relationship exists between the load current I_{load} and input power P_{in} of an LDO regulator. An attacker can therefore determine the variations in f_c by monitoring the variations in P_{in} to nullify RDVFS technique under DPA attacks. The correlation between the input power and load current of an LDO regulator is so high that an attacker can visually extract the workload information without using any advanced analysis techniques.

7.2.2 Buck Converter with VFS Load

A buck converter, as shown in Fig. 7.4, can have three different operating modes: continuous conduction mode (CCM), discontinuous conduction mode (DCM), and the boundary between CCM and DCM, (BCM). The relationships between the input voltage V_{in} and the output voltage V_{dd} of



(a)



(b)

Figure 7.3 (a) Transient load current profile of an LDO voltage regulator with VFS load and (b) Transient input power profile of an LDO voltage regulator with VFS load.

a buck converter (shown in Fig. 7.4) operating in these three operating modes are

$$V_{dd} = \begin{cases} DV_{in} & , K_2 > 1 - D, (CCM) \\ DV_{in} & , K_2 = 1 - D, (BCM) \\ \frac{2V_{in}}{1 + \sqrt{1 + 4K_2/D^2}} & , K_2 < 1 - D, (DCM) \end{cases} \quad (7.4)$$

where D is the duty cycle of the input switching signal. The critical value is $K_2 = 2Lf_s/R$ where L is the inductance of the filter inductor, f_s is the switching frequency, and R is the impedance of load. It is quite difficult for an attacker to analyze the variations of V_{dd} if the buck converter works

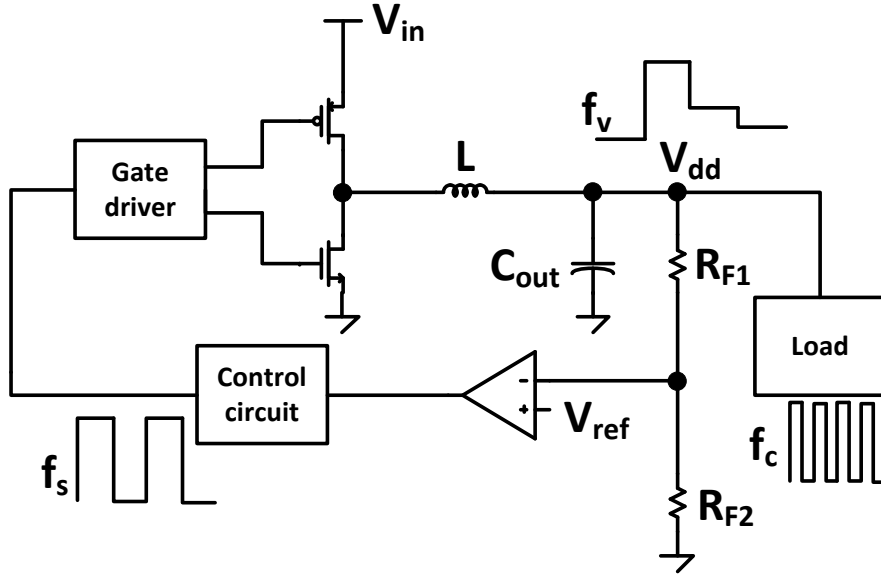


Figure 7.4 Schematic of a conventional buck converter.

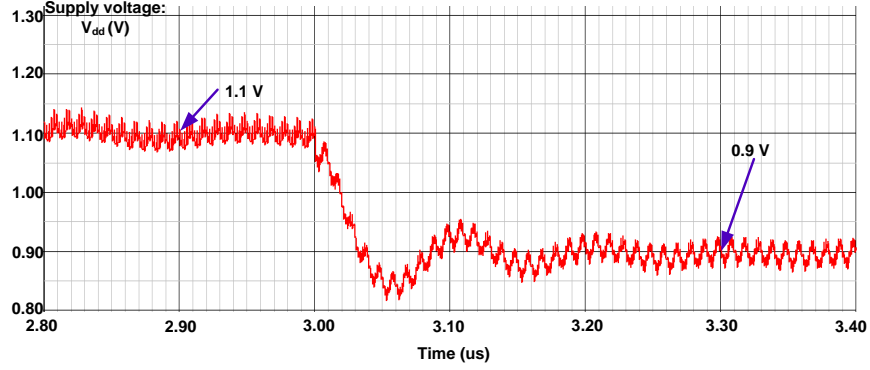
in the DCM since the critical value K_2 would become uncertain due to the variations in the value of the load impedance R under different input data. An attacker can, however, still determine the changes in V_{dd} by monitoring the slope of the input power profile which is a strong function of the filter inductor current. When the inductor is in the charging state, the relationship between V_{dd} and the slope of input current S_1 is

$$S_1 = \frac{dI_{in}}{dt} = \frac{V_{in} - V_{dd}}{L}. \quad (7.5)$$

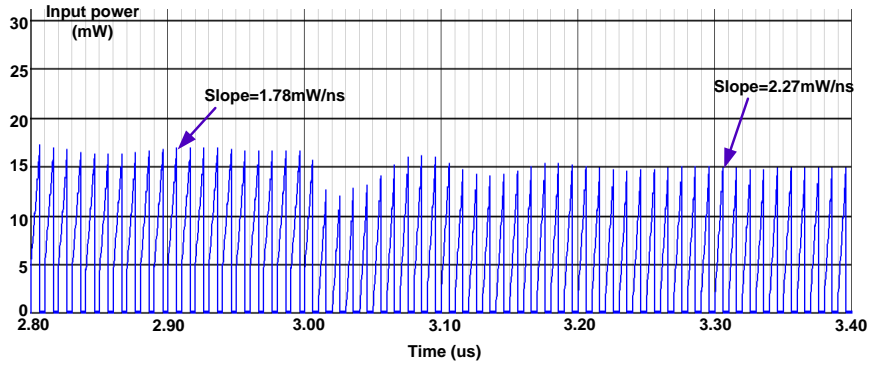
Similarly, the relationship between V_{dd} and the slope of input power S_2 is

$$S_2 = \frac{dP_{in}}{dt} = \frac{1}{L}(V_{in}^2 - V_{in}V_{dd}). \quad (7.6)$$

We investigate the possible leakage of critical workload information through the slope of the monitored input power signature via simulations. The relationship between S_2 and V_{dd} of a buck converter is analyzed under a switching load when the clock frequency and supply voltage (f_c, V_{dd}) pair for the switching load varies between (440 MHz, 0.8 V) and (830 MHz, 1.2 V). The switching frequency of buck converter is typically around 100MHz [45]. When V_{dd} drops from 1.1



(a)



(b)

Figure 7.5 (a) Transient supply voltage (output voltage) V_{dd} of a buck converter with VFS load and (b) Transient input power profile of a buck converter with VFS load.

V to 0.9 V, S_2 increases from 1.78 mW/ns to 2.27 mW/ns, as shown in Fig. 7.5. An inversely linear relationship exists between S_2 and V_{dd} , as illustrated in Fig. 7.6. This inversely linear relationship demonstrates the possible information leakage through the slope of input power profile that may nullify RDVFS technique under DPA attacks.

7.2.3 Switched-Capacitor (SC) Converter with VFS Load

An SC voltage converter utilizes one or multiple flying capacitors with a switch network where the flying capacitors charge from the input voltage V_{in} and discharge to the output node periodically to generate a DC output voltage V_{dd} . The basic architecture of an SC voltage converter is illustrated in Fig. 7.7. Different voltage conversion ratios can be obtained by modifying the connections of the switches and capacitors within an SC converter.

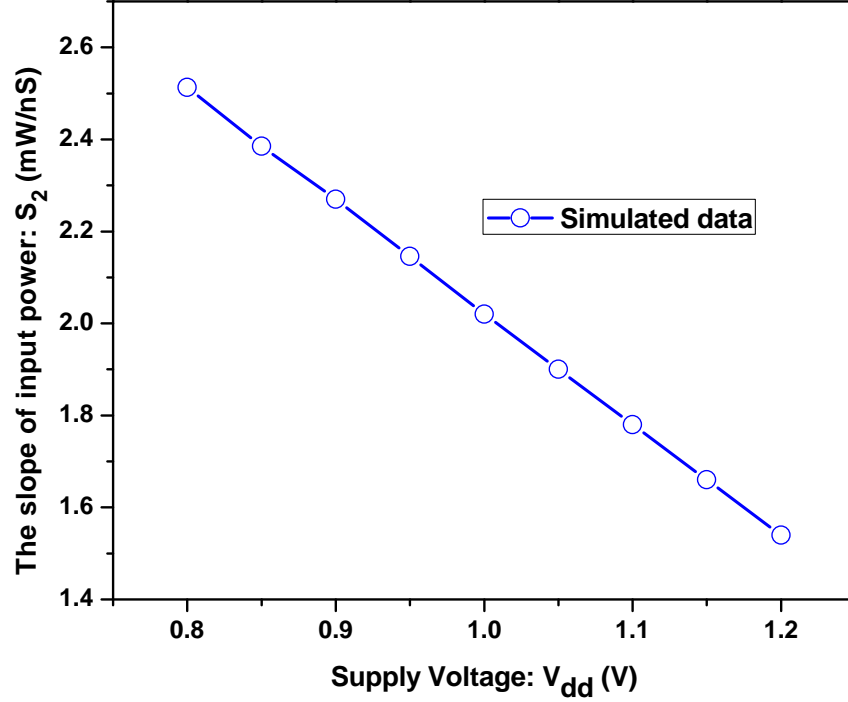


Figure 7.6 Relationship between the supply voltage V_{dd} and the slope of the input power S_2 in the charging state.

The relationship between the switching frequency f_s and the load current I_{load} of an SC converter is [52]

$$A(V_{dd})f_s = I_{load}, \quad (7.7)$$

where $A(V_{dd})$ is a function of the supply voltage V_{dd} . Typically, the switching frequency of an SC converter is around $100MHz$ [71], which is much lower than the clock frequency f_c of a typical S-box which can be around $500MHz$ [8]. Therefore, in a single switching period of an SC converter, several spikes occur due to the high clock frequency of the transistors. Assuming that the number of the transitions of load power within a switching period is M , the relationship between f_s and f_c

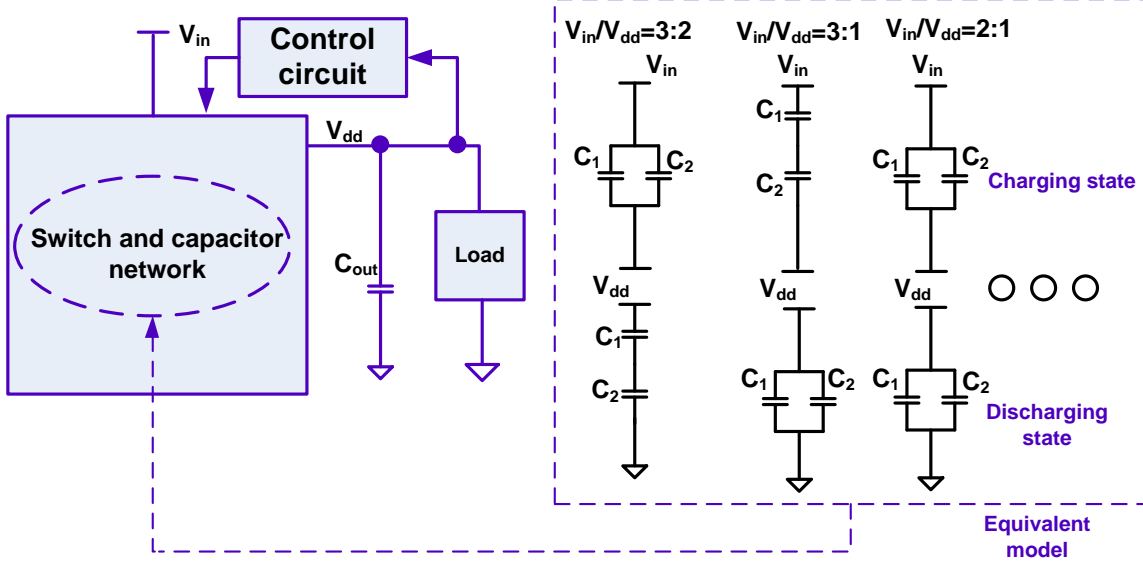


Figure 7.7 Basic architecture of a switched-capacitor (SC) voltage converter.

can be written as

$$\begin{aligned}
 f_s &= \frac{1}{A(V_{dd})} I_{load} = \frac{1}{A(V_{dd})} \frac{P_{dyn}}{V_{dd}} \\
 &= \frac{1}{A(V_{dd})} \frac{\sum_{i=1}^M \alpha_i f_c V_{dd}^2}{V_{dd}} = \frac{f_c V_{dd}}{A(V_{dd})} \sum_{i=1}^M \alpha_i,
 \end{aligned} \tag{7.8}$$

where P_{dyn} is the dynamic power consumption of a cryptographic circuit and $\alpha_i (i = 1, 2, \dots)$ is the corresponding activity factor. While the value of $\sum_{i=1}^M \alpha_i$ is determined by the input data, the switching frequency f_s , which may be exploited to obtain critical information about f_c , is masked by scrambling the monitored activity factor $\sum_{i=1}^M \alpha_i$. An SC converter with a variable $\sum_{i=1}^M \alpha_i$ is analyzed under a switching load circuit with 670 MHz clock frequency and 1 V supply voltage [8] while $\sum_{i=1}^M \alpha_i$ varies between 50pF and 400pF. As shown in Fig. 7.8, the switching frequency f_s is successfully changed by varying $\sum_{i=1}^M \alpha_i$ in input power profile with a constant f_c .

When the SC converter is in the charging state, the equality denoting the charging of the flying capacitor should be satisfied as

$$\frac{V_{in} - V_1(t)}{R(V_{dd})} = C_{top}(V_{dd}) \frac{dV_1(t)}{dt}, \tag{7.9}$$

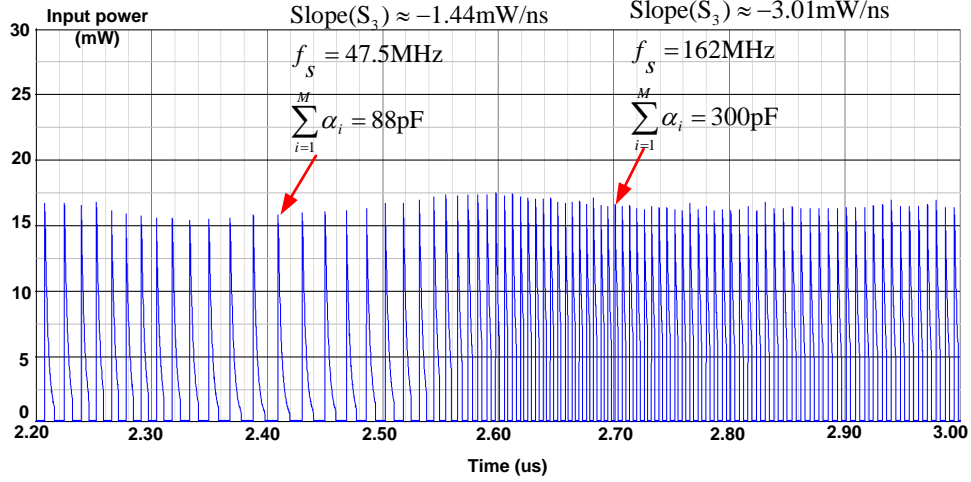


Figure 7.8 Transient input power of an SC converter with variable $\sum_{i=1}^M \alpha_i$.

where $C_{top}(V_{dd})$ is the capacitance of the top plate in the equivalent flying capacitor, $R(V_{dd})$ is the equivalent series resistance, and $V_1(t)$ is the voltage of the top plate of the equivalent flying capacitor. The expression for $V_1(t)$, the input power in charging state $P_{in}(t)$, and the slope of input power in charging state S_3 , respectively, are

$$V_1(t) = V_1(0) + (V_{in} - V_1(0))(1 - e^{-t/R(V_{dd})C_{top}(V_{dd})}), \quad (7.10)$$

$$P_{in}(t) = V_{in} \frac{dV_1(t)}{dt} = \frac{V_{in}^2 - V_{in}V_1(0)}{R(V_{dd})C_{top}(V_{dd})} e^{-t/R(V_{dd})C_{top}(V_{dd})}, \quad (7.11)$$

$$S_3 = \frac{dP_{in}(t)}{dt} = -\frac{V_{in}^2 - V_{in}V_1(0)}{R^2(V_{dd})C_{top}^2(V_{dd})} e^{-t/R(V_{dd})C_{top}(V_{dd})}, \quad (7.12)$$

where $V_1(0)$ is the voltage of the top plate in the equivalent flying capacitor before charging. To prevent the leakage of the supply voltage V_{dd} information through the input power profile from the slope of the input power S_3 in the charging state, the variations of the supply voltage (reflected by $R(V_{dd})C_{top}(V_{dd})$) and the variations of load power induced by different input data (reflected by $V_1(0)$) are also scrambled together. As shown in Fig. 7.8, S_3 also depends on the variation of $\sum_{i=1}^M \alpha_i$ in input power profile when V_{dd} is fixed.

Table 7.1 Inserted Noise $N_{j,k}(f_c, V_{dd})$, ($j, k = 1, 2, 3$) into the Power Consumption Profile of a Cryptographic Circuit through Countermeasures that Employ Different Voltage Regulators against DPA Attacks (Detail Explanation can be Found in Appendix C).

Regulator Technique	LDO regulator	Buck converter	SC converter
RDVFS	$N_{1,1}(f_c, V_{dd})$ $= 0$	$N_{1,2}(f_c, V_{dd})$ $= 0$	$N_{1,3}(f_c, V_{dd}) =$ $\log(F(V_{dd})) + 2\log(V_{dd})$
RDVS	$N_{2,1}(f_c, V_{dd})$ $= 2 \log(V_{dd})$	$N_{2,2}(f_c, V_{dd})$ $= 0$	$N_{2,3}(f_c, V_{dd}) =$ $2\log(V_{dd})$
AVFS	$N_{3,1}(f_c, V_{dd})$ $= 2 \log(V_{dd})$	$N_{3,2}(f_c, V_{dd})$ $= \log(f_c)$	$N_{3,3}(f_c, V_{dd}) =$ $\log(f_c) + 2\log(V_{dd})$

7.3 Security Evaluation of On-Chip Voltage Regulation with VFS Technique Against DPA Attacks

Countermeasures against side-channel attacks either insert noise to the side-channel leakage or reduce the critical signal in the side-channel leakage. VFS-based countermeasures typically insert noise to the power consumption profile to increase the number of measurements that an attacker needs to perform for a successful attack. As mentioned in the *Introduction*, the dynamic power consumption of cryptographic circuits P_{dyn} is

$$P_{dyn} = \alpha f_c V_{dd}^2. \quad (7.13)$$

After taking logarithm of both of the sides, (7.13) can be written as

$$\log(P_{dyn}) = \log(\alpha) + \log(f_c) + 2\log(V_{dd}), \quad (7.14)$$

where $\log(\alpha)$ represents the side-channel signal related with DPA attacks. The amount of uncertain noise $N_{j,k}(f_c, V_{dd})$ that is inserted through different countermeasures that employ three different types of voltage regulators varies significantly, as shown in Table 7.1. When a cryptographic circuit

employs the AVFS technique with an SC converter, the inserted noise would contain both random f_c and random V_{dd} due to the independent relationship between f_c and V_{dd} . When a cryptographic circuit employs the RDVS technique with an SC converter, the inserted noise would only contain random V_{dd} as the clock frequency f_c is fixed. The inserted noise would be zero when the RDVFS technique employs an LDO regulator or a buck converter as either f_c or V_{dd} would leak through the input power profile. By utilizing the correlation between f_c and V_{dd} , the inserted noise in the side-channel through the countermeasures may be eliminated. However, if a cryptographic circuit employs an SC converter with the RDVFS technique, the uncertain noise would contain both the random clock frequency and supply voltage. As compared to the AVFS technique, a linear relationship exists between the clock frequency f_c and supply voltage V_{dd} when the RDVFS technique employs an SC converter. The clock frequency can therefore be denoted as a function of the supply voltage (*i.e.*, $f_c = F(V_{dd}) = K_1 \cdot V_{dd} + B$ where $K_1 = 975 \text{ MHz/V}$ and $B = -340 \text{ MHz}$ when $V_{dd} \in [0.8V, 1.2V]$ and $f_c \in [440\text{MHz}, 830\text{MHz}]$ [8]).

7.3.1 Security of On-Chip Voltage Regulation with True Random VFS Technique Against DPA Attacks

When all of the aforementioned techniques are true random, the clock frequency f_c and supply voltage V_{dd} would have uniform distributions. Let's assume that V_{DD1} and V_{DD2} are, respectively, the minimum and maximum voltage values that V_{dd} can operate. Similarly, f_1 and f_2 are, respectively, the minimum and maximum frequency values that f_c can take. When the number of discrete values that V_{dd} can take within $[V_{DD1}, V_{DD2}]$ is N , the resolution of supply voltage ΔV_{dd} and i^{th} , ($i = 1, 2, 3, \dots, N$) possible value $V_{dd,i}$ within $[V_{DD1}, V_{DD2}]$ can be, respectively, denoted as

$$\Delta V_{dd,i} = \frac{V_{DD2} - V_{DD1}}{N - 1}, \quad (7.15)$$

$$V_{dd,i} = \frac{(i - 1) \times (V_{DD2} - V_{DD1})}{N - 1} + V_{DD1}. \quad (7.16)$$

Similarly, assuming that frequency can get N different values within $[f_1, f_2]$, the i^{th} possible value $f_{c,i}$ can be denoted as

$$f_{c,i} = \frac{(i-1) \times (f_2 - f_1)}{N-1} + f_1. \quad (7.17)$$

If the frequency² of the voltage scaling operation is f_v , the mean value of the inserted noise $E(N_{j,k}(f_c, V_{dd}))$ for on-chip voltage regulation based and uniformly distributed RDVFS technique ($j = 1$), RDVS technique ($j = 2$), and AVFS technique ($j = 3$), respectively, are

$$E(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N [\frac{f_{c,i}}{f_v}]} \sum_{i=1}^N [\frac{f_{c,i}}{f_v}] N_{1,k}(f_{c,i}, V_{dd,i}), \quad (7.18)$$

$$E(N_{2,k}(f_c, V_{dd})) = \frac{1}{N} \sum_{i=1}^N N_{2,k}(f_c, V_{dd,i}), \quad (7.19)$$

$$E(N_{3,k}(f_c, V_{dd})) = \frac{1}{N \sum_{l=1}^N [\frac{f_{c,l}}{f_v}]} \sum_{l=1}^N \sum_{i=1}^N [\frac{f_{c,l}}{f_v}] N_{3,k}(f_{c,l}, V_{dd,i}). \quad (7.20)$$

The corresponding variance of the inserted noise $Var(N_{j,k}(f_c, V_{dd}))$ can be denoted, respectively, as

$$Var(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N [\frac{f_{c,i}}{f_v}]} \sum_{i=1}^N [\frac{f_{c,i}}{f_v}] (N_{1,k}(f_{c,i}, V_{dd,i}) - E(N_{1,k}(f_c, V_{dd})))^2, \quad (7.21)$$

²Since on-chip voltage regulator can generate variable supply voltage levels V_{dd} , we assume that the frequency of the voltage scaling is f_v .

$$\begin{aligned} \text{Var}(N_{2,k}(f_c, V_{dd})) = \\ \frac{1}{N} \sum_{i=1}^N (N_{2,k}(f_c, V_{dd,i}) - E(N_{2,k}(f_c, V_{dd})))^2, \end{aligned} \quad (7.22)$$

$$\begin{aligned} \text{Var}(N_{3,k}(f_c, V_{dd})) = \frac{1}{N \sum_{i=1}^N [\frac{f_{c,l}}{f_v}]} \times \\ \sum_{l=1}^N \sum_{i=1}^N [\frac{f_{c,l}}{f_v}] (N_{3,k}(f_{c,l}, V_{dd,i}) - E(N_{3,k}(f_c, V_{dd})))^2. \end{aligned} \quad (7.23)$$

A cryptographic circuit that employs on-chip voltage regulation based VFS technique can be modeled with two separate noise insertion blocks (noise block₁ and noise block₂), as shown in Fig. 7.9. Accordingly, the correlation coefficient between the input data and monitored power consumption P_{dyn} of that cryptographic circuit can be represented with the correlation between the input data and monitored power dissipation of those two noise insertion blocks. The signal-to-noise ratio (SNR) at the output of the noise block₂ $SNR''_{j,k}$ can be denoted as

$$SNR''_{j,k} = \frac{\text{Var}(\log(\alpha))}{\text{Var}(N_{j,k}(f_c, V_{dd}))}, \quad (7.24)$$

where $\text{Var}(\log(\alpha))$ represents the variance of $\log(\alpha)$. The correlation coefficient $\gamma''_{j,k}$ between the activity factor α and monitored power dissipation P_{dyn} of the cryptographic circuit can be obtained as [75]

$$\gamma''_{j,k} = \frac{1}{\sqrt{1 + \frac{1}{SNR''_{j,k}}}}. \quad (7.25)$$

Correlation coefficient between the input data and monitored power dissipation of the cryptographic circuit is widely used as a metric to evaluate the level of security [3, 75, 93]. Since the operations that take place in the noise block₁ are independent of the operations that take place in the noise block₂, the correlation coefficient $\gamma_{j,k}$ between the input data and monitored power

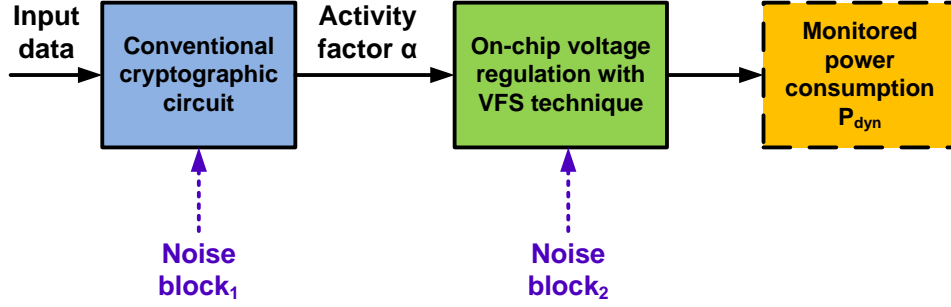


Figure 7.9 Relationship between the input data and monitored power consumption P_{dyn} of a cryptographic circuit that employs an on-chip voltage regulation based VFS technique (*Conventional cryptographic circuit* represents a cryptographic circuit without any countermeasure).

consumption can be written as [75]

$$\gamma_{j,k} = \gamma' \times \gamma''_{j,k}, \quad (7.26)$$

where γ' is the correlation coefficient between the input data and activity factor. Therefore, $(1 - \gamma''_{j,k})$ can be defined as the *correlation coefficient reduction ratio* of a cryptographic circuit that employs a VFS-based countermeasure with on-chip voltage regulation.

A low power and small area substitution-box (S-box) from [80] is implemented at the 130nm CMOS technology node and utilized as the cryptographic circuit under attack. The correlation coefficient reduction ratio that is achieved when different countermeasures are employed to protect the S-box is shown in Fig. 7.10. The S-box that employs an SC converter based RDVFS technique exhibits the highest correlation coefficient reduction ratio under the same variance of V_{dd} . The security implications of the number of (f_c, V_{dd}) pairs N are investigated. As shown Fig. 7.11, the number of possible (f_c, V_{dd}) pairs N has a negligible impact on the correlation coefficient reduction ratio of an S-box that employs RDVFS technique with an SC converter. Additionally, when the variance of V_{dd} exceeds $0.04V^2$, the correlation coefficient reduction ratio of an S-box that employs RDVFS technique with an SC converter starts converging, as shown in Fig. 7.10. A higher variance of V_{dd} causes increased performance degradation for a cryptographic circuit that employs RDVFS technique [8]. Selecting the variance of V_{dd} as $0.04V^2$, therefore, provides a reasonable design tradeoff between security and performance. When the variance of V_{dd} is equal to $0.04V^2$, an S-

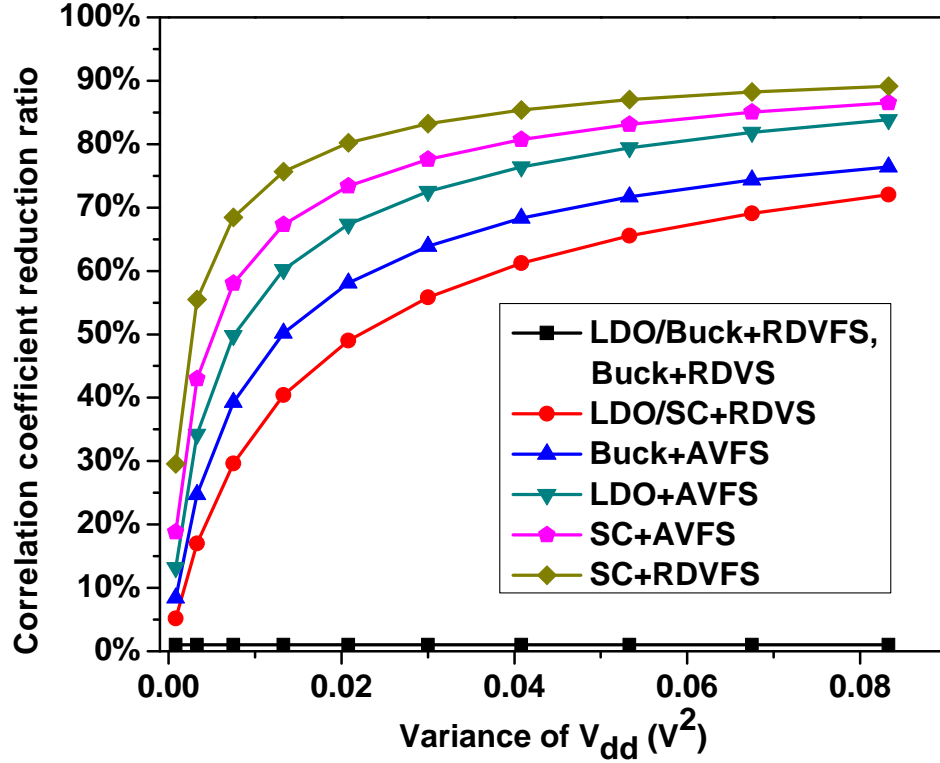


Figure 7.10 Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an-S-box that employs different VFS-based countermeasures (Since a high f_v does not enhance the variance of noise induced by VFS technique, as explained in [7, 8], a moderate voltage scaling frequency of $f_v = 10MHz$ [9] is used for the security analysis to not increase the system design complexity).

box that employs RDVFS technique with an SC converter performs best against DPA attacks as compared to an S-box employs other techniques without significant performance degradation.

Since a true random VFS technique may be difficult to implement in practice, a statistically normally distributed VFS technique is used in the modern processors [94–96]. The detail security analysis of on-chip voltage regulation with normally distributed VFS technique against DPA attacks can be found in Appendix E.

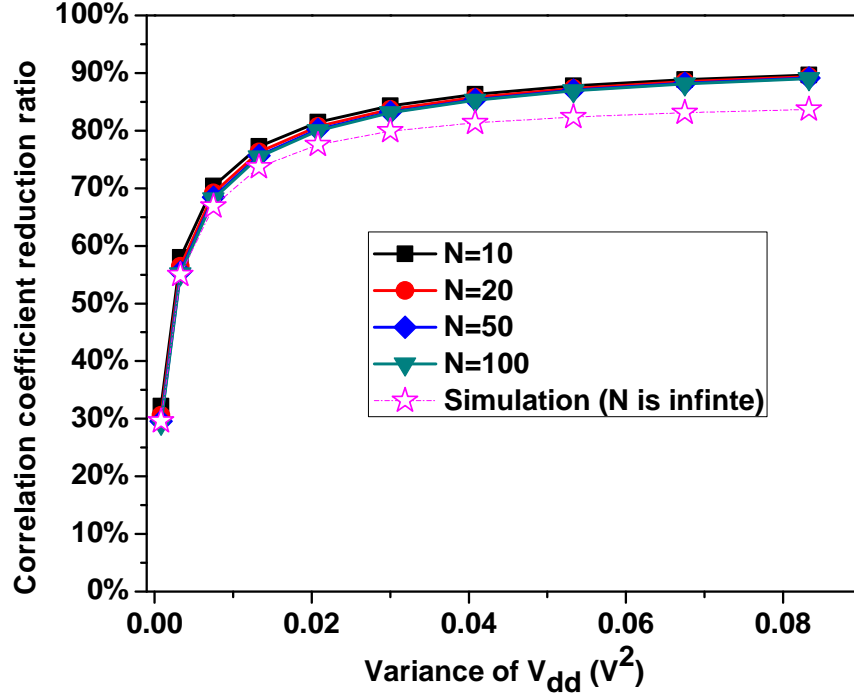


Figure 7.11 Variance of the supply voltage V_{dd} versus the correlation coefficient reduction ratio for an S-box that employs RDVFS technique with an SC converter with various possible (f_c, V_{dd}) pairs.

7.4 Security Evaluation of On-Chip Voltage Regulation with VFS Technique Against LPA Attacks

A leakage power analysis (LPA) attack is a type of side-channel attack, which is utilized by an attacker to leak the secret key by exploiting the correlation between the input data and leakage power dissipation of a cryptographic circuit [3]. The side-channel leakage current of a cryptographic circuit I_{leak} can be denoted as [3]

$$I_{leak} = \omega I_H + (m - \omega) I_L, \quad (7.27)$$

where ω is the hamming weight of input data and m is the number of bits in the input data. $I_H(I_L)$ is the leakage current when the input bit is high (low). Since $I_H(I_L)$ is a function of the supply

Table 7.2 Inserted Noise $M_{j,k}(V_{dd})$, ($j, k = 1, 2, 3$) into the Power Consumption Profile of a Cryptographic Circuit through Countermeasures that Employ Different Voltage Regulators against LPA Attacks.

Regulator Technique	LDO regulator	Buck converter	SC converter
RDVFS	$M_{1,1}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$	$M_{1,2}(V_{dd})$ $= 0$	$M_{1,3}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$
RDVS	$M_{2,1}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$	$M_{2,2}(V_{dd})$ $= 0$	$M_{2,3}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$
AVFS	$M_{3,1}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$	$M_{3,2}(V_{dd})$ $= 0$	$M_{3,3}(V_{dd})$ $= \log(V_{dd}) + 1.19V_{dd}$

voltage V_{dd} [97], the leakage power dissipation P_{leak} of a cryptographic circuit can be written as

$$\begin{aligned}
 P_{leak} &= V_{dd}I_{leak} \\
 &= V_{dd}(\omega I_H(V_{dd}) + (m - \omega)I_L(V_{dd})) \\
 &= V_{dd}I_{leak,0}K(V_{dd}),
 \end{aligned} \tag{7.28}$$

where $I_{leak,0}$ is the component of leakage current which is independent of the supply voltage V_{dd} and $K(V_{dd})$ is the component of leakage current which is strongly correlated with V_{dd} .

In sub-micro CMOS integrated circuits (ICs), the relationship between the leakage current of the CMOS ICs and supply voltage V_{dd} can be approximated as an exponent relationship ($I_{leak} = I_{leak,0}K(V_{dd}) \approx I_{leak,0}exp(aV_{dd})$) [97]. In order to determine the value of the parameter a , two different input data patterns (input data₁ and input data₂) are applied to a 130nm CMOS based S-box [80]. The simulated relationship between the leakage current and supply voltage V_{dd} is shown in Fig. 7.12. We use two different exponent functions $K_1(V_{dd}) = b_1exp(aV_{dd})$ and $K_2(V_{dd}) = b_2exp(aV_{dd})$ to curve-fit the relationship between the leakage current and supply voltage V_{dd} induced by input data₁ and input data₂, respectively. After fitting as shown in Fig. 7.12, the expressions

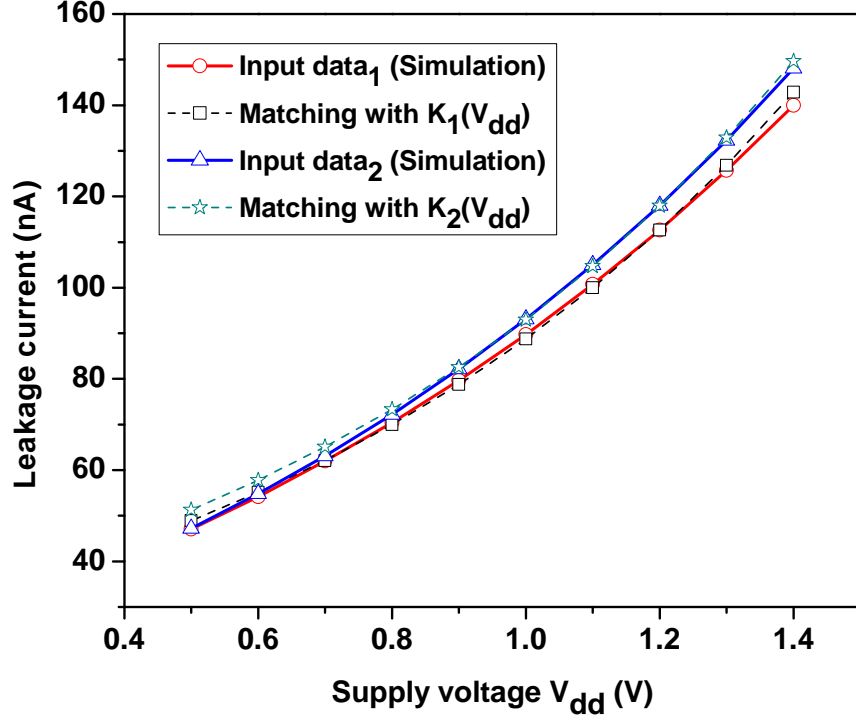


Figure 7.12 Supply voltage V_{dd} versus leakage current of an S-box implemented in 130nm CMOS technology under two different input data.

of $K_1(V_{dd})$ and $K_2(V_{dd})$ can be respectively determined as

$$K_1(V_{dd}) = 27 \times \exp(1.19 \times V_{dd}) \approx 27K(V_{dd}), \quad (7.29)$$

$$K_2(V_{dd}) = 28.29 \times \exp(1.19 \times V_{dd}) \approx 28.29K(V_{dd}). \quad (7.30)$$

Therefore, the leakage power dissipation of the S-box P_{leak} can be denoted as

$$\begin{aligned} P_{leak} &= V_{dd} I_{leak,0} K(V_{dd}), \\ &\approx V_{dd} \times I_{leak,0} \times \exp(1.19 \times V_{dd}). \end{aligned} \quad (7.31)$$

After taking logarithm of both sides, (7.31) becomes

$$\log(P_{leak}) \approx \log(I_{leak,0}) + \log(V_{dd}) + 1.19V_{dd}, \quad (7.32)$$

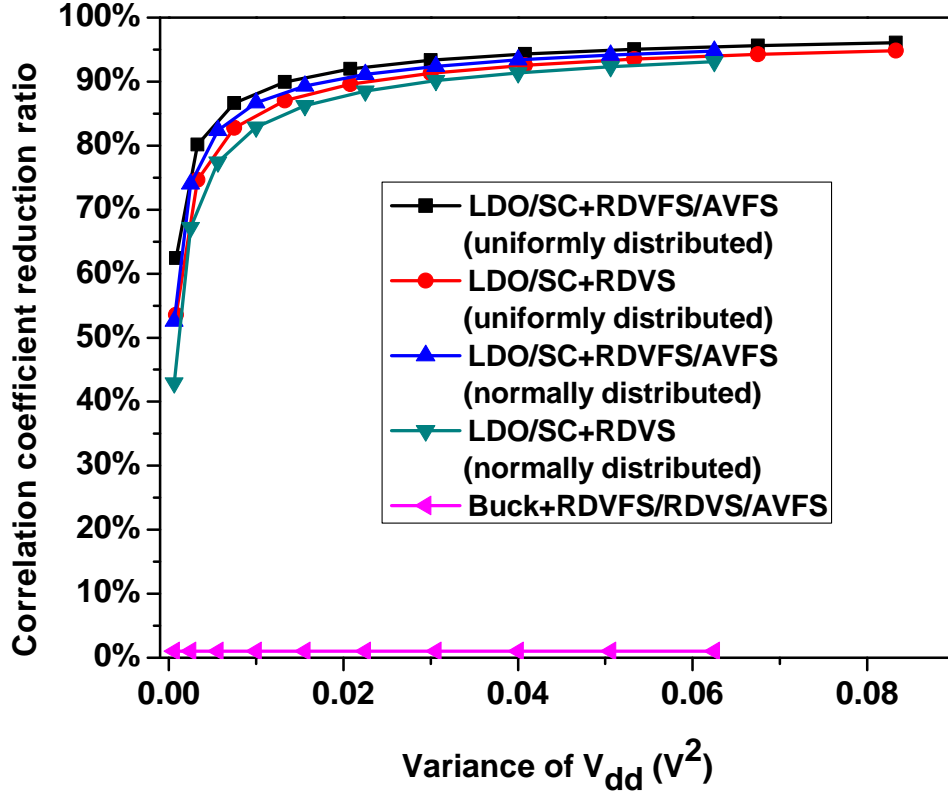


Figure 7.13 Variance of supply voltage V_{dd} versus the correlation coefficient reduction ratio of an S-box that employs different countermeasures ($f_v = 10MHz$ and $N = 50$).

where $\log(I_{leak,0})$ is the side-channel signal which may provide useful information under an LPA attack. The characteristics of the inserted noise $M_{j,k}(V_{dd})$ to an S-box through different countermeasures against LPA attacks are listed in Table 7.2. Since a buck converter leaks the supply voltage V_{dd} from the slope of input power, the uncertain noise $M_{j,2}(V_{dd})$ that is inserted by a buck converter based VFS technique becomes zero.

As shown in Fig. 7.13, an S-box that employs the RDVFS technique with an SC converter can achieve a correlation coefficient reduction ratio of over 90% when the variance of supply voltage V_{dd} is greater than $0.04V^2$.

7.5 Overhead Analysis

The power overhead of several VFS-based countermeasures with on-chip voltage regulation is summarized in Table 7.3. An S-box [80] that houses an SC voltage converter exhibits the

Table 7.3 Correlation Coefficient Reduction Ratio (CCRR), Dynamic Power (D-Power) Consumption, and Leakage Power (L-Power) Consumption of an S-Box that Houses On-Chip Voltage Regulators Implemented with True Random and Normally Distributed VFS-based Countermeasures against DPA and LPA Attacks (Supply Voltage Range $V_{DD2} - V_{DD1} = 0.7V$), X_d and X_l Are, Respectively, the Dynamic and Leakage Power Consumption of an S-box without any Countermeasure (Detail Explanation can be Found in Appendix D).

	DPA attacks				LPA attacks			
	True random		Normally distributed		True random		Normally distributed	
	CCRR	D-Power	CCRR	D-Power	CCRR	L-Power	CCRR	L-Power
LDO+RDVFS	0	0.746X_d	0	0.692X_d	94.3%	0.7116X_l	92.41%	0.6948X_l
Buck+RDVFS	0	0.746X_d	0	0.692X_d	0	0.7116X_l	0	0.6948X_l
SC+RDVFS	85.41%	0.746X_d	80.94%	0.692X_d	94.3%	0.7116X_l	92.41%	0.6948X_l
LDO+RDVS	61.2%	2.0391X_d	51.07%	2.0195X_d	92.56%	2.7274X_l	90.14%	2.6820X_l
Buck+RDVS	0	2.0391X_d	0	2.0195X_d	0	2.7274X_l	0	2.6820X_l
SC+RDVS	61.2%	2.0391X_d	51.07%	2.0195X_d	92.56%	2.7274X_l	90.14%	2.6820X_l
LDO+AVFS	76.43%	0.6097X_d	69.07%	0.5427X_d	94.3%	0.7116X_l	92.41%	0.6948X_l
Buck+AVFS	68.32%	0.6097X_d	59.52%	0.5427X_d	0	0.7116X_l	0	0.6948X_l
SC+AVFS	80.74%	0.6097X_d	77.31%	0.5427X_d	94.3%	0.7116X_l	92.41%	0.6948X_l

highest correlation coefficient reduction ratio (CCRR) of about 85.41% (80.94%) with true random (normally distributed) RDVFS technique under DPA attacks and about 94.3% (92.41%) with true random (normally distributed) RDVFS technique under LPA attacks. The corresponding dynamic power (D-Power) consumption of the S-box is $0.746X_d$ ($0.692X_d$) with true random (normally distributed) RDVFS technique whereas the corresponding leakage power (L-Power) dissipation is $0.7116X_l$ ($0.6948X_l$) with true random (normally distributed) RDVFS technique. X_d represents the dynamic power consumption of an S-box without any countermeasure and X_l is the leakage power dissipation of an S-box without any countermeasure. A detailed explanation of power consumption overhead of different techniques tabulated in Table 7.3 can be found in Appendix D.

There are two main sources of the additional area overhead that need to be considered for an S-box that employs a VFS technique with an on-chip voltage regulator: area overhead induced by on-chip voltage regulator and area overhead induced by VFS technique. Since an on-chip voltage

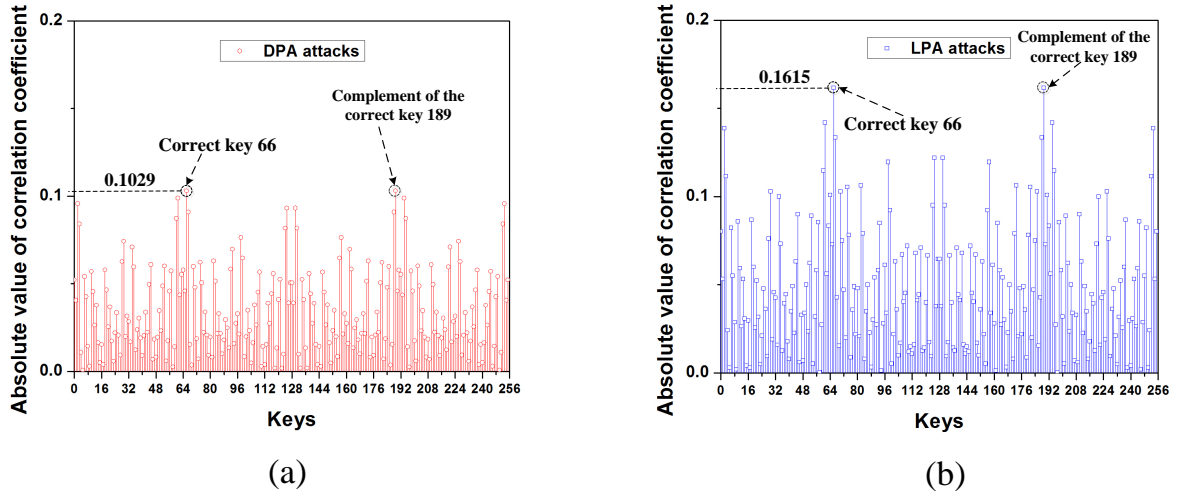


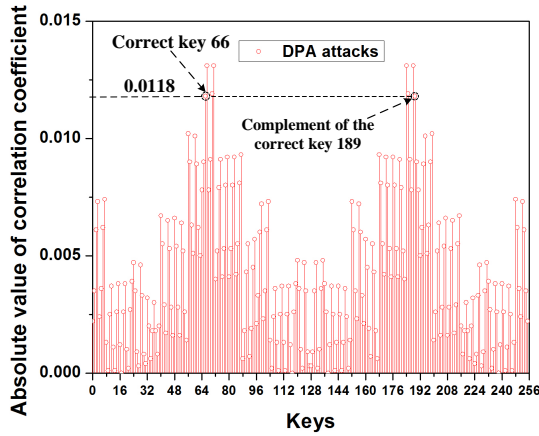
Figure 7.14 Absolute value of the correlation coefficient versus all of the possible keys after inputting 1,000 plaintexts with the hamming-weight model: (a) An S-box without countermeasure under DPA attacks and (b) An S-box without countermeasure under LPA attacks.

regulator utilized to generate fast VFS [71] causes less than 1% area overhead [91], the area overhead induced by on-chip voltage regulator can be neglected. The VFS techniques, RDVFS and RDVS, would not cause extra area overhead based on the analysis provided in [7, 8]. AVFS technique, however, has a 3% area overhead induced by the redundant register duplication to minimize the circuit contamination delay [8].

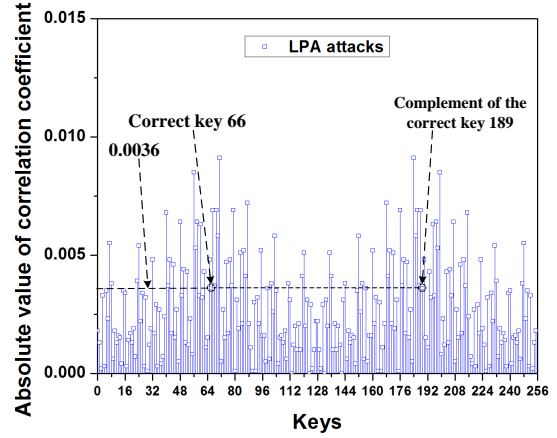
7.6 DPA and LPA Attack Simulations

DPA and LPA attacks are performed in Cadence on two different S-boxes that are implemented at 130nm CMOS technology: one S-box [80] without any countermeasure and another S-box [80] that employs a true random RDVFS technique with an SC converter. As shown in Fig. 7.14, the correct key³ of the S-box without countermeasure can be obtained by performing DPA attacks or LPA attacks after inputting 1,000 plaintexts. However, the correlation coefficient of the correct key under LPA attacks is higher than the correlation coefficient of the correct key

³In hamming-weight model, the correlation coefficient distinction between the correct key and complement of the correct key is the polarity [3]. The correlation coefficient of the correct key is positive, while the correlation coefficient of the complement of the correct key is negative. In order to make the highest correlation coefficient more obvious, in Fig. 7.14 and Fig. 7.15, we normalized all of the correlation coefficients with absolute values.



(a)



(b)

Figure 7.15 Absolute value of correlation coefficient versus all the possible keys after inputting 1 million plaintexts with hamming-weight model ($V_{DD2} - V_{DD1} = 0.7V$): (a) An S-box that employs RDVFS technique with an SC converter under DPA attacks and (b) An S-box that employs RDVFS technique with an SC converter under LPA attacks.

under DPA attacks. This can be interpreted as LPA attacks are able to leak a higher amount of critical information from the S-box as compared to DPA attacks when there is no countermeasure.

In the second experiment, DPA and LPA attacks are performed against an S-box that employs a true random RDVFS technique with an SC converter. After inputting one million plaintexts, neither DPA nor LPA attacks are able to fetch the correct key as shown in Fig. 7.15. However, the correlation coefficient of the correct key under LPA attacks is much lower than the correlation coefficient of the correct key under DPA attacks when RDVFS technique with an SC converter is enabled. This behavior indicates that LPA attacks are more sensitive to noise.

After inputting one million plaintexts to the S-box that employs a true random RDVFS technique with an SC converter, the correlation coefficient reduction ratio of the correct key is 88.53% (97.77%) under DPA (LPA) attacks. These values are higher than the theoretical values of 85.41% (94.3%) which are listed in Table 7.3. An intuitive explanation is provided below.

- The theoretical values tabulated in Table 7.3 are the correlation coefficient reduction ratios of an S-box that employs different countermeasures assuming that the attacker can apply any number of attacks until the secret key within the S-box is obtained (i.e. more than one million plaintexts). However, in DPA and LPA attack simulations, we applied one million plaintexts

and the S-box that employs a true random RDVFS technique with an SC converter could not be cracked after inputting one million plaintexts as shown in Fig. 7.15. This indicates the presence of significant amount of noise in the S-box. If more plaintexts are applied to filter the noise, the correlation coefficient of the correct key would be enhanced and the correlation coefficient reduction ratio would decrease, approaching the theoretical value.

7.7 Conclusion

The security implications of different on-chip voltage regulator topologies implemented within various voltage/frequency scaling-based countermeasures such as RDVFS, RDVS, and AVFS techniques against power analysis attacks are investigated. The side-channel leakage mechanisms of three widely used on-chip voltage regulator topologies are investigated. The security impact of on-chip voltage regulators is evaluated based on the correlation coefficient between the input data and monitored power consumption of a cryptographic circuit. Correlation coefficient reduction ratio is proposed to simplify the security evaluation. RDVFS technique implemented with a switched-capacitor voltage converter can reduce correlation coefficient over 80% (92%) against DPA (LPA) attacks and the measurement-to-disclose (MTD) value is enhanced over 1 million by masking the clock frequency, supply voltage, and dynamic power consumption information from a malicious attacker.

CHAPTER 8: CONCLUSION

On-chip voltage regulation can be utilized as a lightweight and efficient countermeasure against power analysis attacks. Converter-reshuffling (CoRe) voltage converter utilizes a pseudo-random number generator (PRNG) to increase the input power trace entropy against DPA attacks. Time-delayed CoRe voltage converter eliminates the risk of having a zero input power trace entropy against machine learning-based DPA attacks by delaying half of phases with a certain time period. However, charge-withheld CoRe voltage converter further enhances the input power trace entropy against DPA attacks through utilizing two PRNGs to control the charging and discharging of flying capacitors.

As compared to a substitution-box (S-box) without employing on-chip voltage regulation, the measurement-to-disclose (MTD) value is enhanced about 71.4 times against DPA attacks if CoRe voltage converter is utilized to power an S-box. When a conventional AES engine employs a centralized CoRe voltage converter, the MTD value is enhanced over 544 times against DPA attacks. However, when CoRe voltage converter is co-designed with an improved AES engine, the MTD value can be enhanced over 9,100 times against DPA attacks by reshuffling the power noise generated from the S-boxes which are not under DPA attacks.

If the CoRe voltage converter is designed with security adaptive mode, the MTD value is enhanced over 6,145 times against LPA attacks through activating the discharging resistor to scramble the input power profile when LPA attacks are sensed. As shown in the simulation results, when an S-box is powered by a security-adaptive (SA) voltage converter, the MTD value of the S-box is over 2 million against LPA attacks. By contrast, the MTD value of an S-box without countermeasure is less than 500.

Additionally, if conventional switched-capacitor (SC) converter employs random dynamic voltage and frequency scaling (RDVFS), the correlation coefficient between the input data and monitored power dissipation reduces over 80 (92) percent against DPA (LPA) attacks. As demonstrated in the simulations, the MTD value of an S-box that employs RDVFS with an SC converter is over 1 million against both DPA and LPA attacks by masking the leakage of the clock frequency and supply voltage information in the input power profile. However, for an S-box without countermeasure, the MTD value is less than 1,000 against both DPA and LPA attacks.

CHAPTER 9: FUTURE WORK

9.1 Utilizing On-Chip Multi-Phase Buck Converter as a Countermeasure Against Electro-Magnetic (EM) Attacks

In my previous research works [11, 54, 56, 59, 82, 87], we mainly utilized on-chip multi-phase switched-capacitor (SC) converter to mask the actual power dissipation of the cryptographic circuit from a malicious attacker in the input power profile against power analysis attacks. However, as shown in Fig. 9.1, the attacker may bypass the on-chip voltage regulator and implement electro-magnetic (EM) attacks on the cryptographic circuit directly. The attacker may use a near-field or far-field probe to capture the EM emissions radiated from the cryptographic circuit and exploit the correlation between the input data and EM emissions leaked from the cryptographic circuit. As a result, a cryptographic circuit with on-chip multi-phase SC converter may still be vulnerable against EM attacks.

To protect a cryptographic circuit against EM attacks, a multi-phase buck converter can be utilized to co-design with the cryptographic circuit. The EM radiation from an inductor is significantly stronger than a capacitor [98]. Therefore, as shown in Fig. 9.2, all the inductors in the multi-phase buck converter can be uniformly distributed among the cryptographic circuit in the layout. Under such condition, with the impact of pseudo-random number generator (PRNG), the random EM emissions radiated from randomly reshuffled inductors in each switching period can act as noise to reduce the signal-to-noise ratio (SNR) significantly against EM attacks.

Although multi-phase buck converter can be utilized as a countermeasure against EM attacks, if the attacker implements power analysis attacks and EM attacks on a cryptographic circuit with on-chip multi-phase buck converter simultaneously, the secret key in the cryptographic circuit

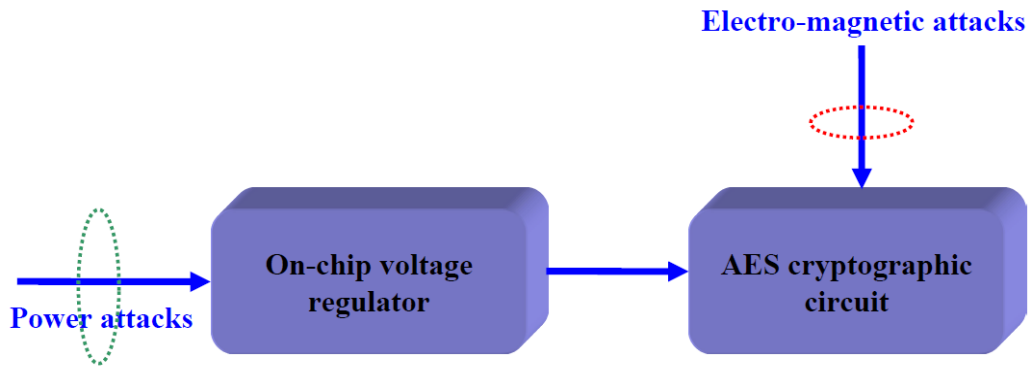


Figure 9.1 Attacker can bypass the on-chip voltage regulator and implement EM attacks directly.

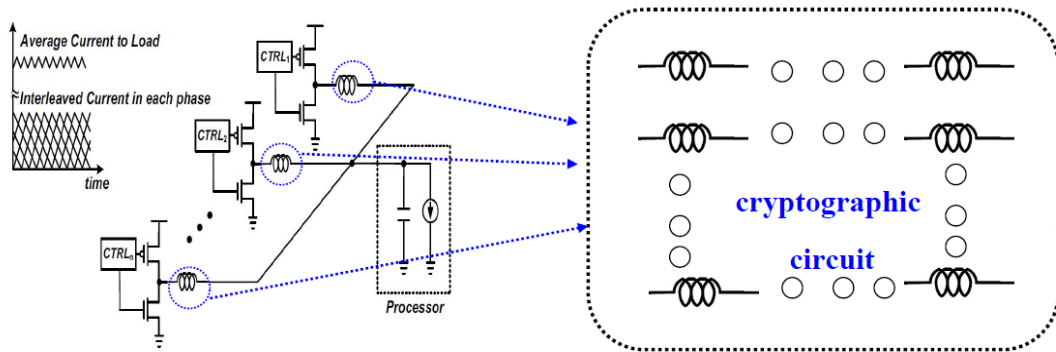


Figure 9.2 Distribute inductors of multi-phase buck converter uniformly among the cryptographic circuit in the layout.

may still can be leaked to the malicious attacker. The reason is that the EM emissions radiated from inductors may leak the critical information about PRNG if EM attacks are implemented, the leaked critical information about PRNG may be utilized by the attacker to eliminate the power noise generated by PRNG to execute power analysis attacks successfully. Therefore, in future research, the joint EM attacks and power analysis attacks also need to be considered for securing a cryptographic circuit with on-chip voltage regulators.

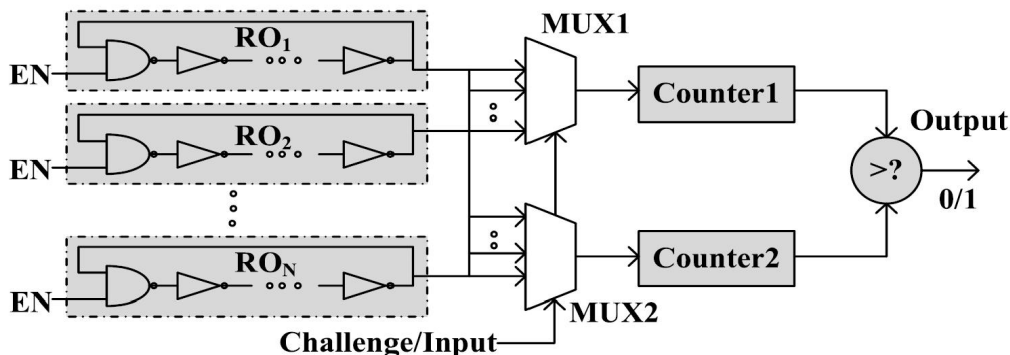


Figure 9.3 Architecture of conventional RO PUF in [10].

9.2 Utilizing On-Chip Multi-Phase SC Converter as a Physical Unclonable Function (PUF)

Physical unclonable function (PUF) utilizes the random variations in physical materials to generate non-duplicated signatures for cryptography [10, 99, 100]. Currently, generating lightweight PUFs are extremely crucial for securing internet of things (IoT) [100, 101]. All the existing PUFs can be categorized as weak PUFs and strong PUFs [102]. Weak PUFs only generate a few signatures or even a single signature, which can be utilized for authentication [99]. Ring-oscillator (RO) PUF is a popular and lightweight weak PUF [10, 100, 101], which utilizes the oscillating frequency mismatch induced by the random process variations in two identical CMOS RO loops. The multiplexers are used to record the number of RO loops with a higher oscillating frequency to generate a unique binary secret data [10, 100, 101], as shown in Fig. 9.3¹.

Other than the RO PUF, several other lightweight weak PUFs: coating PUF [103], cross-coupled logic gates [104], SRAM-PUF [105], buskeeper-PUF [106], and DAC-PUF [99] also have been proposed over the past decade. However, to the best of our knowledge, on-chip voltage regulator PUF (VR-PUF) has not been studied yet.

In a multi-phase SC converter, the random fabricating process variations would make the flying capacitors in each sub-phase have different capacitance mismatches. When the multi-phase SC converter is powered, the input power signature would become unique and non-duplicate due

¹Copyright permission can be found in Appendix F.

to the random flying capacitance in each sub-phase. For instance, in a 16-phase SC converter, assume six phases are activated to provide power to the load and the sequence of active phases is #2-#4-#5-#8-#12-#15. If another 16-phase SC converter is designed with the same parameter and same sequence of active phases, the input power signatures of those two 16-phase SC converters are different due to the impact of random capacitance variations in the flying capacitors.

Since there is a PRNG in the multi-phase SC converter, when the sequence of active phases is reshuffled by the PRNG, the multi-phase SC converter would generate another different input power profile. Therefore, with the impact of PRNG, multi-phase SC converter also can be designed as strong PUFs since a large amount of different input power signatures can be achieved. In future research, intra-HD and inter-HD will be the two vital parameters to evaluate the proposed VR-PUF. For a perfect weak PUF, the intra-HD should be 0% and inter-HD should be 50% [99]. In addition, if the proposed VR-PUF is applied as a strong PUF, the challenge-response-pairs (CRP) [99, 102] need to be considered to evaluate how many different signatures can VR-PUF output.

REFERENCES

- [1] D. Oswald and R.-U. Bochum, "ID and IP theft with side-channel attacks," 2014. [Online]. Available: <http://www.slideshare.net/phdays/1300-david-oswald-id-and-ip-theft-with-sidechannel-attacks>.
- [2] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A low overhead DPA countermeasure circuit based on ring oscillators," *IEEE Transactions on Circuits and System II: Express Briefs*, vol. 57, no. 7, pp. 546–550, Jul. 2010.
- [3] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.
- [4] O. A. Uzun and S. Kose, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 169–179, Jun. 2014.
- [5] Y. Wang and Y. Ha, "FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network," *IEEE Transactions on Circuits and System II: Express Briefs*, vol. 60, no. 1, pp. 36–40, Jan. 2013.
- [6] F. Regazzoni, Y. Wang, and F. X. Standaert, "Fault attack for the iterative operation of AES S-Box," in *Proc. Constructive Side-Channel Analysis and Secure Design (COSADE)*, Feb. 2011, pp. 56–66.
- [7] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," in *Proc. VLSI design*, Jan. 2007, pp. 854–862.
- [8] N. D. P. Avirneni and A. K. Somani, "Countering power analysis attacks using reliable and aggressive designs," *IEEE Transactions on Computers*, vol. 63, no. 6, pp. 1408–1420, Jun. 2014.
- [9] B. Lee, E. Nurvitadhi, R. Dixit, C. Yu, and M. Kim, "Dynamic voltage scaling techniques for power efficient video decoding," *the EUROMICRO Journal*, vol. 51, no. 10, pp. 633–652, 2005.
- [10] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335–348, Sep. 2016.
- [11] W. Yu and S. Kose, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," in *Proc. Design Automation Conference (DAC)*, Jun. 2015, pp. 1–6.

- [12] M. Arora, “How secure is AES against brute force attacks?” 2012. [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1279619.
- [13] W. Yu and S. Kose, “A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks,” *IEEE Transactions on Circuits and System I: Regular Papers*, in press.
- [14] P. Rakers, L. Connell, T. Collins, and D. Russell, “Secure contactless smartcard ASIC with DPA protection,” *IEEE Journal of Solid-State Circuits*, vol. 36, no. 3, pp. 559–565, Mar. 2001.
- [15] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, “Power-gated MOS current mode Logic (PG-MCML): A power aware DPA-resistant standard cell library,” in *Proc. Design Automation Conference (DAC)*, May 2011, pp. 1014–1019.
- [16] W. Cilio, M. Linder, C. Porter, J. Di, D. R. Thompson, and S. C. Smith, “Mitigating power- and timing-based side-channel attacks using dual-spacer dual-rail delay-insensitive asynchronous logic,” *Microelectronics Journal*, vol. 44, no. 3, pp. 258–269, Mar. 2013.
- [17] J. A. Ambrose, R. G. Ragel, and S. Parameswaran, “Randomized instruction injection to counter power analysis attacks,” *ACM Transactions on Embedded Computing Systems*, vol. 11, no. 3, pp. 69:1–69:28, Mar. 2012.
- [18] C. Clavier, J.-S. Coron, and N. Dabbous, Eds., *Differential power analysis in the presence of hardware countermeasures*. Springer, 2000.
- [19] W. Yu and S. Kose, “Security implications of simultaneous dynamic and leakage power analysis attacks on nanoscale cryptographic circuits,” *IET Electronics Letters*, vol. 52, no. 6, pp. 466–468, Mar. 2016.
- [20] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” *Journal of Cryptographic Engineering*, vol. 1, no. 1, pp. 5–27, 2011.
- [21] S. Yang, W. Wolf, N. Vijaykrishnan, D. Serpanos, and Y. Xie, “Power attack resistant cryptosystem design: A dynamic voltage and frequency switching approach,” in *Proc. Design, Automation and Test in Europe (DATE)*, Mar. 2005, pp. 64–69.
- [22] W. Yu and S. Kose, “False key-controlled aggressive voltage scaling: A countermeasure against LPA attacks,” *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, in press.
- [23] S. Kose and E. G. Friedman, “An area efficient fully monolithic hybrid voltage regulator,” in *Proc. ISCAS*, May 2010, pp. 2718–2721.
- [24] I. Vaisband, B. Price, S. Kose, Y. Kolla, E. G. Friedman, and J. Fischer, “Distributed LDO regulators in a 28 nm power delivery system,” *Analog Integrated Circuits and Signal Processing*, vol. 83, no. 3, pp. 295–309, 2015.
- [25] S. Kose and E. G. Friedman, “Fast algorithms for power grid analysis based on effective resistance,” in *Proc. ISCAS*, May 2010, pp. 3661–3664.

- [26] I. Vaisband, M. Azhar, E. G. Friedman, and S. Kose, "Digitally controlled pulse width modulator for on-chip power management," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 12, pp. 2527–2534, Dec. 2014.
- [27] S. Kose and E. G. Friedman, "On-chip point-of-load voltage regulator for distributed power supplies," in *Proc. GLVLSI*, May 2010, pp. 377–380.
- [28] S. Kose, E. Salman, and E. G. Friedman, "Shielding methodologies in the presence of power/ground noise," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 19, no. 8, pp. 1458–1468, Aug. 2011.
- [29] S. Kose and E. G. Friedman, "Effective resistance of a two layer mesh," *IEEE Transactions on Circuits and System II: Express Briefs*, vol. 58, no. 11, pp. 739–743, Nov. 2011.
- [30] S. Kose, I. Vaisband, and E. G. Friedman, "Digitally controlled wide range pulse width modulator for on-chip power supplies," in *Proc. ISCAS*, May 2013, pp. 2251–2254.
- [31] S. Kose and E. G. Friedman, "Distributed power delivery for energy efficient and low power systems," in *Proc. Signals, Systems, and Computers*, Nov. 2012, pp. 757–761.
- [32] S. Kose, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "An area efficient on-chip hybrid voltage regulator," in *Proc. ISQED*, Mar. 2012, pp. 398–403.
- [33] S. Kose and E. G. Friedman, "Fast algorithms for IR voltage drop analysis exploiting locality," in *Proc. Design Automation Conference (DAC)*, Jun. 2011, pp. 996–1001.
- [34] I. Savidis, S. Kose, and E. G. Friedman, "Power grid noise in TSV-based 3-D integrated systems," in *Proc. Government Microcircuit Applications and Critical Technology*, Mar. 2011, pp. 129–132.
- [35] S. Kose and E. G. Friedman, "Distributed power network co-design with on-chip power supplies and decoupling capacitors," in *Proc. System Level Interconnect Prediction (SLIP)*, Jun. 2011.
- [36] S. Kose, E. Salman, and E. G. Friedman, "Shielding methodologies in the presence of power/ground noise," in *Proc. ISCAS*, May 2009, pp. 2277–2280.
- [37] S. Kose and E. G. Friedman, "Design methodology to distribute on-chip power in next generation integrated circuits," in *Proc. SoC*, Sep. 2010, pp. 15–18.
- [38] M. J. Azhar and S. Kose, "An enhanced pulse width modulator with adaptive duty cycle and frequency control," in *Proc. ISCAS*, May 2014, pp. 958–961.
- [39] I. Savidis, S. Kose, and E. G. Friedman, "Power noise in TSV-based 3-D integrated circuits," *IEEE Journal of Solid-State Circuits*, vol. 48, no. 2, pp. 587–597, Feb. 2013.
- [40] S. Kose, "Thermal implications of on-chip voltage regulation: Upcoming challenges and possible solutions," in *Proc. Design Automation Conference (DAC)*, Jun. 2014, pp. 1–6.
- [41] O. A. Uzun and S. Kose, "Regulator-gating methodology with distributed switched capacitor voltage converters," in *Proc. ISVLSI*, Jul. 2014, pp. 13–18.

- [42] S. Kose, “Regulator-gating: Adaptive management of on-chip voltage regulators,” in *Proc. GLVLSI*, May 2014, pp. 105–110.
- [43] Y. K. Ramadass, A. A. Fayed, and A. P. Chandrakasan, “A fully-integrated switched-capacitor step-down DC-DC converter with digital capacitance modulation in 45 nm CMOS,” *IEEE Journal of Solid-State Circuits*, vol. 45, no. 12, pp. 2557–2565, Dec. 2010.
- [44] E. Alon and M. Horowitz, “Integrated regulation for energy-efficient digital circuits,” *IEEE Journal of Solid-State Circuits*, vol. 43, no. 8, pp. 1795–1807, Aug. 2008.
- [45] W. Kim, M. S. Gupta, G.-Y. Wei, and D. Brooks, “System level analysis of fast, per-core DVFS using on-chip switching regulators,” in *Proc. High Performance Computer Architecture (HPCA)*, Feb. 2008, pp. 123–134.
- [46] L. Benini, A. Bogliolo, and G. D. Micheli, “A survey of design techniques for system-level dynamic power management,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 8, no. 3, pp. 299–316, Mar. 2000.
- [47] V. Kursun and E. G. Friedman, Eds., *Multi-voltage CMOS circuit design*. John Wiley & Sons, 2006.
- [48] G. R. Mora, Ed., *Analog IC design with low-dropout regulators (LDOs)*. McGraw-Hill Publishers, 2009.
- [49] C. F. Lee and P. K. Mok, “A monolithic current-mode CMOS DC-DC converter with on-chip current-sensing technique,” *IEEE Journal of Solid-State Circuits*, vol. 39, no. 1, pp. 3–14, Jan. 2004.
- [50] V. Kursun, S. G. Narendra, V. K. De, and E. G. Friedman, “Analysis of buck converters for on-chip integration with a dual supply voltage microprocessor,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 11, no. 3, pp. 514–522, Jun. 2003.
- [51] G. A. R. Mora, Ed., *Current efficient, low voltage, low drop-out regulators*. Ph.D. thesis, Georgia Institute of Technology, 1996.
- [52] T. M. A. *et al.*, “A 4.6 W/mm² power density 86% efficiency on-chip switched capacitor DC-DC converter in 32 nm SOI CMOS,” in *Proc. Applied Power Electronics Conference and Exposition*, Mar. 2013, pp. 692–699.
- [53] B. Kopf and D. Basin, “An information-theoretic model for adaptive side-channel attacks,” in *Proc. Computer and communications security (CCS)*, Oct. 2007, pp. 286–296.
- [54] W. Yu and S. Kose, “Time-delayed converter-reshuffling: An efficient and secure power delivery architecture,” *IEEE Embedded Systems Letters*, vol. 7, no. 3, pp. 73–76, Sep. 2015.
- [55] H. Maghrebi, S. Guilley, J. L. Danger, and F. Flament, “Entropy-based power attack,” in *Proc. Hardware-Oriented Security and Trust (HOST)*, Jun. 2010, pp. 1–6.
- [56] W. Yu and S. Kose, “Charge-withheld converter-reshuffling (CoRe): A countermeasure against power analysis attacks,” *IEEE Transactions on Circuits and System II: Express Briefs*, vol. 63, no. 5, pp. 438–442, May 2016.

- [57] H. Jeon, Ed., *Fully integrated on-chip switched capacitor DC-DC converters for battery-powered mixed-signal SoCs*. Ph.D. thesis, Northeastern Univ., 2012.
- [58] M. D. Seeman, Ed., *A design methodology for switched-capacitor DC-DC converters*. Ph.D. thesis, Univ. of California at Berkeley, 2009.
- [59] W. Yu and S. Kose, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 63, no. 8, pp. 1152–1163, Aug. 2016.
- [60] D. Wu, X. Cui, W. Wei, R. Li, D. Yu, and X. Cui, "Research on circuit level countermeasures for differential power analysis attacks," in *Proc. Solid-State and Integrated Circuit Technology*, Oct. 2012, pp. 1–3.
- [61] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.
- [62] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proc. Design Automation Conference (DAC)*, Jun. 2013, pp. 1–9.
- [63] G. Khedkar, D. Kudithipudi, and G. S. Rose, "Power profile obfuscation using nanoscale memristive devices to counter DPA attacks," *IEEE Transactions on Nanotechnology*, vol. 14, no. 1, pp. 26–35, Jan. 2015.
- [64] F. Regazzoni, T. Eisenbarth, J. Grottschadl, L. Breveglieri, P. Ienne, I. Koren, and C. Paar, "Power attacks resistance of cryptographic S-boxes with added error detection circuits," in *Proc. Defect and Fault-Tolerance in VLSI Systems*, Sep. 2007, pp. 508–516.
- [65] S. Kose, S. Tam, S. Pinzon, B. McDermott, and E. G. Friedman, "Active filter based hybrid on-chip DC-DC converters for point-of-load voltage regulation," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 21, no. 4, pp. 680–691, Apr. 2013.
- [66] J. D. Vos, D. Flandre, and D. Bol, "A sizing methodology for on-chip switched-capacitor DC/DC converters," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 61, no. 5, pp. 1597–1606, May 2014.
- [67] Y. Lu, Y. Wang, Q. Pan, W.-H. Ki, and C. P. Yue, "A fully-integrated low-dropout regulator with full-spectrum power supply rejection," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 62, no. 3, pp. 707–716, Mar. 2015.
- [68] S.-W. Hong and G.-H. Cho, "High-gain wide-bandwidth capacitor-less low-dropout regulator (LDO) for mobile applications utilizing frequency response of multiple feedback loops," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 63, no. 1, pp. 46–57, Jan. 2016.
- [69] Z. Toprak-Deniz, M. Sperling, J. F. Bulzacchelli, G. Still, R. Kruse, S. Kim, D. Boerstler, T. Gloekler, R. Robertazzi, K. Stawiasz, T. Diemoz, G. English, D. Hui, P. Muench, and J. Friedrich, "Distributed system of digitally controlled microregulators enabling per-core DVFS for the POWER8™ microprocessor," in *Proc. IEEE International Solid-State Circuits Conference (ISSCC)*, Feb. 2014, pp. 98–99.

- [70] S. Kose and E. G. Friedman, “Distributed on-chip power delivery,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 2, no. 4, pp. 704–713, Dec. 2012.
- [71] P. Zhou, A. Paul, C. H. Kim, and S. S. Sapatnekar, “Distributed on-chip switched-capacitor DC-DC converters supporting DVFS in multicore systems,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 9, pp. 1954–1967, Sep. 2014.
- [72] A. Hodjat and I. Verbauwhede, “Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors,” *IEEE Transactions on Computers*, vol. 55, no. 4, pp. 366–372, Apr. 2006.
- [73] F. Wu, L. Wang, and J. Wan, “A low cost and inner-round pipelined design of ECB-AES-256 crypto engine for solid state disk,” in *Proc. Networking, Architecture and Storage (NAS)*, Jul. 2010, pp. 485–491.
- [74] T. Good and M. Benaissa, “Very small FPGA application-specific instruction processor for AES,” *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 53, no. 7, pp. 1477–1486, Jul. 2006.
- [75] F. Standaert, E. Peeters, G. Rouvroy, and J. Quisquater, “An overview of power analysis attacks against field programmable gate arrays,” *Proceedings of the IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.
- [76] E. A. Burton, G. Schrom, F. Paillet, J. Douglas, W. J. Lambert, K. Radhakrishnan, and M. J. Hill, “FIVR-Fully integrated voltage regulators on 4th generation Intel Core SoCs,” in *Proc. Applied Power Electronics Conference and Exposition (APEC)*, Mar. 2014, pp. 432–439.
- [77] P. A. Hung, K. Klomkarn, and P. Sooraksa, “Image encryption based on chaotic map and dynamic S-box,” in *Proc. Intelligent Signal Processing and Communications Systems (ISPACS)*, Nov. 2013, pp. 435–439.
- [78] A. Joshi, P. K. Dakhole, and A. Thatere, “Implementation of S-Box for advanced encryption standard,” in *Proc. Engineering and Technology (ICETECH)*, Mar. 2015, pp. 1–5.
- [79] J. Park, S. Moon, D. Choi, Y. Kang, and J. Ha, “Fault attack for the iterative operation of AES S-Box,” in *Proc. Computer Sciences and Convergence Information Technology (ICCIT)*, Nov. 2010, pp. 550–555.
- [80] N. Ahmad and S. M. R. Hasan, “Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using novel XOR gate,” *Integration, the VLSI Journal*, vol. 46, no. 4, pp. 333–344, Sep. 2013.
- [81] N. Kamoun, L. Bossuet, and A. Ghazel, “Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cipher,” in *Proc. Signals, Circuits and Systems (SCS)*, Nov. 2009, pp. 1–6.
- [82] W. Yu and S. Kose, “Security-adaptive voltage conversion as a lightweight countermeasure against LPA attacks,” *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, in press.

- [83] S. M. D. Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, “Side-channel attacks from static power: When should we care?” in *Proc. Design, Automation and Test in Europe (DATE)*, Mar. 2015, pp. 145–150.
- [84] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, “Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations,” *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 61, no. 2, pp. 429–442, Feb. 2014.
- [85] D. D. Huang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, “AES-based security coprocessor IC in 0.18-um CMOS with resistance to differential power analysis side-channel attacks,” *IEEE Journal of Solid-State Circuits*, vol. 41, no. 4, pp. 781–791, Apr. 2006.
- [86] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, “DPA-secured quasi-adiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes,” *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 62, no. 1, pp. 149–156, Jan. 2015.
- [87] W. Yu and S. Kose, “Exploiting voltage regulators to enhance various power attack countermeasures,” *IEEE Transactions on Emerging Topics in Computing*, in press.
- [88] K. Tiri and I. Verbauwhede, “A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation,” in *Proc. Design, Automation and Test in Europe (DATE)*, Feb. 2004, pp. 246–251.
- [89] N. S. Kim, K. Flautner, D. Blaauw, and T. Mudge, “Drowsy instruction caches. Leakage power reduction using dynamic voltage scaling and cache sub-bank prediction,” in *Proc. Microarchitecture*, 2002, pp. 219–230.
- [90] A. Moradi, “Side-channel leakage through static power-Should we care about in practice?-,” in *Proc. Cryptographic Hardware and Embedded Systems*, 2014, pp. 562–579.
- [91] E. J. F. *et al.*, “The 12-Core POWER8 processor with 7.6 Tb/s IO bandwidth, integrated voltage regulation, and resonant clocking,” *IEEE Journal of Solid-State Circuits*, vol. 50, no. 1, pp. 10–23, Jan. 2015.
- [92] X. Qu, Z.-K. Zhou, B. Zhang, and Z.-J. Li, “An ultralow-power fast-transient capacitor-free low-dropout regulator with assistant pushpull output stage,” *IEEE Transactions on Circuits and System II: Express Briefs*, vol. 60, no. 2, pp. 96–100, Feb. 2013.
- [93] S. A. Seyyedi, M. Kamal, H. Noori, and S. Safari, “Securing embedded processors against power analysis based side channel attacks using reconfigurable architecture,” in *Proc. Embedded and Ubiquitous Computing (EUC)*, Oct. 2011, pp. 255–260.
- [94] J. Kim, S. Yoo, and C.-M. Kyung, “Program phase and runtime distribution-aware online DVFS for combined Vdd/Vbb scaling,” in *Proc. Design, Automation and Test in Europe (DATE)*, Apr. 2009, pp. 417–422.
- [95] S. Garg, D. Marculescu, R. Marculescu, and U. Ogras, “Technology-driven limits on DVFS controllability of multiple voltage-frequency island designs: A system-level perspective,” in *Proc. Design Automation Conference (DAC)*, Jul. 2009, pp. 818–821.

- [96] Q. Wu, P. Juang, M. Martonosi, and D. W. Clark, "Voltage and frequency control with adaptive reaction time in multiple-clock-domain processors," in *Proc. High-Performance Computer Architecture*, Feb. 2005, pp. 178–189.
- [97] C. Gopalakrishnan, Ed., *High level techniques for leakage power estimation and optimization in VLSI ASICs*. Ph.D. Dissertation, Univ. of South Florida, 2003.
- [98] H. W. Ott, "Understanding and controlling common-mode emissions in high-power electronics," http://www.hotconsultants.com/pdf_files/APEC-2002.pdf.
- [99] A. Herkle, J. Becker, and M. Ortmanns, "Exploiting weak PUFs from data converter nonlinearity—E.g., a multibit CT $\Delta\Sigma$ Modulator," *IEEE Transactions on Circuits and System I: Regular Papers*, vol. 63, no. 7, pp. 994–1004, Jul. 2016.
- [100] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid RO PUF with improved thermal stability for lightweight applications," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 7, pp. 1143–1147, Jul. 2015.
- [101] D. Yamamoto, M. Takenaka, K. Sakiyama, and N. Torii, "Security evaluation of bistable ring PUFs on FPGAs using differential and linear analysis," in *Proc. Computer Science and Information Systems (FedCSIS)*, Sep. 2014, pp. 911–918.
- [102] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.
- [103] P. Tuyls, G.-J. Schrijen, B. Skoric, J. Geloven, N. Verhaegh, and R. Wolters, "Read-proof hardware from protective coatings," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, Oct. 2006, pp. 369–383.
- [104] Y. Su, J. Holleman, and B. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," *IEEE Journal of Solid-State Circuits*, vol. 43, no. 1, pp. 69–77, Jan. 2008.
- [105] J. Guajardo, S. S. Kumar, G.-J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Proc. Cryptographic Hardware and Embedded Systems (CHES)*, Sep. 2007, pp. 63–80.
- [106] P. Simons, E. v. d. Sluis, and V. v. d. Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in *Proc. HOST*, Jun. 2012, pp. 7–12.

APPENDICES

Appendix A: Correlation Coefficient of Conventional On-Chip Voltage Regulators

If the attacker decides to sample the total input power consumption within K consecutive switching periods as one sample of the power data in a COC VR that provides power to a single S-box, the total sampled input power $P'_{in,n}(K, \theta)$ within K consecutive switching periods is

$$\begin{aligned} P'_{in,n}(K, \theta) &= \left(1 - \frac{\theta}{2\pi} + \frac{\Delta t}{T_s}\right) \frac{j_{n+1}P_0}{\eta_1} \\ &+ \left(\frac{\theta}{2\pi} - \frac{\Delta t}{T_s}\right) \frac{j_{n+K+1}P_0}{\eta_1} + \sum_{u=2}^K \frac{j_{n+u}P_0}{\eta_1}. \end{aligned} \quad (\text{A.1})$$

The mean value of the total sampled input power within K consecutive switching periods of a COC VR $\mu_c(K, \theta)$ is

$$\begin{aligned} \mu_c(K, \theta) &= \left(1 - \frac{\theta}{2\pi} + \frac{\Delta t}{T_s}\right) \mu'_c + \left(\frac{\theta}{2\pi} - \frac{\Delta t}{T_s}\right) \mu'_c \\ &+ (K - 1) \mu'_c = K \mu'_c, \end{aligned} \quad (\text{A.2})$$

where μ'_c is

$$\mu'_c \approx \sum_{j=j_{min}}^{j_{max}} \frac{jP_0\sqrt{M_1}}{\eta_1\sigma_s\sqrt{2\pi}} \exp\left(-\frac{(j \times P_0 - \mu_s)^2}{2\sigma_s^2/M_1}\right). \quad (\text{A.3})$$

The variance of total sampled input power within K consecutive switching periods of a COC VR $\sigma_c^2(K, \theta)$ is

$$\begin{aligned} \sigma_c^2(K, \theta) &= \left(1 - \frac{\theta}{2\pi} + \frac{\Delta t}{T_s}\right) (\sigma'_c)^2 + \left(\frac{\theta}{2\pi} - \frac{\Delta t}{T_s}\right) (\sigma'_c)^2 \\ &+ (K - 1) (\sigma'_c)^2 = K (\sigma'_c)^2, \end{aligned} \quad (\text{A.4})$$

where $(\sigma'_c)^2$ is

$$(\sigma'_c)^2 = \frac{1}{j_{max} - j_{min} + 1} \sum_{j=j_{min}}^{j_{max}} (jP_0/\eta_1 - \mu'_c)^2. \quad (\text{A.5})$$

The correlation coefficient $\gamma_c(K, \theta)$ of a COC VR can therefore be obtained as

$$\gamma_c(K, \theta) = \frac{E(P'_{in,n}(K, \theta) \times P_{load,n}(K, \theta))}{\sigma_c(K, \theta) \times \sqrt{K/M_1}\sigma_s} - \frac{\mu_c(K, \theta) \times K\mu_s}{\sigma_c(K, \theta) \times \sqrt{K/M_1}\sigma_s}, \quad (\text{A.6})$$

where

$$\begin{aligned} E(P'_{in,n}(K, \theta) \times P_{load,n}(K, \theta)) &= \frac{1}{(j_{max} - j_{min} + 1)^{K+1}} \\ &\times \left(\sum_{j_{n+K+1}=j_{min}}^{j_{max}} \dots \sum_{j_{n+1}=j_{min}}^{j_{max}} \left(\left(1 - \frac{\theta}{2\pi} + \frac{\Delta t}{T_s}\right) \frac{j_{n+1}P_0}{\eta_1} \right. \right. \\ &+ \left. \left. \left(\frac{\theta}{2\pi} - \frac{\Delta t}{T_s}\right) \frac{j_{n+K+1}P_0}{\eta_1} + \sum_{u=2}^K \frac{j_{n+u}P_0}{\eta_1} \right) \times \right. \\ &\left. \left(\left(1 - \frac{\theta}{2\pi}\right) j_{n+1}P_0 + \frac{\theta}{2\pi} j_{n+K+1}P_0 + \sum_{u=2}^K j_{n+u}P_0 \right) \right). \end{aligned} \quad (\text{A.7})$$

Accordingly, the average correlation coefficient of a COC VR $\overline{\gamma_c(K)}$ can be denoted as

$$\overline{\gamma_c(K)} = \frac{1}{2\pi} \int_0^{2\pi} \gamma_c(K, \theta) d\theta. \quad (\text{A.8})$$

Appendix B: Guidelines on the Selection of a Suitable Active Critical Frequency F_{ac}

Two different kinds of noise may impact the MTD enhancement ratio of a cryptographic circuit that employs a CoRe voltage converter: i) measurement power noise from devices that are used to perform the measurement and ii) reshuffling power noise from the CoRe voltage converter.

When a cryptographic circuit is in a normal working mode (*i.e.*, clock frequency $f_c \approx F_1 f_s$ and F_1 is an integer), the measured input power $P_{MIP,i}$ of the CoRe voltage converter induced by the i^{th} input data is

$$P_{MIP,i} = P_{in,i}^*(\theta, 1/(F_1 f_s)) + P_{M,i}, \quad (\text{B.1})$$

where $P_{in,i}^*(\theta, 1/(F_1 f_s))$ is the actual input power of the CoRe voltage converter induced by the i^{th} input data and $P_{M,i}$ is the corresponding measurement power noise. When the variance of $P_{in,i}^*(\theta, 1/(F_1 f_s))$ is $\sigma_1^2(\theta, 1/(F_1 f_s))$, the average variance $\overline{\sigma_1^2(1/(F_1 f_s))}$ of $P_{in,i}^*(\theta, 1/(F_1 f_s))$ becomes

$$\overline{\sigma_1^2(1/(F_1 f_s))} = \frac{1}{2\pi} \int_0^{2\pi} \sigma_1^2(\theta, 1/(F_1 f_s)) d\theta. \quad (\text{B.2})$$

Accordingly, the signal-to-noise ratio (SNR) of the input power profile $SNR_M(1/(F_1 f_s))$ can be written as

$$SNR_M(1/(F_1 f_s)) = \frac{\overline{\sigma_1^2(1/(F_1 f_s))}}{\sigma_M^2}, \quad (\text{B.3})$$

where σ_M^2 is the variance of the measurement power noise.

However, when the attacker lowers the clock frequency from $F_1 f_s$ to f_c (*i.e.*, $F_1 f_s/f_c$ is an integer, the attacker can measure $F_1 f_s/f_c$ number of leakage power data), the total measured input power $P_{TMIP,i}$ of the CoRe voltage converter induced by the i^{th} input data is

$$P_{TMIP,i} = P_{in,i}^*(\theta, 1/f_c) + \sum_{j_1=1}^{F_1 f_s/f_c} P_{M,i,j_1}, \quad (\text{B.4})$$

where P_{M,i,j_1} is the corresponding measurement power noise related with the j_1^{th} measurement under the i^{th} input data. Therefore, the SNR of the input power profile $SNR_M(1/f_c)$ can be written as

$$SNR_M(1/f_c) = \frac{\overline{\sigma_1^2(1/f_c)}}{\frac{F_1 f_s}{f_c} \sigma_M^2}. \quad (\text{B.5})$$

The correlation coefficient $\gamma_M(1/f_c)$ between the actual input power and measured input power of the CoRe voltage converter with measurement power noise when the clock frequency is f_c can be written as [75]

$$\gamma_M(1/f_c) = \frac{1}{\sqrt{1 + \frac{1}{SNR_M(1/f_c)}}}. \quad (\text{B.6})$$

When the clock frequency is f_c and the average correlation coefficient between the actual input power and load power of the CoRe voltage converter is $\overline{\gamma_{Re}(1/f_c)}$ ¹, the measurement power noise and reshuffling power noise from the CoRe voltage converter are independent. The correlation coefficient $\gamma_t(1/f_c)$ between the measured input power and load power of the CoRe voltage converter can therefore be written as [75]

$$\gamma_t(1/f_c) = \gamma_M(1/f_c) \times \overline{\gamma_{Re}(1/f_c)}. \quad (\text{B.7})$$

The total MTD enhancement ratio $MTD_t(1/f_c)$ induced by the measurement power noise and reshuffling power noise from the CoRe voltage converter is [75]

$$MTD_t(1/f_c) \propto \frac{1}{(\gamma_t(1/f_c))^2}. \quad (\text{B.8})$$

¹Modeling of the average correlation coefficient of voltage converter with a variable clock frequency is analyzed in Section 6.4.1.

As compared to a cryptographic circuit with the clock frequency of $(1/F_0)f_s$, the MTD value of a cryptographic circuit with the clock frequency of f_c would be enhanced $f_s/(f_cF_0)$ times. $MTD_t(1/f_c)$ therefore becomes

$$MTD_t(1/f_c) \simeq \frac{\frac{1}{F_0}f_s}{f_c} \times \frac{1}{(\gamma_t(1/f_c))^2}. \quad (\text{B.9})$$

As shown in Fig. 6.3(b), the minimum MTD enhancement ratio of a cryptographic circuit with the SA voltage converter is 6,145. When the MTD enhancement ratio induced by the measurement power noise and reshuffling power noise from the CoRe voltage converter is lower than the minimum MTD enhancement ratio induced by the SA voltage converter, the discharging resistor R_c needs to be activated to trigger the SA voltage converter to enhance the security. Therefore, an approximately optimum active critical frequency F_{ac} can be determined by solving

$$MTD_t(1/F_{ac}) \simeq \frac{\frac{1}{F_0}f_s}{F_{ac}} \times \frac{1}{(\gamma_t(1/F_{ac}))^2} = 6145. \quad (\text{B.10})$$

Appendix C: Detailed Explanation of Table 7.1 and Table 7.2

As demonstrated in Section 7.2, the parameters that leak due to the usage of three different voltage regulators with a VFS load can be summarized in Table C.1(a). As explained in Section 7.2, an LDO regulator leaks the information regarding the clock frequency f_c of the VFS load, while a buck converter leaks information regarding the supply voltage V_{dd} of the VFS load. However, an SC converter with VFS load prevents the leakage of f_c and V_{dd} as demonstrated in Section 7.2.3.

The inserted noise induced by three different VFS techniques against DPA attacks is shown in Table C.1(b). For RDVFS technique against DPA attacks, the inserted noise can be written as $\log(f_c) + 2\log(V_{dd})$ based on equation (7.14). Since, there is a one-to-one linear relationship between f_c and V_{dd} in RDVFS technique, the relationship between f_c and V_{dd} can be denoted as $f_c = F(V_{dd})$ or $V_{dd} = F^{-1}(f_c)$ where F^{-1} is the inverse function of F . Therefore, the inserted noise induced by RDVFS technique against DPA attacks also can be written as $\log(F(V_{dd})) + 2\log(V_{dd})$ or $\log(f_c) + 2\log(F^{-1}(f_c))$. For RDVS technique against DPA attacks, since clock frequency f_c is fixed, from equation (7.14), the inserted noise can be written as $2\log(V_{dd})$. However, for AVFS technique against DPA attacks, from equation (7.14), the inserted noise is $\log(f_c) + 2\log(V_{dd})$. Unlike RDVFS technique, the clock frequency f_c is independent of the supply voltage V_{dd} in AVFS technique, therefore, f_c can not be denoted as a function of V_{dd} in AVFS technique.

As shown in Table 7.1, when an LDO regulator is implemented within different VFS techniques against DPA attacks, the VFS noise related to f_c can be eliminated due to the leakage of f_c . Similarly, for a buck converter implemented within different VFS techniques against DPA attacks, the VFS noise related to V_{dd} can be eliminated due to the leakage of V_{dd} . Since an SC converter implemented within different VFS techniques against DPA attacks prevents the leakage of f_c and V_{dd} , the VFS noise is retained without reduction.

The inserted noise induced by three different VFS techniques against LPA attacks is shown in Table C.1(c). Since all of the VFS techniques (RDVFS, RDVS, and AVFS) contain the information of the V_{dd} scaling as demonstrated in equation (7.32), the inserted noise from all of the VFS techniques against LPA attacks can be written as $\log(V_{dd}) + 1.19V_{dd}$. Since a buck converter with

Table C.1 (a) Parameter Leakage of Three Different Voltage Regulators with VFS Load, (b) Inserted Noise Induced by Three Different VFS Techniques against DPA Attacks, and (c) Inserted Noise Induced by Three Different VFS Techniques against LPA Attacks.

(a)

	LDO regulator	Buck Converter	SC converter
Leakage	f_c	V_{dd}	0

(b)

	RDVFS	RDVS	AVFS
Noise	$\log(F(V_{dd})) + 2\log(V_{dd})$ OR $\log(f_c) + 2\log(F^{-1}(f_c))$	$2\log(V_{dd})$	$\log(f_c) + 2\log(V_{dd})$

(c)

	RDVFS	RDVS	AVFS
Noise	$\log(V_{dd}) + 1.19V_{dd}$	$\log(V_{dd}) + 1.19V_{dd}$	$\log(V_{dd}) + 1.19V_{dd}$

a VFS load leaks the supply voltage V_{dd} , the inserted noise from a buck converter with different VFS techniques related with V_{dd} against LPA attacks can be eliminated, as tabulated in Table 7.2.

Appendix D: Power Consumption Overhead of Different Countermeasures

The dynamic power dissipation P_{dyn} of the S-box mentioned in *Chapter 7* is

$$P_{dyn} = \alpha f_c V_{dd}^2. \quad (\text{D.33})$$

In Fig. D.1(a), $(f'_{c,0}, V'_{dd,0})$ is the clock frequency and supply voltage of an S-box that does not employ a VFS technique. When the S-box employs RDVS technique as shown in Fig. D.1(a), the supply voltage becomes higher than $V'_{dd,0}$, increasing the dynamic power dissipation of the S-box as compared to the dynamic power dissipation of the S-box without a VFS technique.

When an S-box employs RDVFS technique as shown in Fig. D.1(b), the clock frequency and supply voltage can be lower than $f'_{c,0}$ and $V'_{dd,0}$, respectively. As a result, the dynamic power dissipation of the S-box that employs RDVFS technique is lower than the dynamic power dissipation of the S-box without a VFS technique.

When an S-box employs AVFS technique as shown in Fig. D.1(c), the clock frequency and supply voltage can also be lower than $f'_{c,0}$ and $V'_{dd,0}$, respectively. However, as compared to RDVFS technique, the clock frequency and supply voltage of an S-box that employs AVFS technique no longer have a one-to-one relationship (*i.e.*, the clock frequency is independent of the supply voltage). Therefore, when the supply voltage is high, the clock frequency does not need to be high in AVFS technique. This property of the AVFS technique can make the dynamic power dissipation of the S-box that employs AVFS technique lower than the dynamic power dissipation of the S-box that employs RDVFS technique.

The leakage power dissipation P_{leak} of an S-box as derived in equation (7.31) is

$$P_{leak} \approx V_{dd} \times I_{leak,0} \times \exp(1.19 \times V_{dd}). \quad (\text{D.31})$$

Unlike the dynamic power dissipation P_{dyn} of an S-box, the leakage power dissipation P_{leak} is actually independent of the clock frequency f_c .

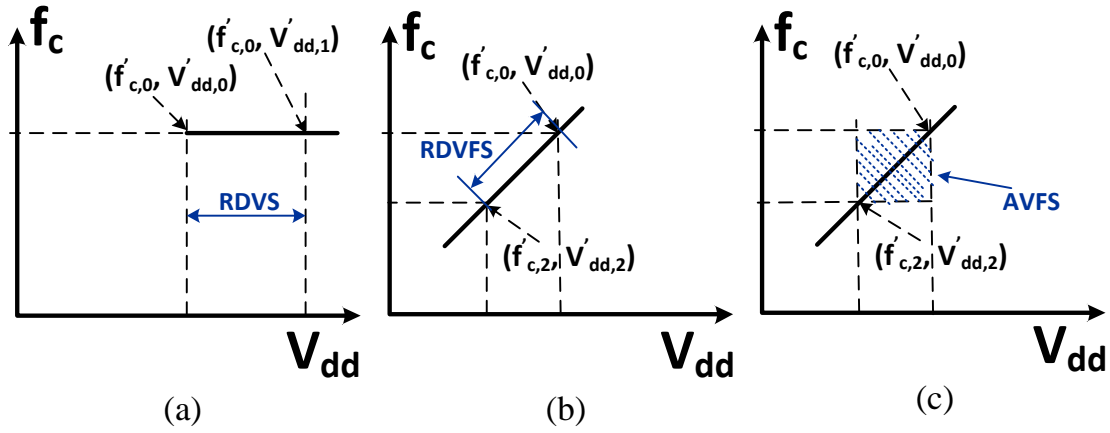


Figure D.1 Supply voltage V_{dd} versus clock frequency f_c under different VFS techniques: (a) RDVS technique, (b) RDVFS technique, and (c) AVFS technique.

When an S-box employs RDVS technique as shown in Fig. D.1(a), since the the supply voltage is higher than $V'_{dd,0}$, the leakage power dissipation of the S-box employs RDVS technique is higher than the leakage power dissipation of the S-box that does not employ a VFS technique. For an S-box that employs either RDVFS or AVFS technique (respectively illustrated in Fig. D.1(b) and in Fig. D.1(c)), since the the supply voltage can be lower than $V'_{dd,0}$, the leakage power dissipation of the S-box that employs RDVFS or AVFS technique is lower than the leakage power dissipation of the S-box that does not employ a VFS technique.

Appendix E: On-Chip Voltage Regulation with Normally Distributed VFS Technique

Assuming that the clock frequency f_c and the supply voltage V_{dd} of a RDVFS technique conform to a normal distribution with the mean values μ_f and μ_v , respectively, as

$$\mu_f = \frac{f_1 + f_2}{2}, \quad (\text{E.34})$$

$$\mu_v = \frac{V_{DD1} + V_{DD2}}{2}, \quad (\text{E.35})$$

the relationship between the variance of the clock frequency σ_f^2 and the variance of the supply voltage σ_v^2 becomes

$$\sigma_f^2 = \left(\frac{\mu_f}{\mu_v}\right)^2 \sigma_v^2. \quad (\text{E.36})$$

If ΔV_{dd} is the minimum supply voltage resolution that is defined as

$$\Delta V_{dd} = \frac{V_{DD2} - V_{DD1}}{N - 1}, \quad (\text{E.37})$$

the below approximated equation is satisfied when N is sufficiently large

$$\sum_{i=1}^N \frac{\Delta V_{dd}}{\sigma_v \sqrt{2\pi}} \exp\left(-\frac{(V_{dd,i} - \mu_v)^2}{2\sigma_v^2}\right) \approx 1. \quad (\text{E.38})$$

Assuming that the total number of input (f_c, V_{dd}) data is W , the corresponding number of input $(f_{c,i}, V_{dd,i})$ data W_i is

$$W_i \approx \frac{W}{\sigma_v \sqrt{2\pi}} \exp\left(-\frac{(V_{dd,i} - \mu_v)^2}{2\sigma_v^2}\right). \quad (\text{E.39})$$

The mean value of the uncertain noise $E(N_{j,k}(f_c, V_{dd}))$ for on-chip voltage regulation based and normally distributed RDVFS technique ($j = 1$), RDVS technique ($j = 2$), and AVFS technique

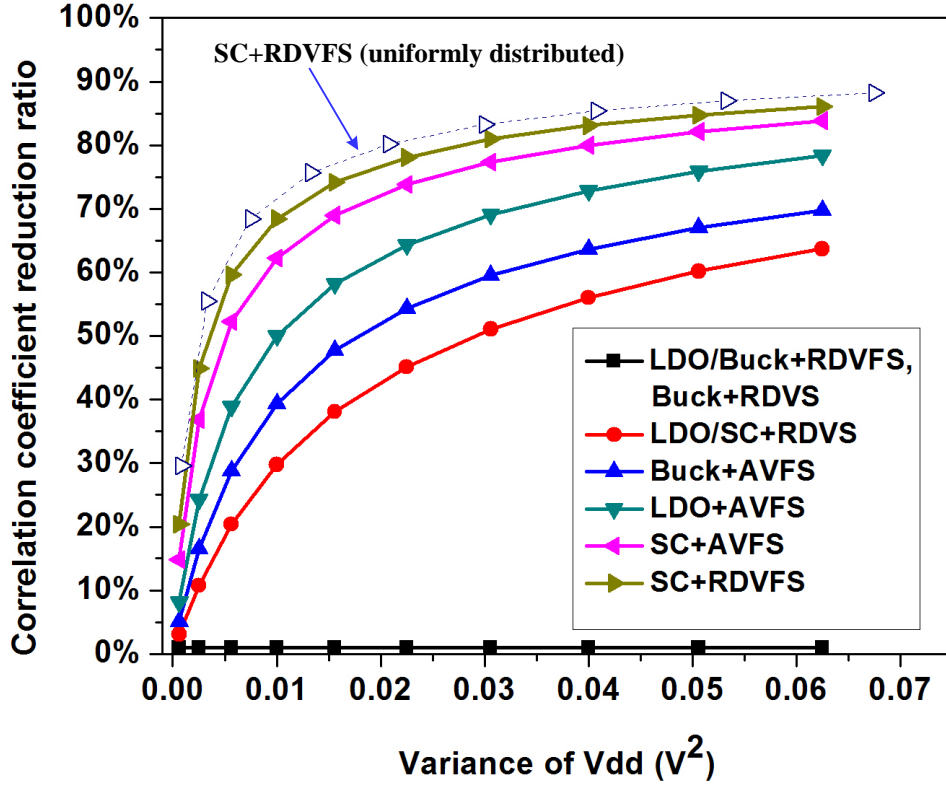


Figure E.1 Variance of supply voltage V_{dd} versus correlation coefficient reduction ratio of an S-box that employs different techniques (VFS techniques conform to normal distribution, $f_v = 10MHz$, and $N = 50$) as compared to uniformly distributed RDVFS with an SC voltage converter.

($j = 3$) become

$$E(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N W_i \left[\frac{f_{c,i}}{f_v} \right]} \sum_{i=1}^N W_i \left[\frac{f_{c,i}}{f_v} \right] N_{1,k}(f_{c,i}, V_{dd,i}), \quad (\text{E.40})$$

$$E(N_{2,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N W_i} \sum_{i=1}^N W_i N_{2,k}(f_c, V_{dd,i}), \quad (\text{E.41})$$

$$E(N_{3,k}(f_c, V_{dd})) = \frac{1}{\sum_{l=1}^N \sum_{i=1}^N W_l W_i \left[\frac{f_{c,l}}{f_v} \right]} \times \sum_{l=1}^N \sum_{i=1}^N W_l W_i \left[\frac{f_{c,l}}{f_v} \right] N_{3,k}(f_{c,l}, V_{dd,i}). \quad (\text{E.42})$$

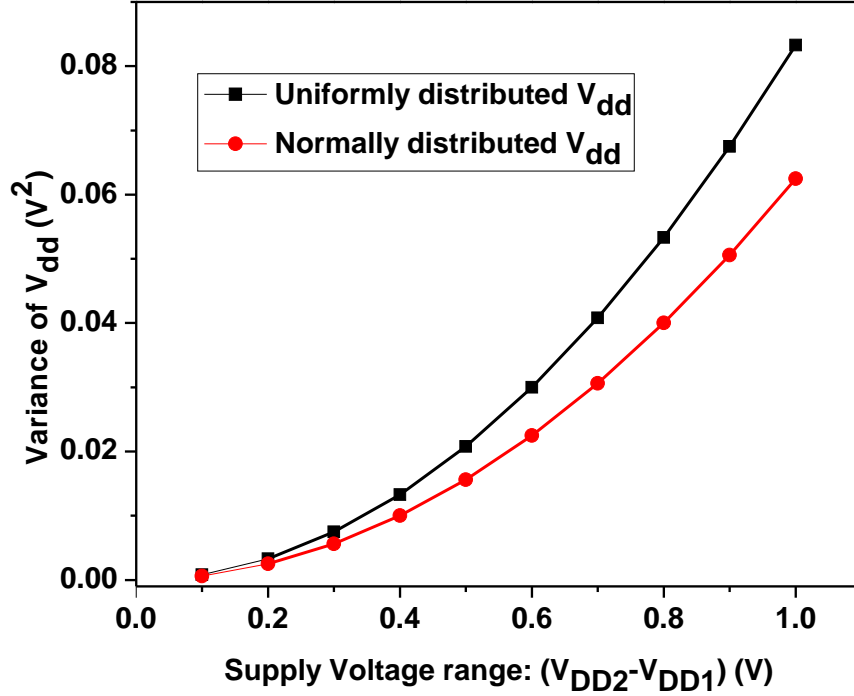


Figure E.2 Variance of the supply voltage V_{dd} versus the supply voltage range ($V_{DD2} - V_{DD1}$) for uniformly and normally distributed V_{dd} .

The corresponding variance of uncertain noise $Var(N_{1,k}(f_c, V_{dd}))$ can be written as

$$Var(N_{1,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N W_i \left[\frac{f_{c,i}}{f_v} \right]} \times \sum_{i=1}^N W_i \left[\frac{f_{c,i}}{f_v} \right] (N_{1,k}(f_{c,i}, V_{dd,i}) - E(N_{1,k}(f_c, V_{dd})))^2, \quad (\text{E.43})$$

$$Var(N_{2,k}(f_c, V_{dd})) = \frac{1}{\sum_{i=1}^N W_i} \times \sum_{i=1}^N W_i (N_{2,k}(f_c, V_{dd,i}) - E(N_{2,k}(f_c, V_{dd})))^2, \quad (\text{E.44})$$

$$\begin{aligned}
\text{Var}(N_{3,k}(f_c, V_{dd})) &= \frac{1}{\sum_{l=1}^N \sum_{i=1}^N W_l W_i \left[\frac{f_{c,l}}{f_v}\right]} \times \\
&\sum_{l=1}^N \sum_{i=1}^N W_l W_i \left[\frac{f_{c,l}}{f_v}\right] (N_{3,k}(f_{c,l}, V_{dd,i}) - E(N_{3,k}(f_c, V_{dd})))^2.
\end{aligned} \tag{E.45}$$

As shown in Fig. E.1, an S-box [80] with the RDVFS technique employing an SC converter still exhibits the highest correlation coefficient reduction ratio as compared to the S-boxes that employ other techniques. Moreover, as compared to the S-box with uniformly distributed RDVFS technique employing an SC converter, the S-box with normally distributed RDVFS technique employing an SC converter has a slightly lower correlation coefficient reduction ratio under the same variance of the supply voltage. However, as shown in Fig. E.2, for achieving the same variance of supply voltage, the normally distributed RDVFS technique needs to have a larger supply voltage range ($V_{DD2} - V_{DD1}$), which would degrade the performance of the cryptographic circuits as compared to the uniformly distributed RDVFS technique.

Appendix F: Copyright Permissions

The following copyright permission notice is for the Fig. 1.1 of *Chapter 1*



The screenshot shows the Copyright Clearance Center RightsLink interface. At the top left is the Copyright Clearance Center logo. To its right is the RightsLink logo. Further right are navigation buttons for Home, Create Account, and Help, along with a chat icon. The main content area displays a request for permission to reuse content from an IEEE publication. The request details are as follows:

	Title: Chosen-message SPA attacks against FPGA-based RSA hardware implementations	<input type="button" value="LOGIN"/>
	Conference Proceedings: 2008 International Conference on Field Programmable Logic and Applications	If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials. Already a RightsLink user or want to learn more?
	Author: Atsushi Miyamoto; Naofumi Homma; Takafumi Aoki; Akashi Satoh	
	Publisher: IEEE	
	Date: 8-10 Sept. 2008	
	Copyright © 2008, IEEE	

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

Copyright © 2017 Copyright Clearance Center, Inc. All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#). Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the Fig. 1.2 of *Chapter 1*

Copyright Clearance Center RightsLink® Home Create Account Help Chat

IEEE
Requesting permission to reuse content from an IEEE publication

Title: A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine
Author: Po-Chun Liu
Publication: Circuits and Systems Part II: Express Briefs, IEEE Transactions on
Publisher: IEEE
Date: Feb. 2012
Copyright © 2012, IEEE

LOGIN
If you're a [copyright.com user](#), you can login to RightsLink using your copyright.com credentials. Already a [RightsLink user](#) or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

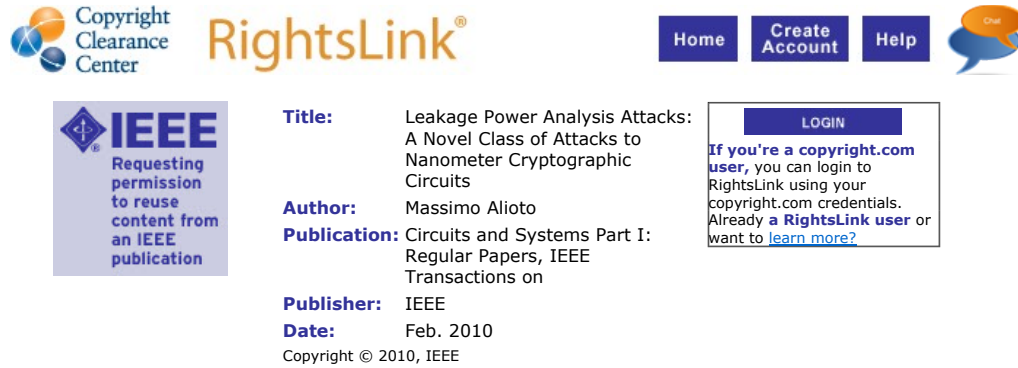
- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK **CLOSE WINDOW**

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#).
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the Fig. 1.3 and Fig. 1.4 of *Chapter 1*



The screenshot shows the Copyright Clearance Center RightsLink interface. At the top left is the Copyright Clearance Center logo, and at the top right are navigation buttons for Home, Create Account, and Help, along with a chat icon. The main content area features a blue box on the left with the IEEE logo and the text "Requesting permission to reuse content from an IEEE publication". To the right, the following information is displayed:

Title: Leakage Power Analysis Attacks: A Novel Class of Attacks to Nanometer Cryptographic Circuits
Author: Massimo Alioto
Publication: Circuits and Systems Part I: Regular Papers, IEEE Transactions on
Publisher: IEEE
Date: Feb. 2010
Copyright © 2010, IEEE

On the right side, there is a "LOGIN" button and a text box that reads: "If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials. Already a RightsLink user or want to learn more?"

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

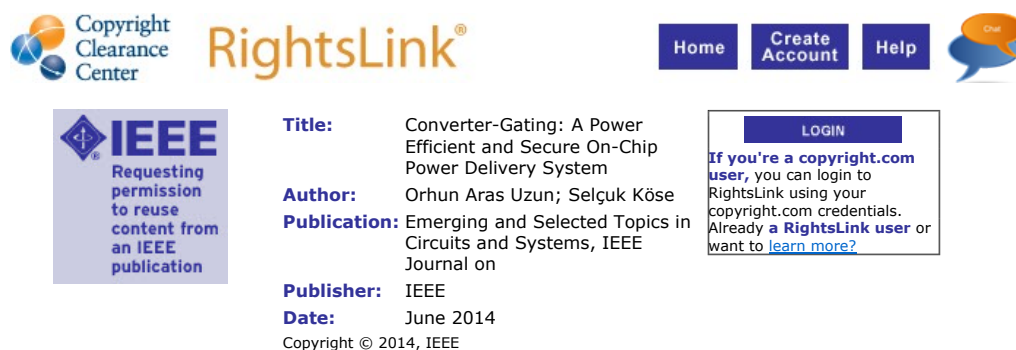
If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.



Copyright © 2017 Copyright Clearance Center, Inc. All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#). Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the Fig. 1.5, Fig. 1.6, and Fig. 1.7 of

Chapter 1



The screenshot shows the RightsLink website interface. At the top left is the Copyright Clearance Center logo. To its right is the RightsLink logo. Further right are navigation buttons for Home, Create Account, and Help, along with a chat icon. Below the navigation is a blue box with the IEEE logo and the text: "Requesting permission to reuse content from an IEEE publication". To the right of this box is a list of publication details: Title: Converter-Gating: A Power Efficient and Secure On-Chip Power Delivery System; Author: Orhun Aras Uzun; Selçuk Köse; Publication: Emerging and Selected Topics in Circuits and Systems, IEEE Journal on; Publisher: IEEE; Date: June 2014; Copyright © 2014, IEEE. To the right of the details is a LOGIN button and a text box that says: "If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials. Already a RightsLink user or want to learn more?".

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ♦ 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line ♦ [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author♦s approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: ♦ [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK ♦♦♦ **CLOSE WINDOW**

Copyright © 2017 Copyright Clearance Center, Inc. All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#). Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 2*



[Home](#) [Create Account](#) [Help](#)



Title: Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks
Conference Proceedings: 2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)
Author: Weize Yu; Orhun Aras Uzun; Selçuk Köse
Publisher: IEEE
Date: 8-12 June 2015
Copyright © 2015, IEEE

[LOGIN](#)
If you're a [copyright.com user](#), you can login to RightsLink using your copyright.com credentials. Already a [RightsLink user](#) or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#) [CLOSE WINDOW](#)

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement.](#) [Terms and Conditions.](#) Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 3*



RightsLink®

Home Create Account Help



Title: Time-Delayed Converter-Reshuffling: An Efficient and Secure Power Delivery Architecture
Author: Weize Yu; Selçuk Köse
Publication: IEEE Embedded Systems Letters
Publisher: IEEE
Date: Sept. 2015
Copyright © 2015, IEEE

LOGIN
If you're a [copyright.com user](#), you can login to RightsLink using your copyright.com credentials. Already a [RightsLink user](#) or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement.](#) [Terms and Conditions.](#)
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 4*



RightsLink®

Home Create Account Help



Title: Charge-Withheld Converter-Reshuffling: A Countermeasure Against Power Analysis Attacks
Author: Weize Yu; Selçuk Köse
Publication: Circuits and Systems Part II: Express Briefs, IEEE Transactions on
Publisher: IEEE
Date: May 2016
Copyright © 2016, IEEE

LOGIN
If you're a **copyright.com** user, you can login to RightsLink using your copyright.com credentials. Already a **RightsLink** user or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ♦ 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line ♦ [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author♦s approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: ♦ [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement.](#) [Terms and Conditions.](#) Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 5*



RightsLink®

Home Create Account Help



Title: A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks
Author: Weize Yu; Selçuk Köse
Publication: Circuits and Systems Part I: Regular Papers, IEEE Transactions on
Publisher: IEEE
Date: Aug. 2016
Copyright © 2016, IEEE

LOGIN
If you're a **copyright.com** user, you can login to RightsLink using your copyright.com credentials. Already a **RightsLink** user or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ♦ 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line ♦ [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author♦s approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: ♦ [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.


BACK CLOSE WINDOW

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement.](#) [Terms and Conditions.](#) Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 6*



Home Create Account Help



Title: Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks
Author: Weize Yu; Selçuk Köse
Publication: Very Large Scale Integration Systems, IEEE Transactions on
Publisher: IEEE
Date: Dec 31, 1969
Copyright © 1969, IEEE

LOGIN
If you're a [copyright.com user](#), you can login to RightsLink using your copyright.com credentials. Already a [RightsLink user](#) or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ♦ 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line ♦ [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: ♦ [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK

CLOSE WINDOW

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#).
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the content of *Chapter 7*



RightsLink®

Home Create Account Help



Title: Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures
Author: Weize Yu; Selcuk Kose
Publication: IEEE Transactions on Emerging Topics in Computing
Publisher: IEEE
Date: Dec 31, 1969
Copyright © 1969, IEEE

LOGIN
If you're a [copyright.com user](#), you can login to RightsLink using your copyright.com credentials. Already a [RightsLink user](#) or want to [learn more?](#)

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line © 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line © [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: © [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

BACK CLOSE WINDOW

Copyright © 2017 [Copyright Clearance Center, Inc.](#) All Rights Reserved. [Privacy statement.](#) [Terms and Conditions.](#)
Comments? We would like to hear from you. E-mail us at customercare@copyright.com

The following copyright permission notice is for the Fig. 9.3 of *Future Work*



The screenshot shows the Copyright Clearance Center RightsLink interface. At the top left is the Copyright Clearance Center logo. To its right is the RightsLink logo. Further right are navigation buttons for Home, Create Account, Help, and an email icon. Below the logo is a box with the IEEE logo and the text: "Requesting permission to reuse content from an IEEE publication". To the right of this box is the copyright notice for the publication: "Title: An Aging-Resistant RO-PUF for Reliable Key Generation; Author: MD. Tauhidur Rahman; Fahim Rahman; Domenic Forte; Mark Tehranipoor; Publication: IEEE Transactions on Emerging Topics in Computing; Publisher: IEEE; Date: July-Sept. 2016; Copyright © 2016, IEEE". To the right of the notice is a LOGIN button and a text box that says: "If you're a copyright.com user, you can login to RightsLink using your copyright.com credentials. Already a RightsLink user or want to learn more?".

Thesis / Dissertation Reuse

The IEEE does not require individuals working on a thesis to obtain a formal reuse license, however, you may print out this statement to be used as a permission grant:

Requirements to be followed when using any portion (e.g., figure, graph, table, or textual material) of an IEEE copyrighted paper in a thesis:

- 1) In the case of textual material (e.g., using short quotes or referring to the work within these papers) users must give full credit to the original source (author, paper, publication) followed by the IEEE copyright line ♦ 2011 IEEE.
- 2) In the case of illustrations or tabular material, we require that the copyright line ♦ [Year of original publication] IEEE appear prominently with each reprinted figure and/or table.
- 3) If a substantial portion of the original paper is to be used, and if you are not the senior author, also obtain the senior author's approval.

Requirements to be followed when using an entire IEEE copyrighted paper in a thesis:

- 1) The following IEEE copyright/ credit notice should be placed prominently in the references: ♦ [year of original publication] IEEE. Reprinted, with permission, from [author names, paper title, IEEE publication title, and month/year of publication]
- 2) Only the accepted version of an IEEE copyrighted paper can be used when posting the paper or your thesis on-line.
- 3) In placing the thesis on the author's university website, please display the following message in a prominent place on the website: In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of [university/educational entity's name goes here]'s products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to http://www.ieee.org/publications_standards/publications/rights/rights_link.html to learn how to obtain a License from RightsLink.

If applicable, University Microfilms and/or ProQuest Library, or the Archives of Canada may supply single copies of the dissertation.

[BACK](#) ♦♦♦ [CLOSE WINDOW](#)

Copyright © 2017 Copyright Clearance Center, Inc. All Rights Reserved. [Privacy statement](#). [Terms and Conditions](#). Comments? We would like to hear from you. E-mail us at customercare@copyright.com

ABOUT THE AUTHOR

Weize Yu received the B.S. and M.S. degrees in electrical engineering from University of Electronic Science and Technology of China, Chengdu, China, and Institute of Microelectronics of Chinese Academy of Sciences, Beijing, China, respectively, in 2009 and 2012. He joined the electrical engineering department of University of South Florida to pursue his Ph.D. degree in Fall 2014. He is awarded with the USF presidential fellowship from 2014 to 2017. During his Ph.D. study, his research interests are mainly focused on power management IC and hardware security.