Distributed On-Chip Power Supply for Security Enhancement in Multicore NoC

Xingye Liu and Paul Ampadu
Department of Electrical and Computer Engineering
Virginia Tech
Blacksburg, USA
xingye15@vt.edu, ampadu@vt.edu

2021 IEEE 34th International System-on-Chip Conference (SOCC) | 978-1-6654-2931-3/21/$31.00 ©2021 IEEE | DOI: 10.1109/SOCC52499.2021.9739219

***Abstract*—We propose a distributed DC/DC converter against correlation power analysis and input voltage glitch injection attacks in emerging multicore applications. Moving towards Internet-of-Things, heterogeneous integration and Network-on-Chip architectures, protecting data privacy and critical operation information for every device become crucial. The proposed DC/DC converter is designed to mitigate correlation power analysis by weakening the input-output relationships for various types of workloads. For steady-state workloads, the correlation factors between input and output currents are reduced to only 0.05. For digital workloads, the correlation factors can vary by 10 times when there are only a few nanoseconds delay of the load current, which greatly prevents attackers from deriving the circuit real operations. Meanwhile, the converter is able to resist 20% input voltage glitches without generating additional spikes or droops while controlling the voltage ripples within 7.5% of the output. Implemented and simulated in 32nm CMOS technology, single channel peak efficiency reaches 85% based on post-layout models. The converter is also able to provide up to 19.3V/μs reference tracking capability for dynamic voltage scaling requests. The security enhancement induces about 20% area overhead and an average 3% efficiency loss. Overall, the proposed converter is a promising countermeasure solution for side-channel attacks in multicore systems without sacrificing too much performance.**

Keywords—DC/DC converter, security, correlation power analysis, distributed power supply, Network-on-Chips

I. INTRODUCTION

Security has become more and more critical for any embedded or integrated systems during the past few decades. While more devices are interconnected enabling the Internet of Things (IoTs), the protection against attackers is no longer limited to sensitive or confidential data that are transmitted, but also includes operation or processing details of any devices in the system [1], [2]. Traditionally, encryption blocks, such as Advanced Encryption Standard (AES) ciphers, are commonly used to secure data and communications and have been studied a lot to achieve better performance without costing more power consumption. However, as the silicon world moves into post-Moore's law era, heterogeneous and larger-scale systems, like multicore systems using Network-on-Chip (NoC) or System-in-Package (SiP) architectures, are introduced to overcome computing-power dilemma [3]. Potential security issues in these emerging computing platforms have not been explored well and previous solutions may not be sufficient or efficient to be implemented. It is necessary to design specialized countermeasures using either hardware or software solutions.

Most of the security attacks targeting NoC are belonged to (1) Denial-of-Service (DoS) attack; (2) unauthorized use, including read or write, of channels or wires; or (3) Hardware Trojans (HT) [4]. In order to perform efficient DoS attacks or hijack a wire, router or channel, attackers have to have enough knowledge of the system and then locate the critical components. Distributed attacks should also be solved in such large-scale systems [5]. Therefore, in this paper our major objective is to prevent attackers from deriving the specific logics or schematics and gathering the operation details, by weakening the existing correlations using a power supply solution.

Power analysis is a commonly seen side-channel attack (SCAs) to steal critical or encrypted information from the system [2]. By collecting operation related data and power consumption profiles, doing differential or correlation power analysis (CPA) can help determine the key information from the system during runtime. Considering that encryption engines always feature distinctive operation modes, analyzing their power consumption profiles could release critical information like the security keys. Due to this, power supplies become very vulnerable to power side-channel attacks (PSCA) and people have done lots of research to enhance the security. Among hardware-based solutions, integrated voltage regulators using either inductors or capacitors [6 - 10], have been widely applied to be the countermeasure to correlation power analysis.

In this paper we follow the concept of using integrated power supply to mitigate potential CPA attacks and also provide sufficient resistance to malicious input voltage glitches injections [11] for large-scale systems. We propose a novel distributed DC/DC converter based on heterogeneous 2.5D SiP architecture [12], [13] which will provide scalability, design flexibility and security. The overall architecture example using the distributed converter is shown in Fig. 1.

Since the proposed converter is distributed in the entire package, we define *Load Region*, in which one proposed converter supports three workloads, to help allocate the converters in the system. In this way, the system can be scaled by adding new load regions with dedicated converter and mapping workloads into it. Each load region should have similar peak total power consumption to avoid thermal issues. The remaining part of the paper is organized as follows. The details of the converter are introduced in Section 2. In Section 3, we provide simulation results related to CPA and input voltage glitch attacks, with analysis for each case. More circuit information is given in Section 4 with comparisons with other works. We conclude the work in Section 5.

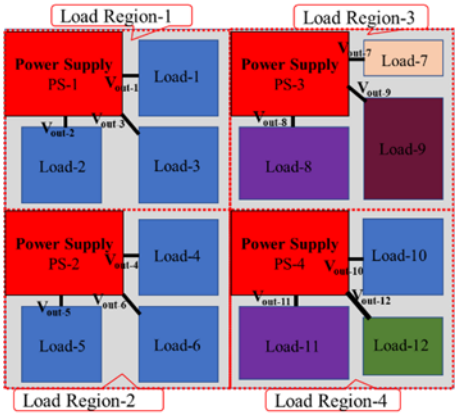


Fig. 1. The example showing how the proposed power supply PS-x (x ϵ N) and three workload chiplets, shown as Load-3x, Load-(3x – 1) and Load-(3x – 2), fit into Load Region-x in the entire system. Each proposed power supply is designed to provide three independent regulated output voltages to either homogeneous (as in Load Region-1 and -2) or heterogeneous (as in Load Region-3 and -4) workloads.

II. Proposed DC/DC Converter

A. Architecture of the Converter

Following the proposed converter shown in Fig. 1, in this paper the converter has three identical output channels. The detailed schematic of three output version is shown in Fig. 2. The converter has two stages: (1) two independent switched capacitor (SC) circuits as first stage, providing two additional internal voltages V_{X1} and V_{X2}; (2) switching blocks and low-pass filters as the second stage for voltage regulation.

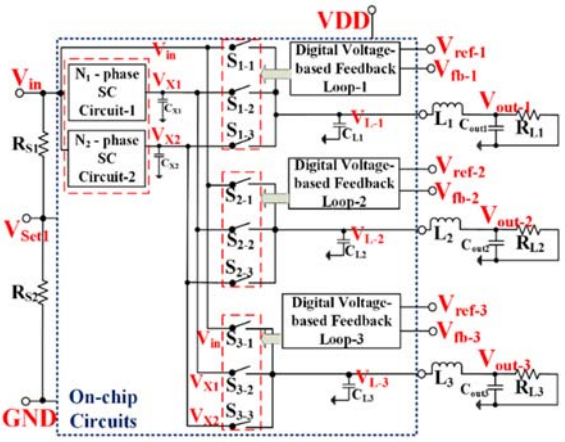


Fig. 2. Schematic of the 3-output version of the converter with two fixed SC circuits and three identical outputs channels, each consisting with three switches and one inductor controlled by independent digital voltage-based feedback loops.

Theoretically, the schematics and conversion ratios of SC circuits are not limited and design is closely related to required sink/source current capability. More internal voltage levels could reduce the output ripples but would need more space for SC circuits. In this design, we set $V_{X1} = 2/3*V_{in}$ and $V_{X2} = 1/3*V_{in}$. C_{out} is about 12nF using off-chip models. We also use transmission gate as switches in all SC circuits to ensure the switching behaviors. For each switching block, two of them are PMOS switch while the left one is using NMOS. Schematic view and layout of SC circuits and switches are shown in Fig. 3 and Fig. 4.

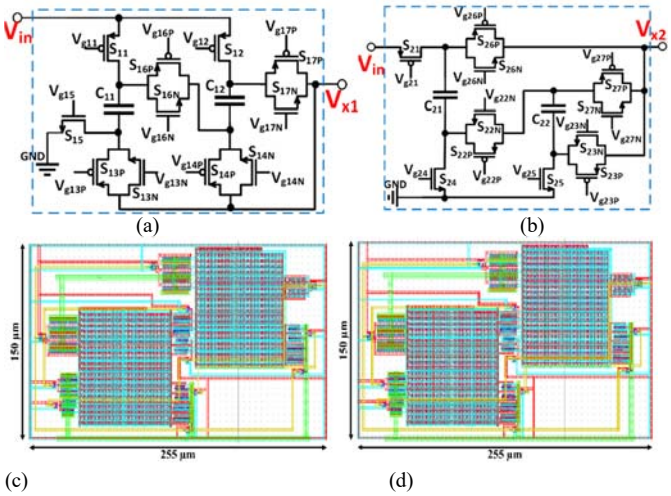


Fig. 3. (a) The schematic of SC circuit-1 located at first stage with voltage conversion ratio 2/3; (b) the schematic of SC circuit-2 with voltage conversion ratio 1/3; (c) layout view of SC circuit-1; (d) layout view of SC circuit-2.

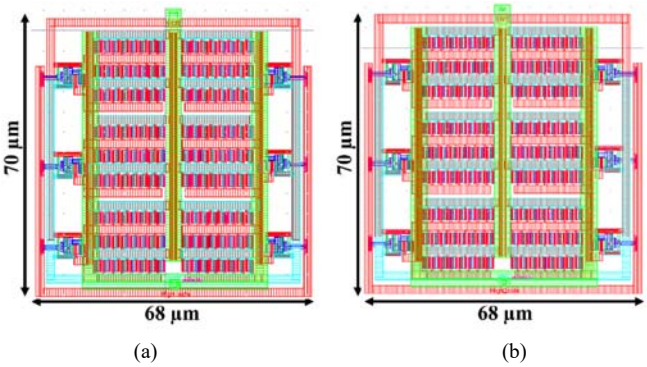


Fig. 4. Layout view of (a) PMOS switch with driving circuits; (b) NMOS switch with driving circuits. Both switches are located at second stage.

The schematics of feedback loops and control are shown in Fig. 5 with theoretical operation waveforms in Fig. 6. The control for each output is divided into two parts: (a) select the proper pair of switches; (b) generate charging time T_{char} and discharging time T_{disc}. For each output, we have the following equations, where V_{req} is the required output voltage, V_{in}, V_{X1} and V_{X2} are shown in Fig. 2:

$$V_{X1} < V_{req} < V_{in},\ V_{out} = T_{char} * V_{in} + T_{disc} * V_{X1} \quad (1)$$

$$V_{X2} < V_{req} < V_{X1},\ V_{out} = T_{char} * V_{X1} + T_{disc} * V_{X2} \quad (2)$$

The design of SC circuits can follow [14] and equations (3) and (4). Switched capacitor circuit switching frequency f_{sw} and switches width W_{sw} are related to flying capacitance C_{fly}, average inductor current I_{Lave} and inductor node voltage V_{L-k} Also, the inductor design is limited by equation (5) where ΔV_L is desired inductor node voltage ripple, T_{tran} is the response time which is determined by the comparators in this work, and I_{Lpeak} is allowed maximum inductor current.

$$f_{sw} \alpha 1/(C_{fly} * V_{L-k} / I_{Lave}) \quad (3)$$

$$W_{sw} \alpha \sqrt{\frac{C_{fly} * I_{Lave}}{V_{L-k}}} \quad (4)$$

$$L > \Delta V_L * T_{tran} / I_{Lpeak} \quad (5)$$

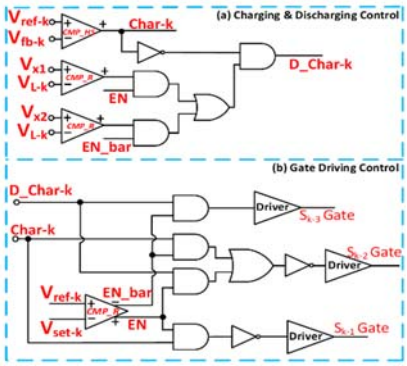


Fig. 5. The control scheme showing (a) charging and discharging signals are generated based on the reference voltage $V_{ref\text{-}k}$, output feedback voltage $V_{fb\text{-}k}$, SC circuits output voltages V_{X1}, V_{X2} and inductor positive node voltage $V_{L\text{-}k}$; (b) gate driving signals for switches that are generated by using charging *Char-k* or discharging *D_Char-k* signals with the external source $V_{set\text{-}k} = V_{X1}$.

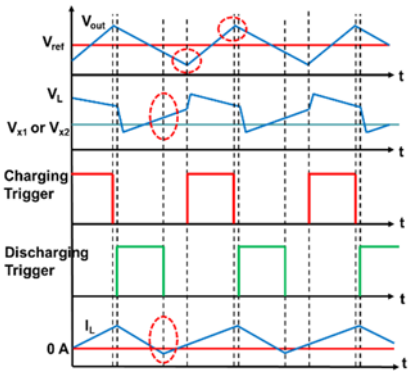


Fig. 6. Theoretical waveforms of the proposed control scheme showing how charging and discharging signals are generated by comparing output voltage V_{out}, reference voltage V_{ref}, inductor node voltage V_L, V_{X1} or V_{X2}.

III. Security Simulation Results

In this section we will show the security related simulation results while using the proposed distributed DC/DC converter circuit. The countermeasure results in this paper are divided into two parts: (a) input voltage glitches injections and (b) correlation power analysis. All the simulations are based on layout models presented in the previous section and sampling step is 0.1ns.

A. Input Voltage Glitches

Responses to input voltage glitches are shown in Fig. 7-9.

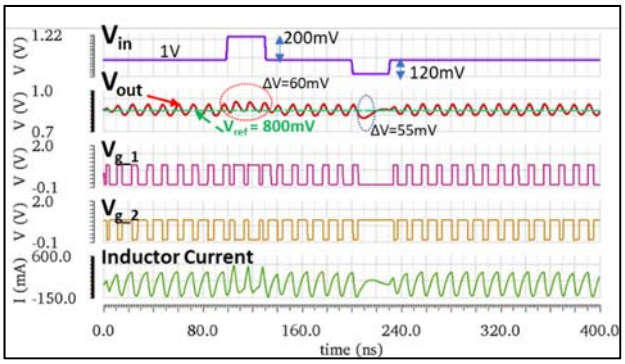


Fig. 7. Single-output responses of the converter when V_{out} = 800mV delivering 100mA and input voltage glitches occur. During either input spike or droop, additional voltage ripples at output are limited to less than 7.5%.

Using 1V as input voltage, we set a 200mV spike glitch and a 120mV droop glitch to check the responses of the system. Single channel responses are shown in Fig. 7 and 8 when V_{out} is 800mV and 600mV respectively. Voltage ripples change slightly during input glitches but the maximum output voltage ripple is always within 7.5% of the output. The responses of all three outputs are shown in Fig. 9 during input glitches. Output-2 and 3 remain very stable and voltage ripples are controlled within 6%. However, since our converter cannot provide boosted voltage, V_{out1} cannot reach the required 910mV when input voltage falls to 880mV.

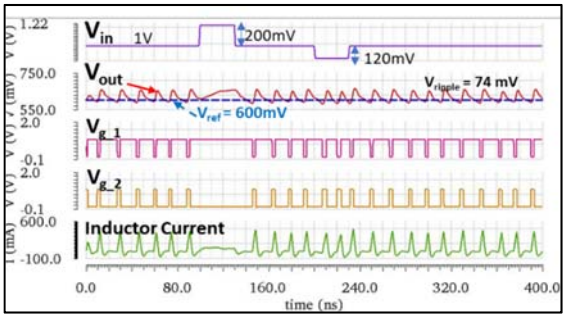


Fig. 8. Single-output responses of the converter when V_{out} = 600mV delivering 100mA and input voltage glitches occur. During either input spike or droop, no additional output voltage ripples are observed.

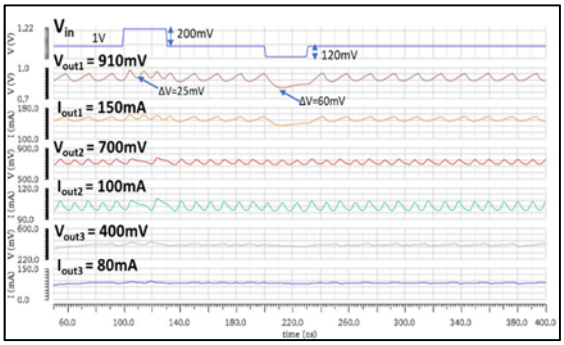
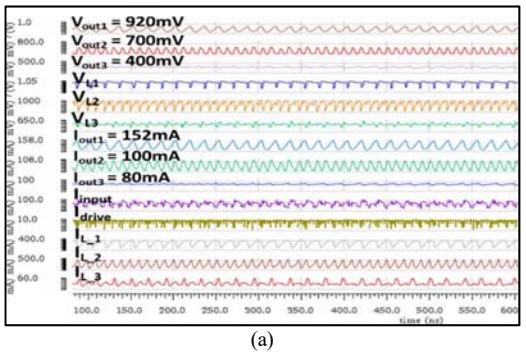


Fig. 9. Three-output responses of the converter during input voltage glitches, where voltage ripples are controlled within 6%. The only voltage shift observed at V_{out1} is because V_{in} falls below the required output.

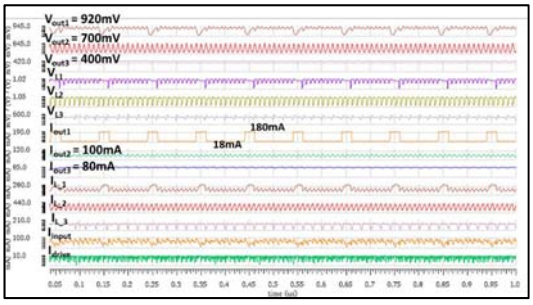
B. Correlation Power Analysis

In this part we provide correlation power analysis results based on different operation conditions. Based on the converter architecture, we assume that attackers can sense *input current*, *inductor node voltages* or *inductor currents* and their target is to determine circuit schematics and load operations. For general NoC based systems, any steady-state loads, voltage scaling transitions or digital workloads (similar to encryptions) could be the potential targets. We will study the converter security by examining the correlation factors between specific circuit operation parameters, such as inductor current and load current.

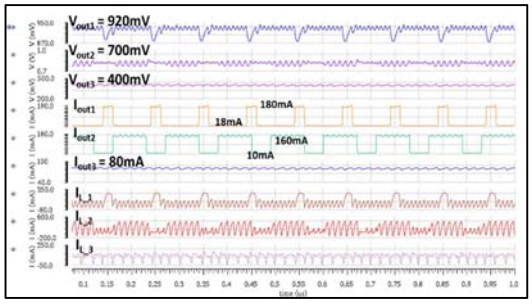
Starting from Fig. 10(a), all the three outputs are supplying steady-state load current. Then we replace one steady-state load with one digital load each time to see how the correlation factors between different parameters change. In Fig. 10(d), all the outputs are supplying digital loads. Based on results from other works, if absolute correlation factor value is larger than 0.1, we will list the corresponding pair of parameters as *related*. V_L is inductor node voltage and I_L is inductor current.



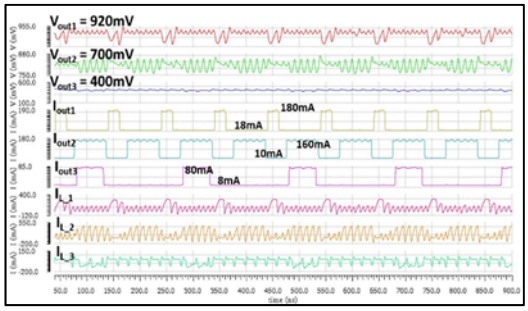
(a)



(b)



(c)



(d)

Fig. 10. Transient operation waveforms of the converter when: (a) all three output loads are in steady-state; (b) only two output loads are in steady-state; (c) only one load is steady-state while other two are digital workloads; (d) all three loads are digital workloads.

To derive the schematic of the circuit and the operation details, these relationships are critical: V_{out} to V_L; I_L to I_{OUT} and I_{IN} to I_{OUT}. Table I shows the correlation factors between V_{out} and inductor node voltage V_L in different conditions. It is quite obvious that each inductor node voltage is directly related to the corresponding output voltage and attackers may recognize the connections between each inductor and output.

However, although V_{out} to V_L correlation is straightforward, it is not enough to derive all the circuit operation details. Table II shows the relationships between the input currents and output currents for different cases. It can be seen that the relationships between input and output currents cannot be identified using steady-state operation waveforms as correlation factors vary a lot and there are no consistent patterns for any outputs.

TABLE I. ABSOLUTE CORRELATION FACTORS FOR V_{OUT} TO V_L

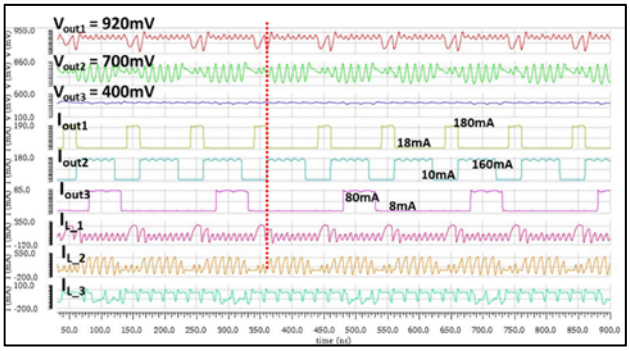
Cases	10(a)	10(b)	10(c)	10(d)
V_{out1} to V_{L1}	0.618	0.353	0.306	0.403
V_{out2} to V_{L2}	0.784	0.814	0.710	0.668
V_{out3} to V_{L3}	0.491	0.562	0.532	0.357

TABLE II. ABSOLUTE CORRELATION FACTORS FOR I_{IN} TO I_{OUT}

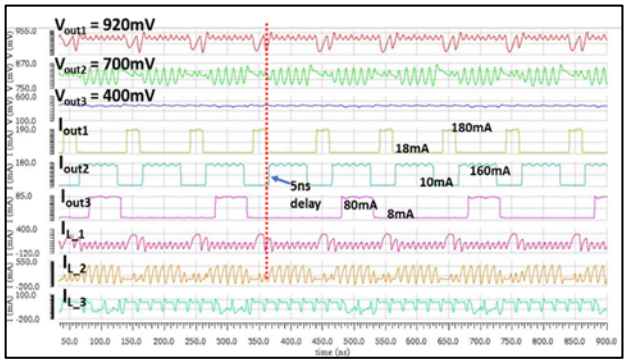
Cases	10(a)	10(b)	10(c)	10(d)
$I_{IN} - I_{OUT1}$	0.057	0.406	0.308	0.024
$I_{IN} - I_{OUT2}$	0.056	0.050	0.326	0.245
$I_{IN} - I_{OUT3}$	0.0005	0.012	0.060	0.244

Due to the fact above that correlations between input and output currents are not consistent and using digital workloads may help determine circuit's operations, we then study the converter's responses in details when all the outputs are connected to digital workloads.

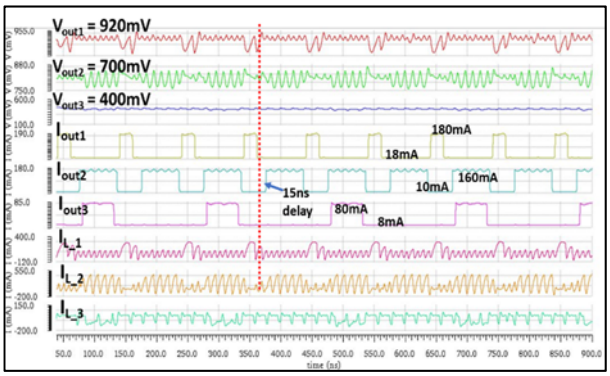
From Fig. 11(a) to 11(c), we list transient operation waveforms of the converter when all the three outputs are connected to digital loads. All loads will be kept at same switching frequency and amplitudes and the only difference is timing. For load 2, there are slightly delays between different cases. In Case 11(b), load 2 current is about 5ns behind that in Case 11(a). And in Case 11(c), this load current is 10ns behind that in Case 11(b). We also set all the output load currents to be aligned at rising edge and shown in Fig. 11(d).



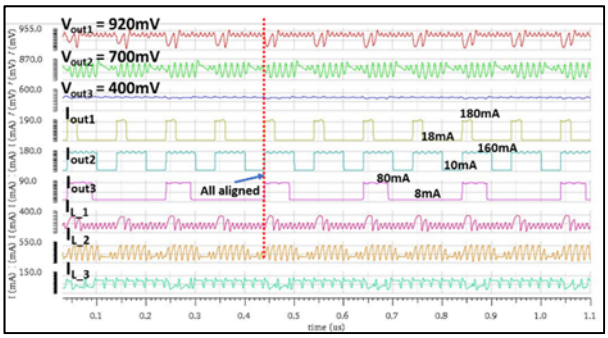
(a)



(b)



(c)



(d)

Fig. 11. Transient operation waveforms when all three outputs are connected digital workloads. Only a few nanoseconds delay is added to I_{OUT2} in (b) and (c) and all three outputs are aligned at rising edge in (d).

For all the four cases shown in Fig. 11, output workloads have the same operation and the only difference is the timing. From 11(a) to 11(c), I_{OUT1} and I_{OUT3} are kept same and only 5ns and 15ns delay is added to I_{OUT2}. Because of the shared circuit components, the inductor current in one channel is actually correlated with output currents in other channels. As marked in Table III, IV and V, I_{L1} is correlated with I_{OUT2} and the correlation factor actually increases by 50% when there is about 15ns measurement delay. Similar phenomena also exist between I_{L2} - I_{OUT3}, and I_{L3} - I_{OUT2}. The correlation factor is increased by 150% and varies almost 10 times for I_{L3} - I_{OUT2}. An effective correlation between I_{L3} and I_{OUT1} also exists which can be confusing for attackers. Since 5ns or 15ns delay could occur easily without being noticed by attackers in real sensing and measurement, such variations of correlation factor could greatly prevent attackers from deriving the correct circuit operations. Meanwhile, if we take a look at the results between input and output currents, the correlation factors also vary significantly. Theoretically, there should be no obvious change for I_{IN} - I_{OUT} correlations since all the loads have the same operations and power. Although the correlation between I_{OUT2} and I_{IN} remains constant, we can find that I_{OUT1} almost shows no correlation with I_{IN} and the correlation factor for I_{OUT3} - I_{IN} varies by 2.5 times. The actual operation and power consumption are hidden well.

To further explore the performance, we set all the output current same as previous three cases but aligned at the rising edge, and the waveforms are shown in Fig. 11(d) with correlation results in Table VI. Compared to the results in other tables, the correlation factors between input and output currents are increased a lot. But the correlation between some inductor currents and output currents, that are mentioned above, becomes weaker. Although forcing alignment of outputs may attenuate the protection to some extent, there still exists multiple misleading correlations for the attackers. Combined with the sensitivity to delays, the proposed converter shows strong protection against side channel analysis by hiding real correlation information.

TABLE III. ABSOLUTE CORRELATION FACTORS FOR CASE 11(a)

Parameters	I_{IN}	I_{L1}	I_{L2}	I_{L3}
I_{OUT1}	0.009	0.570	0.256	0.193
I_{OUT2}	0.243	0.278	0.407	0.023
I_{OUT3}	0.097	0.203	0.097	0.414

TABLE IV. ABSOLUTE CORRELATION FACTORS FOR CASE 11(b)

Parameters	I_{IN}	I_{L1}	I_{L2}	I_{L3}
I_{OUT1}	0.004	0.566	0.262	0.198
I_{OUT2}	0.216	0.405	0.418	0.099
I_{OUT3}	0.207	0.196	0.209	0.422

TABLE V. ABSOLUTE CORRELATION FACTORS FOR CASE 11(c)

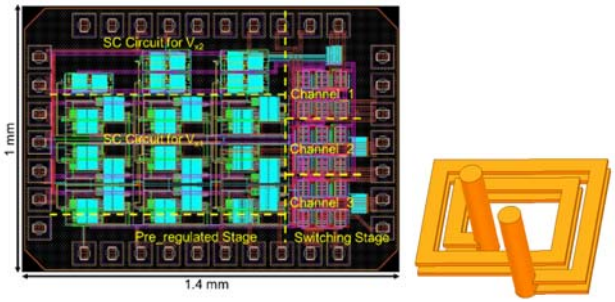
Parameters	I_{IN}	I_{L1}	I_{L2}	I_{L3}
I_{OUT1}	0.024	0.567	0.285	0.203
I_{OUT2}	0.245	0.416	0.421	0.218
I_{OUT3}	0.244	0.197	0.242	0.423

TABLE VI. ABSOLUTE CORRELATION FACTORS FOR CASE 11(d)

Parameters	I_{IN}	I_{L1}	I_{L2}	I_{L3}
I_{OUT1}	0.480	0.553	0.214	0.101
I_{OUT2}	0.540	0.269	0.399	0.221
I_{OUT3}	0.351	0.189	0.171	0.487

IV. CONVERTER PERFORMANCE AND COMPARISONS

The proposed converter, being a hardware solution, can be one of the security improvement stages to protect any kind of workloads. In addition, we also study the general performance of the converter as it is distributed to power multiple workloads in a NoC system. The layout of the converter and the inductor are shown in Fig. 12 and load transient responses and efficiency curves are shown in Fig. 13 and 14.



(a) (b)

Fig. 12. (a) Layout of the proposed converter with three output channels connecting to V_{L-1}, V_{L-2} and V_{L-3} nodes; (b) 3D view of the 2nH Air-core inductor consuming 0.86mm x 0.86mm x 0.75mm space.

The design objective of the converter, in terms of security, is to prevent attackers from deriving the circuit schematics and

stealing relevant operation information. Furthermore, in a large-scale NoC based system, if the attackers cannot identify the schematics and how the workloads are operating, it becomes difficult for them to implement effective DoS attack efficiently and they cannot easily pinpoint the critical connections or wires to hijack and do malicious read/write behaviors.

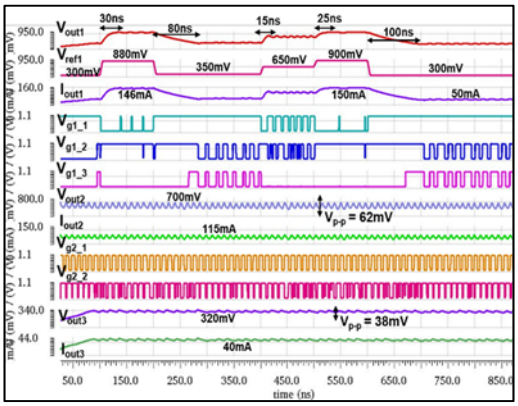


Fig. 13. Transient responses of all outputs when V_{out1} is transitioning between different voltage levels with fixed load impedance showing up to 19.3V/µs step-up and 6.6V/µs step-down reference tracking speed, output-2 is providing 115mA at 700mV and output-3 is providing 40mA at 320mV.

Although the converter shows ultra-fast load transient responses and security improvement, the additional SC circuits and switches generate some power and area overheads. Based on our study, if the converter is optimized only for maximum efficiency, we can save an average 20% area and the efficiency would have an average of 3% boost for all the conditions. For single channel operation, peak efficiency is about 85.5%. We briefly compare our work with others in Table VII.

TABLE VII. COMPARISON WITH OTHER WORKS

	This work	**TVLSI'20 [3]**	**JSSC'18 [7]**	**TVLSI'21 [10]**	**JSSC'19 [15]**
Technique	32nm	65nm	130nm	28nm	130nm
Attack Type	CPA	CPA, CNN & leakage	CPA & leakage	EM side channel	Power/EM side channel
Power Overhead	3%	3.5%	5%	15%	-3.5%
Area Overhead	20%	2.3%	N/A	16%	6.6%
Load Power	165 mW	336 mW	10.5 mW	< 1mW	13.1 mW

V. CONCLUSION

In this paper we presented a distributed power supply featuring single-input-multiple-output architecture to improve security for NoC based large-scale systems. The proposed converter can successfully lower the correlation factor between input current and output current to 0.05 for steady-state operations, which makes it much more difficult for attackers to identify different workloads to perform further attacks. For digital workloads, the converter creates multiple mask correlations between different inductor currents and load currents to mislead attackers. Thus, attackers may not be able to use sensed inductor current to derive the circuit schematics and operation accurately.

However, due to redundant circuits components for multiple output, it brings in about 20% area overhead and 3% power overhead. This might be solved in future works by combining with other control related methods. Since the converter also provides fast load transient responses, it is still a promising hardware solution to be used in large-scale system to improve security against any power side-channel and provide accurate and efficient regulated voltages to multiple workloads.

REFERENCES

[1] A. Singh *et al.*, "Enhanced Power and Electromagnetic SCA Resistance of Encryption Engines via a Security-Aware Integrated All-Digital LDO," in *IEEE Journal of Solid-State Circuits*, vol. 55, no. 2, pp. 478-493, Feb. 2020.

[2] D. Das, S. Ghosh, A. Raychowdhury and S. Sen, "EM/Power Side-Channel Attack: White-Box Modeling and Signature Attenuation Countermeasures," in *IEEE Design & Test*, vol. 38, no. 3, pp. 67-75, June 2021.

[3] J. Yang, J. Han, F. Dai, W. Wang and X. Zeng, "A Power Analysis Attack Resistant Multicore Platform With Effective Randomization Techniques," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 28, no. 6, pp. 1423-1434, June 2020.

[4] L. Daoud, "Secure Network-on-Chip Architectures for MPSoC: Overview and Challenges," *2018 IEEE 61st International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2018, pp. 542-543.

[5] S. Charles, Y. Lyu and P. Mishra, "Real-Time Detection and Localization of Distributed DoS Attacks in NoC-Based SoCs," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 12, pp. 4510-4523, Dec. 2020.

[6] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," in *IEEE Transactions on Emerging Topics in Computing*, vol. 6, no. 2, pp. 244-257, 1 April-June 2018.

[7] M. Kar, A. Singh, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Reducing Power Side-Channel Information Leakage of AES Engines Using Fully Integrated Inductive Voltage Regulator," in *IEEE Journal of Solid-State Circuits*, vol. 53, no. 8, pp. 2399-2414, Aug. 2018.

[8] W. Yu and S. Köse, "Time-Delayed Converter-Reshuffling: An Efficient and Secure Power Delivery Architecture," in *IEEE Embedded Systems Letters*, vol. 7, no. 3, pp. 73-76, Sept. 2015.

[9] Weize Yu, O. A. Uzun and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2015, pp. 1-6.

[10] R. Jevtic, M. Ylitolva, C. Calonge, M. Ojanen, T. Santti and L. Koskinen, "EM Side-Channel Countermeasure for Switched-Capacitor DC–DC Converters Based on Amplitude Modulation," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 29, no. 6, pp. 1061-1072, June 2021.

[11] A. Singh, M. Kar, N. Chawla and S. Mukhopadhyay, "Mitigating Power Supply Glitch based Fault Attacks with Fast All-Digital Clock Modulation Circuit," *2019 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2019, pp. 19-24.

[12] W. J. Lambert, M. J. Hill, K. Radhakrishnan, L. Wojewoda and A. E. Augustine, "Package Inductors for Intel Fully Integrated Voltage Regulators," in *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 6, no. 1, pp. 3-11, Jan. 2016.

[13] R. Mahajan *et al.*, "Embedded Multidie Interconnect Bridge—A Localized, High-Density Multichip Packaging Interconnect," in *IEEE Transactions on Components, Packaging and Manufacturing Technology*, vol. 9, no. 10, pp. 1952-1962, Oct. 2019.

[14] H. Le, S. R. Sanders and E. Alon. "Design Techniques for Fully Integrated Switched-Capacitor DC-DC Converters, " In *IEEE Journal of Solid-State Circuits*, vol. 46, no. 9 (2011), 2120-2131.

[15] A. Singh, M. Kar, S. K. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "Improved Power/EM Side-Channel Attack Resistance of 128-Bit AES Engines With Random Fast Voltage Dithering," in *IEEE Journal of Solid-State Circuits*, vol. 54, no. 2, pp. 569-583, Feb. 2019.