Monolithic 3D Integrated Encryption Core

Ivan Miketic and Emre Salman
Department of Electrical and Computer Engineering
Stony Brook University
Stony Brook, NY
[ivan.miketic, emre.salman]@stonybrook.edu

***Abstract*—Monolithic 3D ICs have vertical interconnects that are comparable in size to local vias, thereby permitting extremely fine-grained vertical integration. SIMON, a lightweight block cipher, is designed and characterized at the GDS level in two types of monolithic 3D design styles: transistor-level, where nMOS and pMOS transistors are split between tiers, and gate-level, where individual gates are partitioned among the tiers. The two 3D implementations as well as a 2D implementation are compared and characterized in terms of area and power. Furthermore, the effect of monolithic inter-tier vias (MIVs) on power and data integrity is analyzed for each custom 3D design. It is shown that power delivery for transistor-level monolithic 3D design is more challenging since all of the pMOS transistors (that are connected to the supply voltage) are located in the bottom tier where there are limited metal resources due to technology constraints.**

***Keywords*—Monolithic 3D integration; power integrity; power delivery networks; ground bounce**

I. Introduction

Monolithic 3D (Mono3D) integration, unlike other vertical integration technologies, provides unprecedented device and interconnect density [1]. Furthermore, Mono3D integration is compatible with emerging memory architectures and device technologies, making it very promising as a "More than Moore" implementation. For example, carbon nanotube based field effect transistor (CNFET) logic and resistive random acccess memory (RRAM) layers have been implemented in Mono3D SoCs [2]. In Mono3D ICs, communication between tiers is achieved through monolithic inter-tier vias (MIVs), which have comparable dimensions to local metal vias. Thus, MIVs are several orders of magnitude smaller than through silicon vias (TSVs) [3].

There are various design styles associated with Mono3D ICs, as shown in Fig. 1. The primary approaches are transistor-level, gate-level, and block-level integration. Transistor-level Mono3D involves placing nMOS and pMOS transistors within different tiers and represents the finest-grained integration. Furthermore, it allows for optimization of top and bottom tier devices. This design style requires the development of a new standard cell library, but allows for existing EDA tools (developed for 2D flows) to be used with minor modifications [4].

Gate-level integration allows for individual gates to be placed in either tier. This approach permits the use of existing 2D standard cell libraries, but requires a partitioning method and development of EDA algorithms to take into account the vertical dimension for cell placement [5].

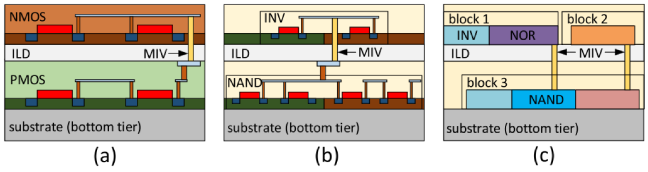

Fig. 1. Design styles for Mono3D technology: (a) transistor-level, (b) gate-level, (c) block-level.

Block-level integration involves having functional blocks of a design split between tiers [6]. Since this approach does not fully take advantage of the fine-grained vertical integration that is facilitated by Mono3D technology, it is not considered in this work.

In this paper, a previously developed Mono3D process design kit (PDK) and cell library [7]–[10] are extended for gate-level integration, while supporting a fully custom design methodology. This methodology is used to design a lightweight encryption core, SIMON, in both transistor-level and gate-level implementations. SIMON is a lightweight block cipher designed for the Internet-of-things (IoT) devices and optimized for compact hardware implementations [11]. In this work, emphasis is placed on the Mono3D power delivery architectures and analyzing characteristics such as ground bounce and power integrity, for both transistor-level and gate-level Mono3D implementations. A 2D implementation is also developed with a custom design methodology as a basis of comparison.

The rest of this paper is organized as follows. Section II provides a background of the design used. Section III discusses the various 3D power distribution networks analyzed in this work. In section IV, simulation results on ground bounce and power integrity are shown for different power distribution networks. Finally, the paper is concluded in Section V.

II. Background on SIMON

Most IoT devices are resource constrained in terms of both area and power [12], [13]. Many encryption algorithms are too computationally complex to be viable for such use cases. SIMON is a Feistel based block cipher developed by the National Security Agency (NSA) for the era of ubiquitous computing. It is lightweight and optimized for hardware implementations

This research is supported by the National Science Foundation (NSF) under grant numbers 1253715 and 1717306.

TABLE I
SIMON PARAMETERS

block size (bits)	key size (bits)
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

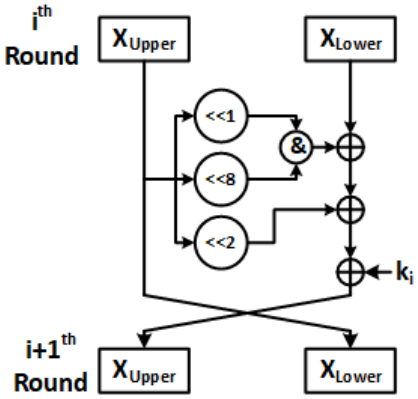

Fig. 2. Round function of SIMON.

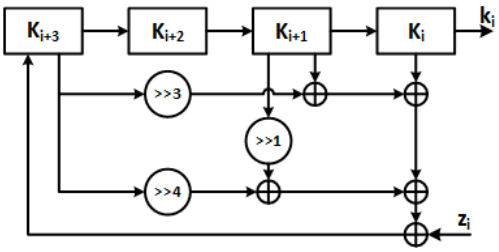

Fig. 3. SIMON key expansion for m=4.

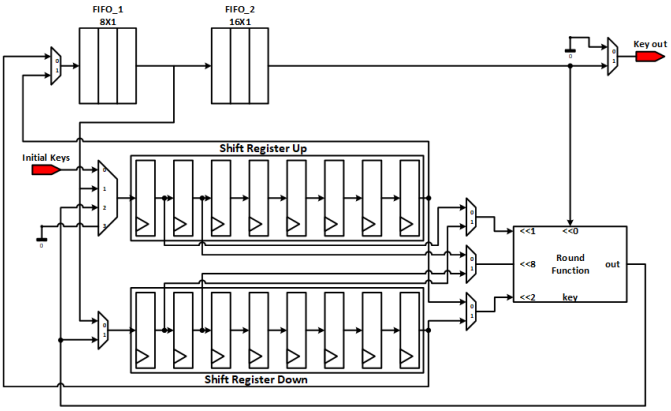

Fig. 4. Bit serialized round function.

(unlike its sister algorithm SPECK), allowing for good performance regardless of platform (ASIC or FPGA) [14]. SIMON was found to have roughly half the footprint of AES in various hardware implementations while meeting satisfactory security requirements [15]. Furthermore, it provides flexible levels of security with ten configurations, as listed in Table I, with a key size of *mn* and a block size of *2n*, where m is the number of keys and n is the word size [15]. An appropriate block and key size must be chosen to fit the required security level of the application. The flexibility of SIMON makes it attractive for a variety of use cases, particularly in IoT applications such as RFID sensor networks, smart cards. This paper is focused on a 32/64 SIMON implementation, meaning that 32 bits of plain-text are encrypted with a 64 bit key in 32 rounds (m=4, n=16). This is the smallest configuration of SIMON and was chosen to minimize area and complexity of the design.

A. Round Function

The operation of the round function for all configurations of SIMON is shown in Fig. 2. The input is split into two words and ran through a series of left circular shifts, bitwise XORs, and bitwise ANDs. At the end of each round, the two word blocks hold the input text for the next round. In each round, X_{upper} performs the operations to compute cipher text, while the current bits in X_{upper} are saved into X_{lower} for use in the next round. After a certain amount of rounds, depending on which configuration of SIMON used, the final cipher text is generated.

B. Key Expansion

The SIMON block cipher uses a different key in each round, as generated by the key expansion function. The operations used are bitwise XOR and right circular shifts. Also, a single bit round constant Z_i is used to eliminate slide properties, circular shift symmetries and introduce randomness [11]. It is important to note that SIMON has multiple key functions depending on what security configuration is chosen (the number of key words *m*), this paper uses the key expansion function for m=4. As shown in Fig. 3, K_i is the key for the current round, which is written to the highest block K_{i+3}. All of the keywords are then shifted one block to the right.

C. Bit Serialized Architecture

Different levels of parallelism (bit level, round level, and encryption level) can be achieved when designing a block cipher [16]. In this work, a bit serialized implementation is used from [17] to fully mimic resource critical IoT devices. This is a FIFO based implementation where the parallelism level is one bit of one round of one encryption engine per clock cycle. The round and key expansion functions for the bit serialized implementation are shown, respectively, in Fig. 4 and Fig. 5. A benefit of this design implementation is that it has the smallest area and lowest power consumption, at the expense of a lower throughput than more parallelized approaches.

Three fully custom SIMON cores are developed in 2D, transistor-level Mono3D and gate-level Mono3D technologies to evaluate the effect of number of MIVs and various power delivery networks. The three designs are also characterized in terms of area and power.

III. PROPOSED IMPLEMENTATION

The proposed implementations in this work utilize a fully functional PDK and cell library developed for transistor-level

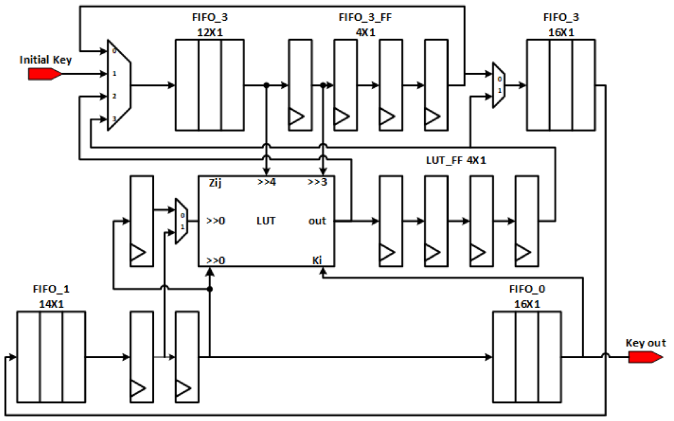

Fig. 5. Bit serialized key expansion.

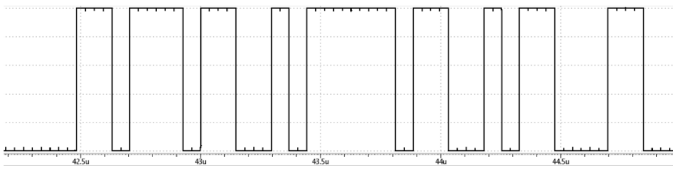

Fig. 6. Functional verification of the SIMON32/64 core in 2D implementation.

monolithic 3D ICs in the 45 nm technology node [7]. This library has been extended in this work to gate-level Mono3D implementation. The primary focus is on power delivery and the effect of number of MIVs on the power supply noise.

It is important to note that current Mono3D fabrication technology causes degraded devices in the top tier due to stringent process temperature requirements [18]. Thus, the pMOS devices of the transistor-level design are placed in the bottom tier (due to inherent lower mobility). To fully mimic fabrication capabilities, the Mono3D library has two metal layers in the bottom tier and 10 metal layers in the top tier. Since SIMON is designed in full custom methodology, the partitioning of the gates among the two tiers (for gate-level Mono3D) is achieved while considering overall area as well as connectivity among cells (interconnect length). The gate-level design uses the 45 nm standard cell library from *Nangate* [19].

Correct operation of the SIMON cores is verified for each implementation. The test vectors consist of initial keys `16'h 1918 1110 0908 0100` and plain-text `8'h 6565 6877`. The correct output of `8'h c69b e9bb` is obtained, as shown in Fig. 6 for the 2D implementation. Note that the encrypted output signals from the monolithic 3D implementations also demonstrate accurate results, but with degraded power/data integrity (depending upon the power network and MIV number) due to ground bounce, as further discussed in Section IV.

A. Power Delivery Networks in Mono3D ICs

The power delivery networks explored within this work are a routed network and power grid [20], [21]. The transistor-level Mono3D design uses a routed network. The gate-level Mono3D design is implemented with both a routed network

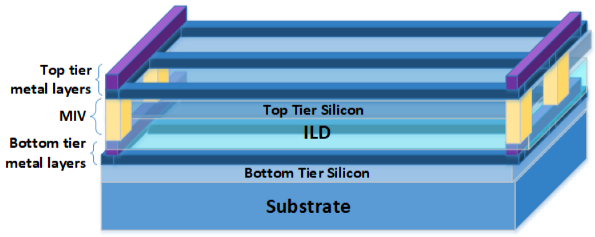

Fig. 7. Routed power network in monolithic 3D technology.

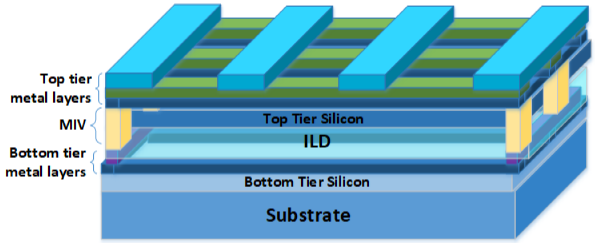

Fig. 8. Power grid network in monolithic 3D technology.

and power grid. The number of MIVs within the power grid is varied for the gate-level Mono3D design to evaluate the effect on power supply noise and ground bounce. Designing power delivery networks for monolithic 3D ICs is challenging due to limited metal resources within the bottom tier, which contains approximately half of the design.

In transistor-level Mono3D, all of the pMOS devices are in the bottom tier, which has only two metal layers. Thus, it is not suitable for a power grid. Alternatively, a grid in the upper tier would need considerable vias and MIVs, thereby causing routing blockages. The routed network connects all of the power rails within the bottom tier and has MIVs and via-stacks run across the vertical sides of the power rails to connect with top tier since power pins are only available within the top tier. An example of a routed power network in Mono3D ICs is shown in Fig. 7.

The power grid network in the gate-level implementation is designed in a similar fashion. The power and ground rails in the bottom tier have via stacks and MIVs going to the upper metal layers in the top tier, but on both the horizontal and vertical rails within the design. This approach reduces the overall impedance. Then, in the upper tier, a two layer grid is designed. An example power grid in Mono3D ICs is shown in Fig. 8.

IV. Simulation Results

The bit serialized SIMON32/64 block cipher is designed in 2D, Mono3D transistor-level, and Mono3D gate-level, all using 45 nm CMOS technology. All of the circuits are powered with a DC source of 1 V and have a clock frequency of 13.56 MHz. The layouts of the 2D, transistor-level and gate-level Mono3D implementations of SIMON are depicted in Fig. 9.

A. Power and Area Characterization

The power consumption for all implementations of SIMON is listed in Table II. Since device power dominates due to relatively small dimensions, the power consumption is similar in all implementations. Transistor-level Mono3D consumes

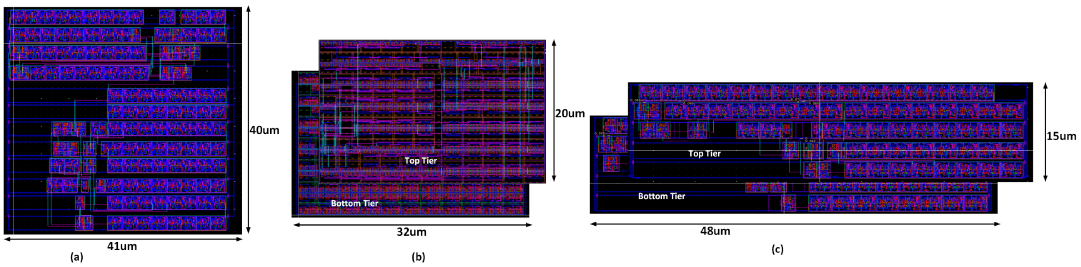

Fig. 9. Full custom SIMON layout Views: (a) 2D, (b) transistor-level Mono3D, (c) gate-level Mono3D.

TABLE II
COMPARISON OF 2D, 3D TRANSISTOR-LEVEL AND 3D GATE-LEVEL MONO3D SIMON IMPLEMENTATIONS.

SIMON Core	Average Power	Area (μm^2)	Footprint (μm x μm)
2D Schematic	75.44 μW	N/A	N/A
2D Layout	87.29 μW	1638.24	41x40
Transistor-level Routed	86.71 μW	1289.01	32x20
Gate-level Routed	85.84 μW	1427.17	48x15
Gate-level Grid	86.38 μW	1427.17	48x15

approximately 10% less footprint than gate-level due to more fine-grained 3D integration. The transistor-level and gate-level designs have approximately 60% and 50% smaller footprints, respectively, than the 2D design. The 2D design is more than twice as large as the two 3D designs because of the custom design methodology prioritizing interconnect length over area.

TABLE III
PARTITIONING OF GATE-LEVEL SIMON.

Tier	Average Power
Top	34.77μW
Bottom	40.67μW

B. Gate-Level Design Partitioning

Manual partitioning is used for the gate-level Mono3D design since SIMON is a sufficiently small circuit. In order to verify that the gate-level design was evenly split, different power supplies were connected to the gates corresponding to each tier. At the schematic level, the average power of each tier was determined, as listed in Table 2. The slight mismatch in bottom and top tier power consumption is due to prioritizing overall interconnect length during partitioning.

C. Power Supply Noise

Power integrity is an important concern for monolithic 3D ICs due to the fine grained MIVs permitting highly parallel and dense designs. The average power supply noise in the gate-level Mono3D SIMON implementation with a power grid is 1 mV and the peak power supply noise is 67 mV. For the transistor-level Mono3D implementation, these numbers are, respectively, 3 mV and 181 mV, as depicted in Fig. 10. This result is expected due to the power grid used in gate-level implementation. Since all of the pMOS devices are placed within the bottom tier (where there are limited metal resources)

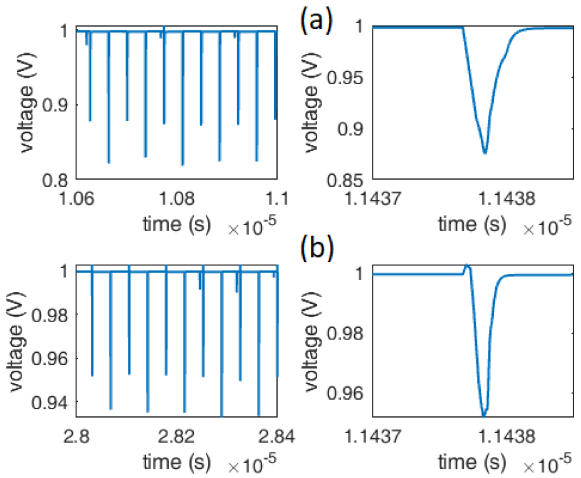

Fig. 10. Time domain power supply noise and zoomed view: (a) transistor-level, (b) gate-level.

in transistor-level Mono3D, satisfying power integrity is significantly more challenging.

D. Effect of Ground Bounce on Data Integrity with Varying Number of MIVs

Similar to stacked 3D systems where TSVs impact both power and signal integrity [22], [23], MIVs play a critical role in ensuring these design objectives in Mono3D ICs. Specifically, significant ground bounce was experienced during the rising and falling edges of the clock signal. The number of MIVs was varied to see the effect of ground bounce on data signals (ciphertext). This analysis was performed for the Mono3D gate-level design with the power grid. In each case, the MIVs are distributed homogeneously along the vertical sides of the power and ground rails. The negative effect of ground bounce on data signals was significantly reduced with approximately 21 MIVs. However, the effect of increasing the number of MIVs saturated once 150 MIVs were inserted, as shown in Fig. 11. Note that if the number of MIVs is not sufficient, significant voltage spikes can be observed, such as the 0.49 V at logic high. Thus, ensuring a certain number of MIVs connecting the power distribution networks among tiers is a critical component to mitigate the effects of ground bounce on data integrity.

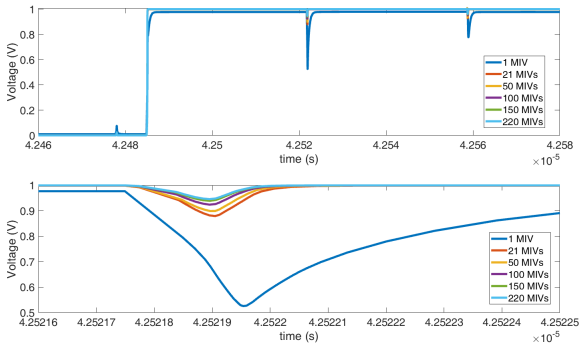

Fig. 11. The effect of ground bounce on output data (ciphertext) integrity (top) and zoomed view (bottom) as a function of number of MIVs.

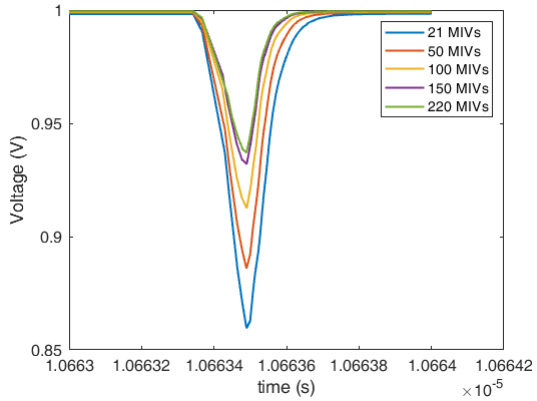

Fig. 12. Effect of number of MIVs on peak power supply noise.

E. Effect of Number of MIVs on Power Supply Noise

The number of MIVs in the power grid of the gate-level Mono3D SIMON is varied and the effect on peak power supply noise is analyzed. When there are only 21 MIVs in the power distribution network, the peak power supply noise is 146 mV. Increasing the number of MIVs to 50 and 100 alleviates this issue by decreasing the peaks to 118 mV and 92 mV, respectively. The power supply noise approximately stabilizes when there are 150 MIVs in the PDN, where the peak power supply noise is 73 mV. With 221 MIVs, there is a peak voltage drop of 67 mV. Thus, the number of MIVs has significant impact on power integrity in Mono3D ICs.

V. Conclusion

Three full custom implementations of the SIMON block cipher are realized in 1) conventional 2D technology, 2) transistor-level Mono3D technology, and 3) gate-level Mono3D technology. These three implementations are characterized and compared in terms of area and power at the same performance. A routed power network and a grid based power network are developed and compared for the Mono3D implementations. Simulation results demonstrate that it is more challenging to ensure power integrity in transistor-level Mono3D ICs. Furthermore, the effect of number of MIVs on both ground bounce and peak power supply noise is studied.

References

[1] C. Liu and S. K. Lim, "A design tradeoff study with monolithic 3d integration," in *Quality Electronic Design (ISQED), 2012 13th International Symposium on*. IEEE, 2012, pp. 529–536.

[2] M. M. Shulaker, T. F. Wu, A. Pal, L. Zhao, Y. Nishi, K. Saraswat, H.-S. P. Wong, and S. Mitra, "Monolithic 3d integration of logic and memory: Carbon nanotube fets, resistive ram, and silicon fets," in *Electron Devices Meeting (IEDM), 2014 IEEE International*. IEEE, 2014, pp. 27–4.

[3] S. K. Samal, D. Nayak, M. Ichihashi, S. Banna, and S. K. Lim, "Monolithic 3d ic vs. tsv-based 3d ic in 14nm finfet technology," in *Proc. SOI-3D-Subthresh. Microel. Tech. Unified Conf*, 2016, pp. 1–2.

[4] Y.-J. Lee, D. Limbrick, and S. K. Lim, "Power benefit study for ultra-high density transistor-level monolithic 3d ics," in *Proceedings of the 50th Annual Design Automation Conference*. ACM, 2013, p. 104.

[5] S. A. Panth, K. Samadi, Y. Du, and S. K. Lim, "Design and cad methodologies for low power gate-level monolithic 3d ics," in *Proceedings of the 2014 international symposium on Low power electronics and design*. ACM, 2014, pp. 171–176.

[6] S. Panth, K. Samadi, Y. Du, and S. K. Lim, "Power-performance study of block-level monolithic 3d-ics considering inter-tier performance variations," in *Design Automation Conference (DAC), 2014 51st ACM/EDAC/IEEE*. IEEE, 2014, pp. 1–6.

[7] C. Yan and E. Salman, "Mono3d: Open source cell library for monolithic 3-d integrated circuits," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 3, pp. 1075–1085, 2018.

[8] C. Yan, S. Kontak, H. Wang, and E. Salman, "Open source cell library mono3d to develop large-scale monolithic 3d integrated circuits," in *IEEE Int. Symp. on Circuits and Systems*, May 2017.

[9] C. Yan and E. Salman, "Routing congestion aware cell library development for monolithic 3d ics," in *Proceedings of the IEEE International Conference on Rebooting Computing*, November 2017.

[10] C. Yan, J. Dofe, S. Kontak, Q. Yu, and E. Salman, "Hardware-efficient logic camouflaging for monolithic 3d ics," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 6, pp. 799–803, June 2018.

[11] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The simon and speck lightweight block ciphers," in *Design Automation Conference*, 2015, pp. 1–6.

[12] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[13] T. Wan, E. Salman, and M. Stanacevic, "A new circuit design framework for iot devices: Charge recycling with wireless power harvesting," in *Circuits and Systems (ISCAS), 2018 IEEE International Symposium on*, May 2016, pp. 2046–2049.

[14] T. Wan and E. Salman, "Ultra low power simon core for lightweight encryption," in *Circuits and Systems (ISCAS), 2018 IEEE International Symposium on*. IEEE, 2018, pp. 1–5.

[15] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Simon and speck: Block ciphers for the internet of things." *IACR Cryptology ePrint Archive*, vol. 2015, p. 585, 2015.

[16] A. Aysu, E. Gulcan, and P. Schaumont, "Simon says, break the area records for symmetric key block ciphers on fpgas." *IACR Cryptology ePrint Archive*, vol. 2014, p. 237, 2014.

[17] E. Gulcan, A. Aysu, and P. Schaumont, "A flexible and compact hardware architecture for the simon block cipher," in *Int. Workshop on Lightweight Cryptography for Security and Privacy*. Springer, 2014, pp. 34–50.

[18] P. Batude, M. Vinet, A. Pouydebasque, C. Le Royer, B. Previtali, C. Tabone, J.-M. Hartmann, L. Sanchez, L. Baud, V. Carron *et al.*, "Advances in 3d cmos sequential integration," in *Electron Devices Meeting (IEDM), 2009 IEEE International*. IEEE, 2009, pp. 1–4.

[19] J. Knudsen, "Nangate 45nm open cell library," *CDNLive, EMEA*, 2008.

[20] E. Salman and E. G. Friedman, *High Performance Integrated Circuit Design*. McGraw-Hill, 2012.

[21] S. M. Satheesh and E. Salman, "Power distribution in tsv based 3d processor-memory stacks," *IEEE Journal on Emerging and Selected Topics in Circ. and Sys.*, vol. 2, no. 4, pp. 692–703, December 2012.

[22] H. Wang and E. Salman, "Decoupling capacitor topologies for tsv-based 3d ics with power gating," *IEEE Trans. on Very Large Scale Integration (VLSI) Systems*, vol. 23, no. 12, pp. 2983–2991, December 2015.

[23] H. Wang, M. H. Asgari, and E. Salman, "Compact model to efficiently characterize tsv-to-transistor noise coupling in 3d ics," *Integration, the VLSI Journal*, vol. 47, no. 3, pp. 296–306, June 2014.