International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Issue: 09 | Sep 2023 www.irjet.net p-ISSN: 2395-0072

IMPLEMENTATION AND PARAMETER ANALYSIS OF CRYPTOGRAPHY TECHNIQUES IN 5G USING XILINX

Miss. Sonal S. Newaskar [1], Dr. Komal P. Kanojia [2], Dr. Bharti Chourasia [3]

[1]P.G. Scholar, Dept. of Electronics & Communication Engineering, SRK University, Bhopal, M.P., India
[2]Professor, Dept. of Electronics & Communication Engineering, SRK University, Bhopal, M.P., India
[3]Professor, Dept. of Electronics & Communication Engineering, SRK University, Bhopal, M.P., India

---

Abstract - *The Internet of Things (IoT) has gained significant traction, especially with the emergence of 5G technology, owing to its diverse range of applications across various industries. However, the rapid expansion of Industrial IoT and industrial control procedures has exposed critical infrastructure to heightened vulnerabilities from cyber-attacks. To mitigate this security risk, lightweight cryptography has been developed, tailored specifically for resource-constrained devices like RFID tags, smart cards, and wireless sensors. There is a wide array of lightweight cryptographic algorithms, each designed with a particular application in mind. These algorithms exhibit varying levels of hardware and software performance under different conditions.*

In today's evolving technological landscape, where IoT and cyber-physical systems (CPS) are at the forefront, the paramount importance of security and privacy cannot be overstated. Lightweight cryptography assumes a crucial role in safeguarding data within this pervasive computing environment. The primary objective of this thesis is to develop a VLSI architecture that excels in both high performance and efficient resource utilization, and subsequently, compare the outcomes with the current Cypher. This cryptographic algorithm will be employed for both encryption and decryption processes.

The widespread adoption of IoT technologies has raised legitimate concerns regarding data security and privacy. As these technologies become increasingly popular and widely used, the need to restrict unauthorized access to data becomes critical. Cryptography emerges as a pivotal tool for preserving data integrity, confidentiality, and user privacy in this context. In this research endeavor, a cryptographic approach is implemented for a 5G application. To simulate and evaluate the proposed approach, Verilog code is utilized within the Xilinx ISE 14.7 program. The comparative analysis with previous work demonstrates superior results, reaffirming the significance of lightweight cryptography in enhancing security and privacy in IoT and 5G applications.

Key Words: Internet of Things (IoT), FPGA, Lightweight Cryptography, Encryption,

1. INTRODUCTION

The domain of VLSI system design for the Internet of Things (IoT) offers a multitude of opportunities that extend beyond conventional semiconductor applications. While traditional system-on-chip designs often prioritize large-scale chips, IoT device design takes a different approach, emphasizing low cost and minimal power consumption.

5G, the fifth generation of cellular mobile communications, marks a significant leap forward from its predecessors, including 4G (LTE/WiMax), 3G (UMTS), and 2G (GSM) systems. The objectives of 5G implementation encompass high data rates, reduced latency, energy efficiency, cost-effectiveness, increased system capacity, enhanced security, and extensive device connectivity.

Cryptography, a discipline rooted in the science of secret codes, plays a pivotal role in ensuring the confidentiality of communications over insecure channels. It safeguards data against unauthorized access and tampering by employing cryptographic systems to transform plaintext into ciphertext, typically utilizing cryptographic keys. Cryptography holds a crucial position in securing data transmissions.

The focal point of this research revolves around the development of efficient hardware implementation techniques for the Lightweight Encryption algorithm in conjunction with the SHA/RSA algorithm. Additionally, it encompasses the design and performance evaluation of the Rijndael algorithm. Field-Programmable Gate Arrays (FPGAs) emerge as versatile integrated circuits that can be readily procured off the shelf and reconfigured by designers themselves. Through rapid reconfiguration, which merely takes a fraction of a second, an FPGA can execute entirely different functions. Within the FPGA, thousands of universal building blocks, known as configurable logic blocks (CLBs), are interconnected using programmable interconnects. This reconfigurability enables each CLB's function and its connections to be altered, ultimately resulting in a fundamentally new digital circuit.

2. LITERATURE SURVEY

Sr. No.	Author Name	Publish Details	Work	Outcome
1	J. G. Pandey	IEEE 2020	A Lightweight VLSI Architecture for RECTANGLE Cipher and its Implementation on an FPGA	Improved area and power requirement
2	T. B. Singha	IEEE 2020	Advanced Encryption Standard for IOT	Improved area and power requirement
3	A. R. Chowdhury	IEEE 2018	Modified LEA Encryption Standard	Efficiency is 18.35%
4	D. Bui	IEEE 2017	Block ciphers as advanced encryption standard	Proposed data path, 32-b key out of 128 b
5	Q. Wu	IEEE 2016	Broadcast encryption	Contributory broadcast Encryption
6	A. Moradi	IEEE 2013	14 AES ASIC cores	DPA-protected and fault attack
7	Z. Shahid	IEEE 2014	Truncated rice code is introduced for binarization of quantized transform coefficients (QTCs) instead of truncated unary code.	Experimental evaluation of the proposed algorithm and give better result.
8	M. M. Wong	IEEE 2012	CFA AES S-boxes	Throughput 3.49 Gbps on a Cyclone I

3. LIGHTWEIGHT CRYPTOGRAPHY

In the realm of IoT systems, where data from the physical world is harnessed, the process of collecting data from devices is susceptible to cyber-attacks. This vulnerability underscores the growing significance of countermeasures centered around encryption. Lightweight cryptography emerges as a pivotal encryption method, distinguished by its compact footprint and/or low computational complexity. Its primary objective is to extend the reach of cryptography into resource-constrained devices. Currently, international standardization efforts and the development of guidelines for lightweight cryptography are in progress. A particular focus within this domain is on authenticated encryption, which combines both confidentiality and data integrity safeguards. As a result, extensive research is being conducted in the field of lightweight cryptography, which maximizes the efficiency of encryption while minimizing computational demands. This lightweight cryptography is particularly well-suited for IoT devices, which must operate on limited power resources. Given that IoT devices grapple with constraints such as limited power, memory, and battery capacity, the concept of "lightweight cryptography" has gained prominence. Lightweight cryptography algorithms are intricately designed to offer robust data protection while minimizing the consumption of critical resources.

Lightweight cryptography (LWC) stands as a category of cryptographic techniques celebrated for their low computational complexity and resource-efficient nature. The rationale behind their utilization within the Internet of Things (IoT) networks becomes evident when considering the stringent resource constraints characteristic of this environment. Key attributes of 5G networks, such as low latency, high throughput, heterogeneous network architecture, and extensive device connectivity, further underscore the relevance of lightweight cryptography in securing IoT networks.

4. PROPOSED METHODOLOGY

The main contribution of the proposed research work is as followings-

- Implementing the VLSI architecture for lightweight cryptography.
- Streamlining the complexity of traditional lightweight cryptography algorithms.
- Conducting simulations using the Isim simulator and examining various parameter outcomes through test bench experimentation.
- Evaluating performance metrics and conducting a comparative analysis with existing approaches.

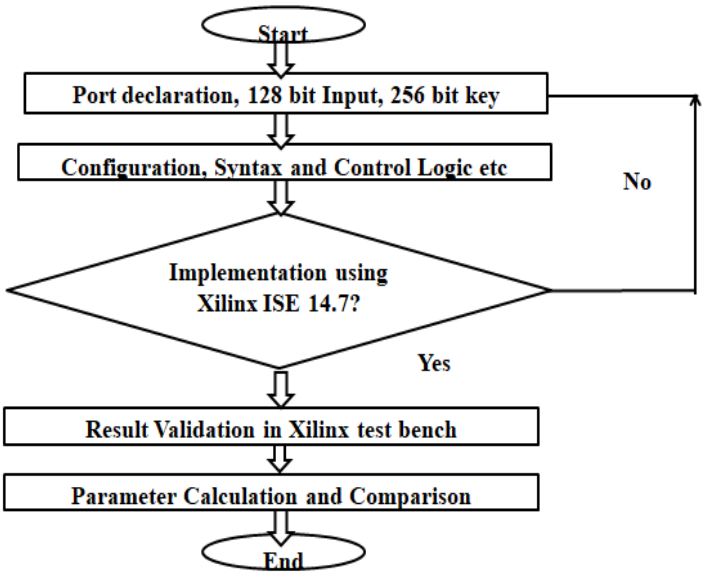

Figure 4.1: Flow Chart

Steps- Let's begin by defining the port declarations, starting with a 128-bit input and a 256-bit key.

- System configuration employing VLSI syntax and control logic.
- Processing input bytes using S-box or Sub Byte operations.
- Proceeding with the Shift Rows operation in the subsequent step.
- Applying the Mix Columns process, involving XOR operations.
- Concluding the data value round with multiple rounds or the Add Round Key operation.
- Generating the VLSI architecture's RTL view following the simulation phase.
- In the simulation step, validating and testing results against the test bench.
- Calculating various performance metrics such as latency, area, power consumption, frequency, and throughput, and comparing them with prior work.

METHODOLOGY OF PROPOSED WORK

While constructing lightweight cryptographic solutions, several recurring themes have come to light:

- **Challenges with Short Block and Key Sizes:** Short block sizes can introduce problems, such as the faster erosion of the Cipher Block Chaining (CBC) mode's security when the number of n-bit blocks encrypted approaches 2^(n/2). Similarly, a short key size can elevate the vulnerability to key-related attacks.
- **Scaling Operations with Input Size:** In symmetric lightweight cryptography, the number of operations roughly doubles as the input size of a symmetric-key primitive increases. For instance, in the PHOTON family, where the number of rounds is set at 12, the number of S-boxes increases by one each time the size is doubled. Similarly, in AES-256, with 14 rounds, the number of S-boxes doubles if the block size doubles.
- **Application-Driven Nature of Lightweight Cryptography:** Lightweight cryptography is inherently application-driven. Consequently, lightweight primitives should be designed to incorporate new academic insights and be well-suited to complement existing protocols effectively.

5. SIMULATION AND RESULTS

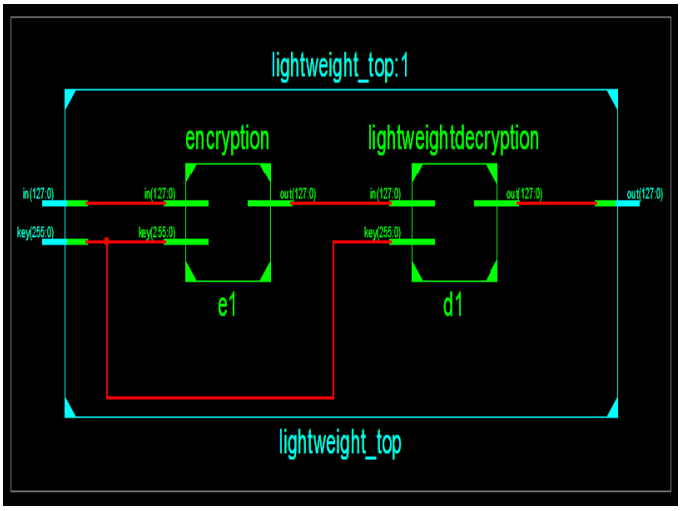

Figure 5.1: Encryption and decryption steps

Figure 5.1 illustrates the encryption and decryption steps within the RTL view, where RTL stands for Register Transfer Level.

Device Utilization Summary (estimated values)			[-]
Logic Utilization	Used	Available	Utilization
Number of Slice LUTs	12505	204000	6%
Number of fully used LUT-FF pairs	0	12505	0%
Number of bonded IOBs	512	600	85%

Figure 5.2: Device Utilization Summary

Figure 5.2 provides a summary of device utilization, offering insights into the total FPGA elements employed in the implementation.

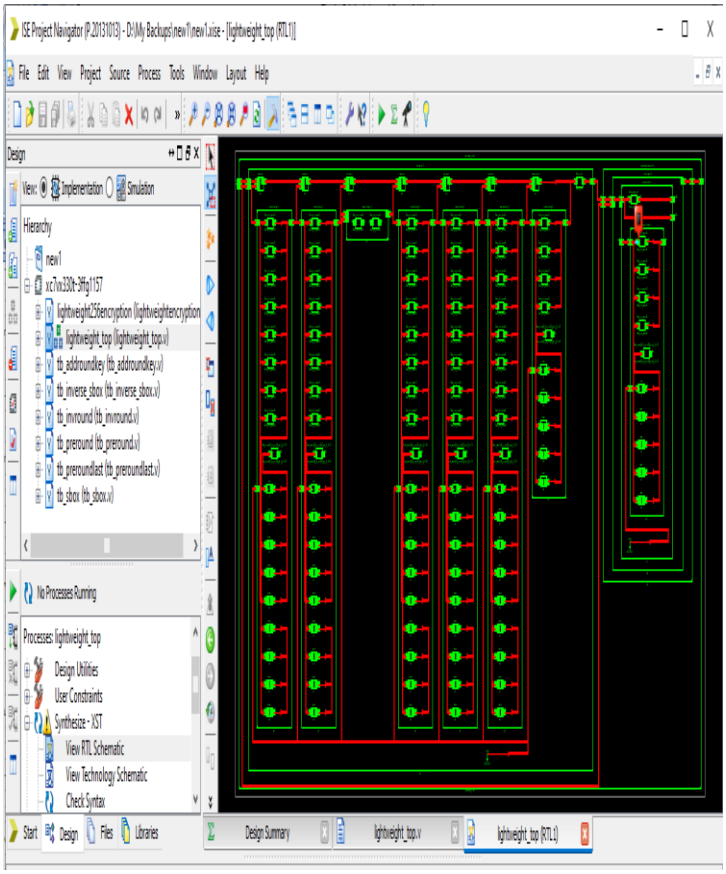

Figure 5.3: Complete RTL view

Figure 5.3 showcases the comprehensive Register Transfer Level view of the proposed implementation, displaying all the top-level logic gate views.

Sr No	Parameter	Value
1	Area	6213 LUT, 512 I/O box
2	Delay or Latency	43.398ns total, logic delay is 3.526ns
3	Power	0.18Mw
4	Frequency	23 MHz
5	Throughput	2949 Mbps
6	Memory	4726336 kilobytes

Table 5.4: Simulation Parameters

Table 5.4 details the simulation parameters utilized during the execution of the Xilinx Verilog script.

Sr No.	Parameters	Previous Work	Proposed Work
1	Input bit	80	128
2	Frequency	10 MHz	23 MHz
3	Area	28860.580	13017
4	Total Power	0.2535 mW	0.18mW
5	Throughput	250 Mbps	2949 Mbps
6	Delay or Latency	100 ns	43.398ns

Table 5.5: Result Comparison

Table 5.5 offers a comparison of results between the previous work and the proposed solution. The previous work operates on an 80-bit data input, while the proposed work employs a more secure 128-bit data input with a 256-bit key. Notably, the proposed work achieves a frequency of 23 MHz compared to the previous work's 10 MHz. Furthermore, the total throughput in the proposed work reaches 2949 Mbps, whereas the existing work achieves 250 Mbps. Additionally, the total latency is reduced to 43.39 ns in the proposed work compared to 100 ns in the previous work.

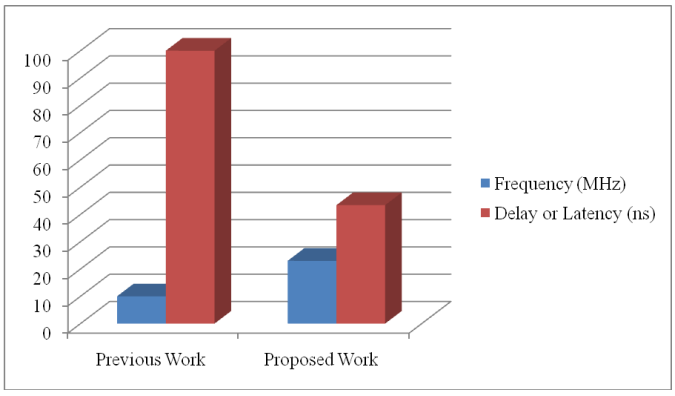

Figure 5.6: Comparison Graph-I

Figure 5.6 presents a graphical representation of frequency and latency. The graph clearly demonstrates that the proposed work attains a superior frequency with minimal latency.

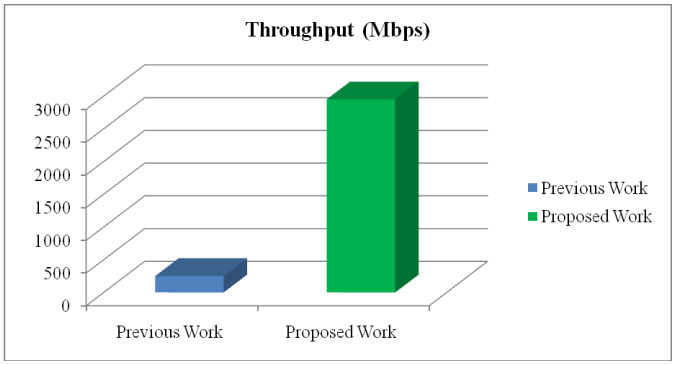

Figure 5.7: Comparison Graph-II

Figure 5.7 provides a graphical representation of throughput, showing that the proposed work delivers enhanced data speed and throughput.

6. CONCLUSION & FUTURE SCOPE

6.1 CONCLUSION

- This study focuses on the implementation of VLSI architecture for lightweight cipher in FPGA applications.
- Simulation is conducted using Verilog code with Xilinx ISE 14.7 software.
- The simulation results reveal that the previous work was based on an 80-bit data input, whereas the proposed approach employs a more secure 128-bit data input with a 256-bit key, enhancing security.
- In terms of frequency, the proposed work achieves 23 MHz, surpassing the 10 MHz frequency of the previous work. Total throughput in the proposed work reaches 2949 Mbps, compared to the existing work's 250 Mbps. Additionally, the total latency is reduced to 43.39 ns in the proposed work, compared to 100 ns in the previous work.
- Lightweight cryptography is characterized by its low computational cost. It aims to expand the utility of cryptography on resource-constrained devices, with ongoing efforts towards international standardization and guideline development. The primary objective of lightweight cryptography is to provide security solutions that require minimal memory, processing resources, and power supply, making it suitable for deployment on resource-limited devices. Lightweight cryptography is anticipated to be more efficient and faster when compared to traditional encryption methods.

6.2 FUTURE SCOPE

In the future, we can explore hybrid cryptographic techniques to enhance security in IoT applications further. Our current work is built upon a foundation of 128-bit data input with a 256-bit key, providing a higher level of security. As the size of data bits increases, we can extend the key size up to 512 bits, enabling us to transmit data securely with reduced power consumption.

- Implement LEA encryption for 512-bit and 1024-bit key lengths.
- Explore modifications to sub-byte, mix columns, or add round key operations and assess their impact, paving the way for further research into diverse modification approaches.
- Conduct practical implementations in real-time applications such as banking systems, home appliances, and the Internet of Things (IoT).
- Perform performance analysis using innovative approaches and calculate additional parameters when employing different methods.

REFERENCES

[1] J. G. Pandey, A. Laddha and S. D. Samaddar, "A Lightweight VLSI Architecture for RECTANGLE Cipher and its Implementation on an FPGA," 2020 24th International Symposium on VLSI Design and Test (VDAT), 2020, pp. 1-6, doi: 10.1109/VDAT50263.2020.9190623.

[2] P. B.S, N. K.J and N. J. C.M, "MEC S-box based PRESENT Lightweight Cipher for Enhanced Security and Throughput," 2020 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER), 2020, pp. 212-217, doi: 10.1109/DISCOVER50404.2020.9278038.

[3] B. Hajri, M. M. Mansour, A. Chehab and H. Aziza, "A Lightweight Reconfigurable RRAM-based PUF for Highly Secure Applications," 2020 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2020, pp. 1-4, doi: 10.1109/DFT50435.2020.9250829.

[4] B. Richter and A. Moradi, "Lightweight Ciphers on a 65 nm ASIC A Comparative Study on Energy Consumption," 2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2020, pp. 530-535, doi: 10.1109/ISVLSI49217.2020.000-2.

[5] P. Singh, B. Acharya and R. K. Chaurasiya, "Efficient VLSI Architectures of LILLIPUT Block Cipher for Resource-constrained RFID Devices," 2019 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 2019, pp. 1-6, doi: 10.1109/CONECCT47791.2019.9012869.

[6] R. Sadhukhan, N. Datta and D. Mukhopadhyay, "Power Efficiency of S-Boxes: From a Machine-Learning-Based Tool to a Deterministic Model," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 12, pp. 2829-2841, Dec. 2019, doi: 10.1109/TVLSI.2019.2925421.

[7] T. Chen, K. Hou, W. Beh and A. Wu, "Low-Complexity Compressed-Sensing-Based Watermark Cryptosystem and Circuits Implementation for Wireless Sensor Networks," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 27, no. 11, pp. 2485-2497, Nov. 2019, doi: 10.1109/TVLSI.2019.2933722.

[8] M. Zhang, L. Zhang, L. Jiang, F. T. Chong and Z. Liu, "Quick-and-Dirty: An Architecture for High-Performance Temporary Short Writes in MLC PCM," in IEEE Transactions on Computers, vol. 68, no. 9, pp. 1365-1375, 1 Sept. 2019, doi: 10.1109/TC.2019.2900036.

[9] M. M. Wong, V. Pudi and A. Chattopadhyay, "Lightweight and High Performance SHA-256 using Architectural Folding and 4-2 Adder Compressor," 2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2018, pp. 95-100, doi: 10.1109/VLSI-SoC.2018.8644825.

[10] S. Mandal, D. Bhattacharjee, Y. Tavva and A. Chattopadhyay, "ReRAM-based In-Memory Computation of Galois Field arithmetic," 2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), 2018, pp. 1-6, doi: 10.1109/VLSI-SoC.2018.8644772.

[11] J. G. Pandey, T. Goel, M. Nayak, C. Mitharwal, A. Karmakar and R. Singh, "A High-Performance VLSI Architecture of the Present Cipher and its Implementations for SoCs," 2018 31st IEEE International System-on-Chip Conference (SOCC), 2018, pp. 96-101, doi: 10.1109/SOCC.2018.8618487.

[12] T. Goel, J. G. Pandey and A. Karmakar, "A High-Performance and Area-Efficient VLSI Architecture for the PRESENT Lightweight Cipher," 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018, pp. 392-397, doi: 10.1109/VLSID.2018.96.

[13] V. B. Y. Kumar, D. Shah, M. Datar and S. B. Patkar, "Lightweight Forth Programmable NoCs," 2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID), 2018, pp. 368-373, doi: 10.1109/VLSID.2018.92.

[14] A. Villegas, R. Asenjo, A. Navarro, O. Plata and D. Kaeli, "Lightweight Hardware Transactional Memory for GPU Scratchpad Memory," in IEEE Transactions on Computers, vol. 67, no. 6, pp. 816-829, 1 June 2018, doi: 10.1109/TC.2017.2776908.

[15] H. M. Kamali, K. Z. Azar and S. Hessabi, "DuCNoC: A High-Throughput FPGA-Based NoC Simulator Using Dual-Clock Lightweight Router Micro-Architecture," in IEEE Transactions on Computers, vol. 67, no. 2, pp. 208-221, 1 Feb. 2018, doi: 10.1109/TC.2017.2735399.

[16] J. G. Pandey, A. Gurawa, H. Nehra and A. Karmakar, "An efficient VLSI architecture for data encryption standard and its FPGA implementation," 2016 International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA), 2016, pp. 1-5, doi: 10.1109/VLSI-SATA.2016.7593054.

[17] C. Deshpande, B. Yuce, N. F. Ghalaty, D. Ganta, P. Schaumont and L. Nazhandali, "A Configurable and Lightweight Timing Monitor for Fault Attack Detection," 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2016, pp. 461-466, doi: 10.1109/ISVLSI.2016.123