Journal of Scientific & Industrial Research
Vol. 80, June 2021, pp. 520-527

Enhanced TACIT Encryption and Decryption Algorithm for Secured Data Routing in 3-D Network-on-Chip based Interconnection of SoC for IoT Application

Jayshree[1,3]*, Gopalakrishnan Seetharaman[1,2]*, and Debadatta Pati[1,3]

[1]Department of Electronics & Communication Engineering
[2]Indian Institute of Information Technology, Tiruchirappalli, Tamil Nadu 620 015, India
[3]National Institute of Technology, Nagaland, Dimapur 797 103, India

Received 20 July 2020; revised 12 April 2021; accepted 19 April 2021

This paper presents an enhanced TACIT (E-TACIT) encryption and decryption routing technique. It protects from illegal extraction of secret data in three-dimensional (3−D) routers of Network-on-Chip (NoC) by generating HASH function-based key. The E-TACIT technique solves keys and blocks size limitation of existing anticipated methods, as it has been designed for 'n' bit key and 'n' block size. Therefore, it secures data while routing process in 3−D NoC based interconnected System-on-chips (SoCs) for Internet-of-Thing (IoT) application. The NoC based interconnection provides high scalability and requires low energy consumption for data processing than conventional bus-based SoCs. The E-TACIT has been examined for Moving Picture Experts Group (MPEG-4). The technique synthesized using Vivado 2016.2 and implemented on ZYNQ XC7Z020-CLG484 FPGA for 1024 bits and verified using a network simulator. Here, we have also incorporated pipelining, re-trimming, and clock gating techniques in the design and used Dual-Port RAM during verification, which helps in achieving low latency and high throughput and occupy less silicon in comparison to Data Encryption Standard (DES) and Advanced Encryption Standard (AES) techniques.

Keywords: Advanced Encryption Standard (AES), Application Specific Network on Chip (ASNoC), Cryptography, Internet-of-Thing (IoT), Security

Introduction

The on-chip communication technology is rapidly growing over the last two decades with the goal to optimize global interconnect performance challenges.[1] It demands designers to embed multiple Intellectual Properties (IP) on a single-chip to meet the trade-off of parameters.[2] The acceleration in the growth of the IP core of System-onChip (SoC) creates complexity challenges. With technology nodes scaling beyond 7-nanometer geometry, the primary difficulties start from Integrated Circuit (IC) manufacturing process, Outsourced Semiconductor Assembling and Testing (OSAT) to IC substrates.[3] The fulfillment of customer demands of high performance for computers, laptops, tablets, and smart-phones is expected to drive the growth of three dimensional 3−D integration, and Through Silicon Via (TSV) interconnects market by 2030.[3,4] Several researchers have focused their work on following four alternative 3−D integration technologies[5]:

- 3−D IC packaging
- 3−D IC through silicon via (3−D IC TSV)
- 3−D silicon TSV (3−D Si TSV)
- 2.5−D through silicon interposer (2.5−D TSI)

Compared with traditional 2−D SoC designing or 2−D System-in-Package (SiP), each technique has several benefits. The 3−D integration, along with novel Network-on-Chip (NoC), is the best candidate to interconnect the various Processing Elements (PE) at present and for future aspects of SoC.[6] The major components of symmetric 3−D NoC interconnection are planner and vertical TSV; 2−D and 3−D router; PE, and Network Interface (NI). The data get transferred from one PE to another PE via 2−D router and planner TSV in the same layer. In contrast, interlayers communication has been performed with the help of 3−D router and vertical TSV. The 2−D router consists of ports such as east, west, north, and south and local, which connect one or more PE, First-In-First-Out (FIFO), crossbar virtual, and switch allocator. The 3−D router is an extended form of 2−D router with two supplementary down-ward port and up-ward port. The NoC reduces the challenge of critical bandwidth limitation and needs less power consumption of global interconnects.[7] Gartner research shows demand for NoC IPs is proliferating.

*Author for Correspondence
E-mail: jay.chy@nitnagaland.ac.in; jgsraman@gmail.com

Unlike microcontroller-based modeling in the past, even resource-constrained Internet-of-Things (IoT) devices now-a-days integrate multiple NoC IPs in Multi-Processors System-on-Chip (MPSoCs). The 3−D NoC provides various new opportunities, still to address security challenges, SoCs operating in IoT applications generally integrate cryptographic hardware cores. It provides security services such as confidentiality and authentication.[8] Protecting our IoT devices and assets such as the sensor data, or encryption keys, we need to consider all security attacks such as communication, life-cycle, physical or software attacks.[9] Some research groups proposed a robust and reconfigurable verification platform for NoC in IoT SoC.[10] Namratha *et al.* proposed reconfigurable NoC for IoT based SoCs.[11] Several authors focused on the power dissipation of 2−D NoC interconnect. Moreover, very few authors addressed in 3−D NoC global interconnect with the optimizing area, delay reduction, and throughput enhancement. This study aimed to design symmetric 3−D NoC architecture with an enhanced TACIT (E-TACIT) encryption and decryption routing technique to protects from illegal extraction secret data in 3−D NoC routers with high throughput, low latency, and die area. The Key salient features of this paper are as follows.

- Proposed 3−D NoC interconnect architecture, in which 3−D router symmetrically placed.
- Two-layer vertically connected Through Silicon Via (TSVs).
- The proposed E-TACIT based secured data routing for 3−D NoC interconnection.
- Genetic algorithm (GA) based IP-core mapping onto router has been incorporated, which is nature-inspired metaheuristic optimization.
- The performance and silicon area analyzed using the XC7Z020-CLG484 ZYNQ FPGA development board.

Background and Motivation

The security attacks are becoming a major concern for on-chip communication with growing multi-cores on a single chip.[11] Various research and development performed on data securing for on-chip. Some of the highly efficient work which addresses security aspects related to the NoC interconnect discussed here. To run sensitive application Gaurav *et al.* presented a security zone with a group of IP cores, which need to be protected with key agreement protocols between two parties.[12] The data is highly secured, whereas it needs higher power consumption and also suffers thermal issues. Leandro *et al.* presented the Data Protection unit (DPU) for NoC-based systems, which has been modeled and implemented within NA/NI.[13] The DPU is capable of checking and restricting the access rights such as write, read, both, or none of the processors. The DPU unit doesn't harm the network latency if a memory request has proper rights, but it requires a larger die area. Jean *et al.* designed NoC based reconfigurable architectures for providing security on-chip based on NI implementation of distributed security rule checking and then separating security and application channels.[14] In this relative and self-complemented street-sign routing technique, introduced the discussed real-life bus-based security solution. Ahmed *et al.* presents an identity and address verification (IAV) security core.[15] It has been embedded in the router to verifi the identity and address range that has to be accessed by in-coming and out-going data packets. Yang *et al.* presents parallel and pipeline execution of ciphers to improve cryptographic block performance based on DES, triple-DES Algorithm (TDEA), and AES.[16] These encryption and decryption and checking of data integrity categories, are shown in Fig. 1 and briefly described as follows.

- *Symmetric ciphers/private key*: In this, transmitter and receiver use the identical secret key for encryption and decryption data. Symmetric ciphers classified as follows:
  - Block ciphers: It operates on the same sized blocks of plaintext/original data and ciphertext/encrypted data.
  - Stream ciphers: At a time, it converts one bit or byte plaintext to ciphertext.
- *Asymmetric ciphers/public key:* It uses a private or secret key mainly for the decryption and a related public key for encryption.

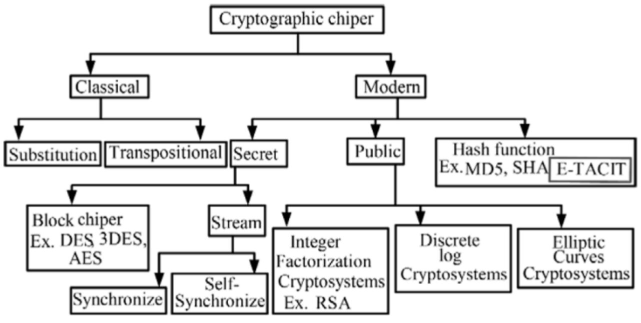
Cryptographic chiper
Classical
Modern
Substitution
Transpositional
Secret
Public
Hash function Ex.MD5, SHA
E-TACIT
Block chiper Ex. DES 3DES, AES
Stream
Synchronize
Self-Synchronize
Integer Factorization Cryptosystems Ex. RSA
Discrete log Cryptosystems
Elliptic Curves Cryptosystems

Fig. 1 — Symmetric 3-D NoC Architecture for IoT SoC Design

- *Hashing algorithms:* It gives a method of mapping messages without or with a key within fixed length value, thereby giving “signatures" for messages.

Kerakalamatti *et al.* used XY routing for packet transaction in a mesh topology, and round-robin arbiter has been used in the router and next the AES applied in the router for cryptography without virtual channel and pipelining techniques.[17] The research gap here is that traditional routing procedures have their strategies restricting the routing traffic via particular routes for specific administrative issues. These strategies-based routing intends the designer to add strategies that enable packets selectively to progress via several routes. In the structured NoC network, it demands to allow a path for secured data transaction to the destination core. This work studies several techniques for attaining security for the NoC network. The methods reviewed and examined are AES, DES, Triple DES, and so on, which have limitations on the block and key size. Therefore, to protect secret information, we have proposed E-TACIT strategies that can handle ‘n’ bits block and ‘n’ bits key size for any NoC network. It improves security in 3−D NoC architecture with the virtual channel and pipelining techniques discussed in the next section.

Architecture and Methodology for Security in 3-D NoC

The Fig. 2 has been modified; it should be noted that the E-TACIT has been examined for Moving Picture Experts Group (MPEG-4) multiprocessor system on chip (MPSoCs), and it is part of IoT application. The internal architecture of the proposed 3-D NoC interconnection subsystem with E-TACIT for MPEG-4 is shown in Fig. 2. The proposed interconnection technique gives programmability and parallelism and enhances the performance of traditional general-purpose computer execution environments by appending application-specific cores. It is flexible, has high performance, and low energy-efficiency, which leads to reduce in latency of interconnect in the edge cloud.[18] These IoT SoCs are equipped with 3−D NoC interconnect subsystem to enhance the performance of traditional general-purpose computer execution environments by appending application-specific cores. It resolves the design complexity, high latency, and low throughput issues of 2−D NoC based on-chip core interconnection in a single. We have proposed a 3−D two-layer mesh topology in which vertical interconnection interconnected TSV in a cost-efficient manner.[19] The 3−D router symmetrically placed. Here, the mesh architecture is represented in the form of X×Y×Z. For further study, a multimedia application, the mesh architecture, is considered in the matrix for as a 2×4×2 for MPEG4. The complete graphic is shown in Fig 2. Here, we have extended the virtual channel router of Dally *et al.* to 3−D with two extra port up and down.[20] The motivation for extending up-and down port is to reduce the hops count and average distance from source to destination. It improves throughput and reduce latency and energy consumption of total network. The router considered as the main core of 3−D NoC based IoT SoC design. It consists of switch allocation, routing computation unit, switch traversal, and virtual allocation. To avoid Head-of-Line (HoL) blocking while packet transaction, the Iterative-Round-Robin-Matching-with-Slip (iSLIP) scheduling was performed for virtual allocation and switch allocation.[21] However, this junction causes different security vulnerabilities in the NoC-based IoT SoCs. Therefore, we have proposed the E-TACIT routing technique, its methodology is elaborated in the next section. The GA based IP-core placement and mapping onto router

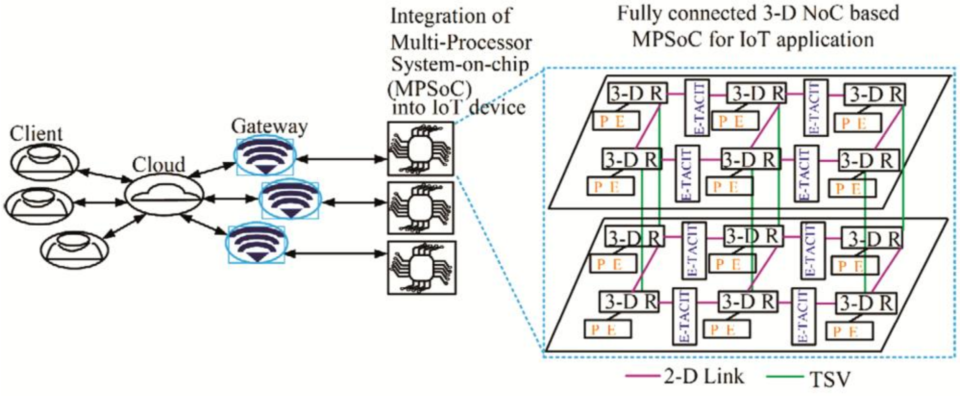

Fig. 2 — Symmetric 3-D NoC Architecture for IoT SoC Design

of 3−D NoC has been incorporated which have been detailed below.

Problem Formulation

For modeling the 3−D NoC, the optimal placement of routers and mapping cores are critical challenge to get high performance for the specific application. The mapping process was divided into two stage *i.e.* the first stage is IP core placement and second is mapping IPs onto router.

Definition 1. Objective Functions

The objective function considered is communication cost (CC), $CC_{i,j}$ described in Eq. (1) and its definition is defined below.

$$CC_{i,j} = \left(\sum_{i,j=1,1}^{n,m} D_{i,j} \right) * \left(\sum_{i,j=1,1}^{n,m} BB_{i,j} \right) \quad \dots (1)$$

where, $D_{i,j}$ is average distance between node i and node j, $BB_{i,j}$ is bisection bandwidth of interconnect, and $CC_{i,j}$ is communication cost of mapping n of commodity or core.

The total communication cost has been described in Eq. (2) defined as follows:

$$\sum_{i,j=1,1}^{n,m} CC_{i,j}\left(f, k \right) \quad \dots (2)$$

Definition 2. Fitness function

Let us assume that the mapping scheme ψ is the member of the set MAP which is consists of all mapping schemes, the proposed objective optimization problems with communication cost is defined as follows:

$$f_1 = \min(CC(\psi)) \quad (3a)$$

$$\textit{subject to } D_{i,j}\left(f, k \right) \geq 1, \quad (3b)$$

$$BB_{i,j}\left(f, k \right) \geq 1 \quad (3c)$$

The objective programming problem is transformed into the min $\sum_{\psi \in \mathrm{MAP}} f_1$

Definition 3. Constraints

Every application specific core to be mapped onto router only once as follows:

$$\sum_{r_S \in R} \mathrm{h}_{c_j} = 1, \qquad \mathrm{j} = 1, 2, \dots \mathrm{p} \quad (4)$$

Algorithm 1 GA based IP core mapping technique onto router of 3-D NoC

```
Initialize population
Set the parameter
For i=1 to max_generation
For each solution
Attain IP core communication graph
Generate placement
Compute fitness Evaluate cost function
end for select crossover mutate
upgrade the population
i=i+1 end for
output the optimal solution
```

Proposed Enhanced TACIT to Improve Security in 3−D NoC Architecture

1) ***Key generation scheme***: In cryptography, key generation is a challenging task for a cryptographer.[22–24]

In proposed work, key exchange and distribution is different than conventional symmetric key between the sender router-1 and the receiver router-1. At first random sequence ‘J’ and ‘K’ has been generated at router-1 and router-2 respectively and later it has been exchanged amongst each other. The first value of random generated sequence is considered as ‘t’ of first column in the Table 1 and Table 2. Here, key

Table 1 — Hash function H–1 and H–2

t	$s_g = s >(t,u,v)$ for H–1	$t_g = t >(s,u,v)$ for H–2
0	$s^t - s.t$	$t^u - t.u$
1	$s^u + (s + u)$	$t^v + (t + v)$
2	$s^v - (u + v)$	$t^s - (v + s)$
3	$t^u + (v.s)$	$u^v + (s.t)$
4	$t^v + (t.s)$	$u^s + (u.t)$
5	$t^s - s$	$u^t - t$
6	$u^s - s$	$v^t - u$
7	$u^t + (t + s - u)$	$v^u + (u + t - v)$
8	$u^v + (t + s + v - u)$	$v^s + (u + t + s - v)$
9	$s.t.v + (s.u)$	$t.u.s + (t.v)$

Table 2 — Hash function H–3 and H–4

t	$u_g = u >(s,t,v)$ for H–3	$v_g = v >(s,t,u)$ for H–4
0	$u^v - u.v$	$v^s - v.s$
1	$u^s + (u + s)$	$v^t + (v + t)$
2	$u^t - (s + t)$	$v^u - (t + u)$
3	$v^s + (t.u)$	$s^t + (u.v)$
4	$v^t + (v.u)$	$s^u + (s.v)$
5	$v^u - u$	$s^v - v$
6	$s^u - u$	$t^v - v$
7	$s^v + (v + u - s)$	$t^s + (s + v - t)$
8	$s^t + (v + u + t - s)$	$t^u + (s + v + u - t)$
9	$u.v.t + (u.s)$	$v.s.u + (v.t)$

generated using ‘t’ and four different hash function (H) given as $s\_g = s >(t,u,v)$ for H–1, $t\_g = t >(s,u,v)$ for H–2, $u\_g = u >(t,s,v)$ for H–3, and $v\_g = v >(t,u,s)$ for H–4 are listed in Table 1 and Table 2. In Table ‘s’ represents the number of lower-case alphabetic characters, ‘t’ represents numerical characters, ‘u’ represents upper case alphabetic characters and ‘v’ represents special characters.

2) E-TACIT encryption and decryption steps:

The E-TACIT encryption process shown in Fig. 3 (a). We have enhanced TACIT.[25] Its steps explained as follows:

1) First permutation has performed by shuffle of packets.
2) ASCII values is generated using ASCII table.
3) To perform XOR ⊕ operation using 4H-key function, key is generated.
4) Performed TACIT logic operation i.e $n^k \oplus k^k$.
5) Converted achieved value from step 4 into binary.
6) Performed bit ⊕operation.
7) Performed bit reverse operation.
8) The decimal value of preceding step value has been analyzed which is the cipher text.
9) Perform all above steps for remaining characters of the packets.

The E-TACIT decryption process is shown in Fig. 3(b). Its steps are explained as follows:

1) In chipered packet, find approximate decimal value of the 1st character.
2) Performed bit reverse operation.
3) Performed bit ⊕inverse operation i.e. J operation.
4) Performed inverse TACIT logic.
5) Next ⊕with next key value.
6) Determined character accordingly.
7) Reshuffle with the help of key.
8) Steps 1 to 6 are repeated if still achieving EoF

Implementing of Proposed enhanced TACIT in NoC Architecture

The 2−D NoC is advanced form of point-to-point (PTP), bus and crossbar on-chip interconnection.[26,27] Therefore, we have proposed the 2−D NoC-BI technique for designing Multimedia SoCs (MSoCs) which can provide low latency, energy consumption, scalability and modularity in comparison to PTP, bus and crossbar on-chip interconnection. Furthermore, to resolves the design security, complexity, high latency and low through issues of 2−D NoC based on-chip core interconnection in a single, we have proposed 3−D multi-layer chip vertical interconnection for cost efficient using of TSV.[4] Here in 3−D NoC-BI technique, the challenges targeted to solve are first, router core placement, second IP core mapping, and third providing secure routing and fourth encrypting data to be transmitted from one router to another router. The mesh topology by Kumar *et al.* considered and extended to multilayer for on-chip routers connection is shown in Fig. 2.[(28)] Here, 2−D virtual channel (VC) router by Dally *et al.* has been extended to vertical ports such as apart from east, west, north, south two extra port up and down incorporated in 3−D NoC which is shown in Fig. 4.[(20)] The router

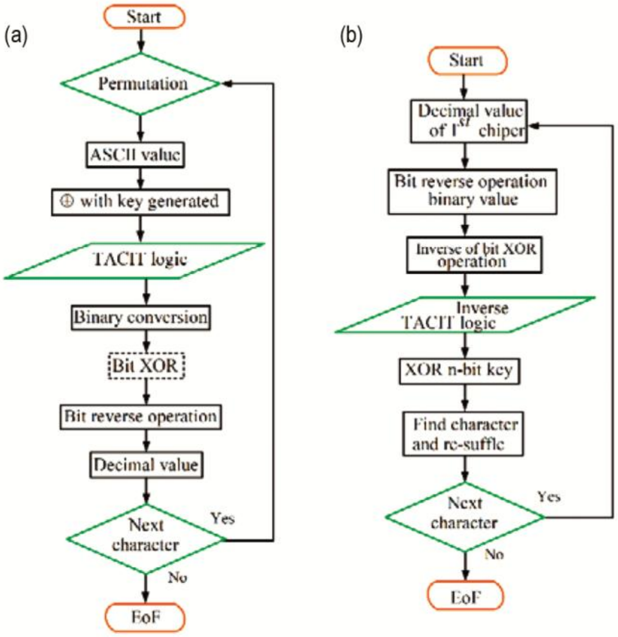

Fig. 3 — TACIT algorithm: (a) Encryption flow (b) Decryption flow.

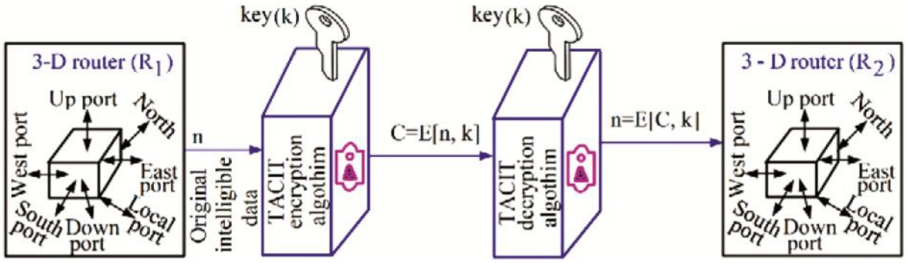

Fig. 4 — Security improvement by Enhanced TACIT in NoC Architecture.

architecture having routing computation unit for this task XYZ routing algorithm has been used. Other subcomponent of routers are virtual allocation (VA), switch allocation (SA) and switch traversal (ST).[29] Here Iterative-Round-Robin-Matching-with-Slip (iSLIP) scheduling algorithms was used for virtual allocation and switch allocation mainly to avoid Head-of-Line (HoL) blocking while packet transaction.[21] System symmetric mapping algorithm was used for traffic mapping. The complete graphics of the router-to-router dater encryption and decryption process output of source router encrypt data before sending it to other router, destination router decrypt data after receiving are shown in Fig. 4.

Results and Discussion

The architecture and methodology have been designed with Verilog hardware descriptive language, and the method used for Verilog implantation is FSM and behavioral style of modeling. The ZYNQ XC7Z020-CLG484 for 1024 bits is the target device. The length of key and size of block for different encryption algorithms have been mentioned in Table. 3.

The main aim of encryption and decryption algorithm is to provide high security. However, the preference for practice of one technique over another depends on various performance metrics such as latency, throughput and silicon area or resource utilization in encryption and decryption which depends on the structure of the algorithm. These structures are categorized based on number of rounds, the block size, and key size. Performing more rounds, provides more security, but increases the complexity problem as well; and larger key size gives higher security. The silicon area or resource utilization in encryption and decryption depends on initialization vectors, the key size, and type of operations. Here, we have compared our proposed E-TACIT algorithm with the existing work of cryptography techniques such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) for real-time MPEG-4 video applications.[30] The DES has been structured for 64-bits block with only key size 56 bits (including 8 parity bits), in 16 Feistel rounds, whereas, AES does not use Feistel network. The AES is a variant of Rijndael ciphers developed by Vincent Rijmen and Joan Daemen. It has a fixed block size of 128 and for 128-bits, 192 bits and 256 bits keys it goes through 10, 12, and 14 rounds respectively for delivering final cipher text or for retrieving original plain text. These DES and AES share same symmetric key where the distribution of key is challenging task. The proposed work is an enhanced form of TACIT which support ‘n’ bits key and block size and more efficient for key size greater than block size.[25] In comparison to DES and AES, here key selection is based on HASH function, still key distribution and bit-reverse process of 6th step can easily be predictable by attacker. In this work we have modified HASH function of four different types to generate key so that it will be difficult for invader to break the key.[25] Here, we have also incorporated Pipelining, Re-trimming, and Clock gating techniques in the design and used Dual-Port RAM during verification which helps in achieving low latency and high throughput and occupy less silicon in comparison to DES and AES. The timing report gives information about latency, total memory utilization, and the throughput value needed to design completely. Here, we have compared our algorithm with the existing work for real-time MPEG-4 video applications.[30] In comparison we have obtained the optimized results.[30] The percentage decrease in latency for encryption is 5.88% compared to DES and 2.67% compared to AES, which is shown in Fig. 5. Whereas, for decryption, it is 8.1% compared to DES and 6.05% in comparison to AES, which is shown in Fig. 6. The percentage increase in throughput for encryption is 4.26% compared to DES and 2.08%

Table 3 — Length of key and size of block for different encryption algorithms

Algorithm	Key length	Block Size
AES	128	128
DES	64	64
Proposed E-TACIT	1024	1024

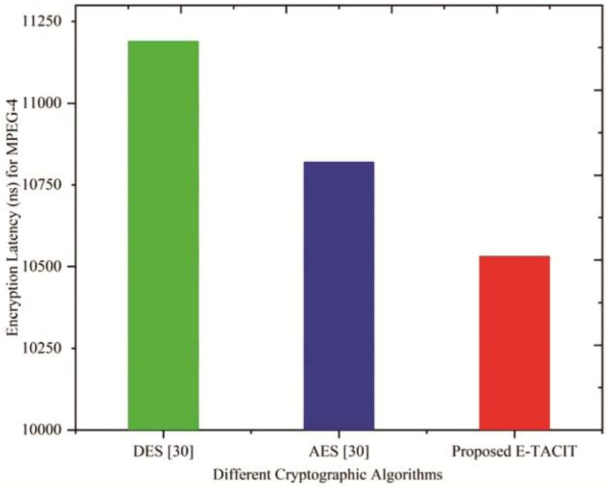

Fig. 5 — Comparison of encryption latency of DES, AES, and proposed E-TACIT cryptography algorithms

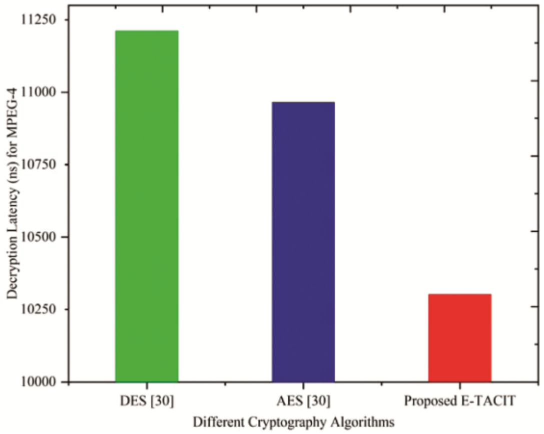

Fig. 6 — Comparison of decryption latency of DES, AES, and proposed E-TACIT cryptography algorithms

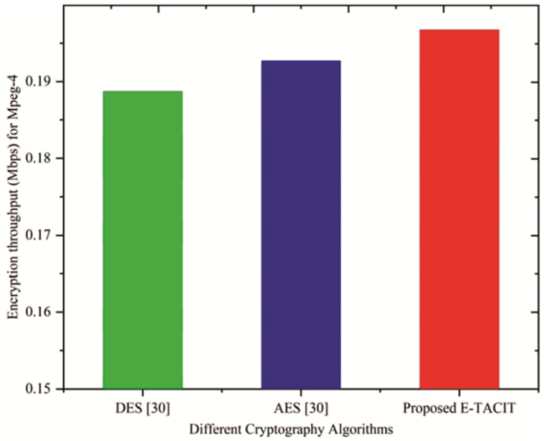

Fig. 7 — Comparison of encryption throughput of DES, AES, and proposed E-TACIT cryptography algorithms

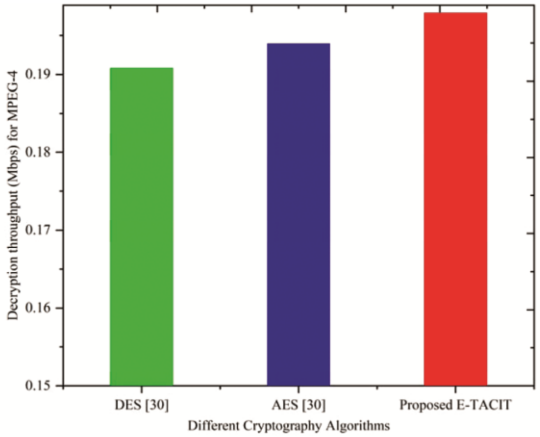

Fig. 8 — Comparison of decryption throughput of DES, AES, and proposed E-TACIT cryptography algorithms

compared to AES which is shown in Fig. 7. Whereas, for decryption, it is 2.05% compared to DES and 2.05% in comparison to AES, which is shown in Fig. 8. The silicon area decrease for encryption is

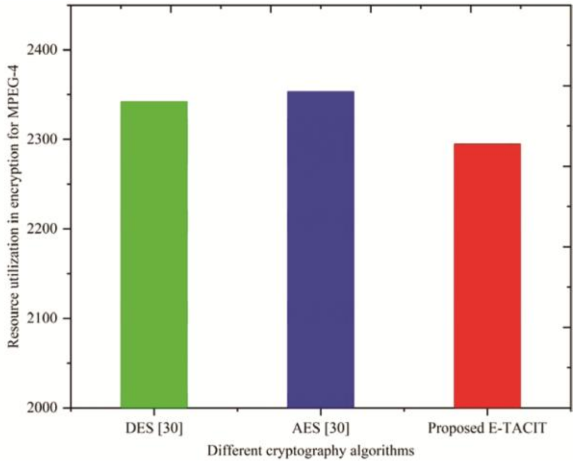

Fig. 9 — Comparison of encryption resource utilization of DES, AES, and proposed E-TACIT cryptography algorithms

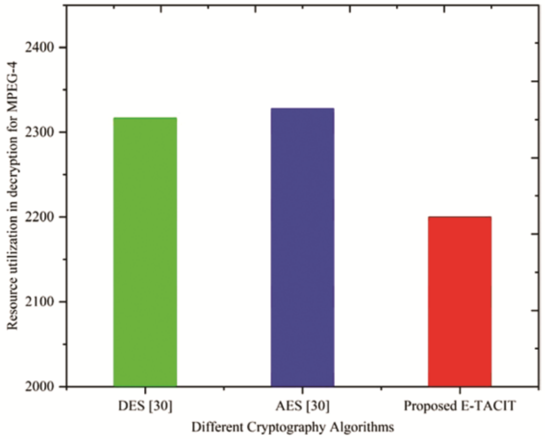

Fig. 10 — Comparison of decryption resource utilization of DES, AES, and proposed E-TACIT cryptography algorithms

2.01% compared to DES and 1.73% compared to AES, which is shown in Fig. 9. Whereas for decryption, it is 5.03% compared to DES and 5.49% in comparison to AES, which is shown in Fig. 10.

Conclusions

This paper presents E-TACIT encryption and description algorithm for secure data routing in 3−D NoC based interconnected SoCs for IoT application. One such multimedia application of IoT is tested and verified in this work. In this E-TACIT, key generation performed is based on four different kinds of the HASH function. This encryption and decryption technique helps in keeping data secure and makes it hard for the trespasser in breaking key. Further, this algorithm can be implemented in more scalable network such as 3−D NoC-bus and Wireless NoC (WiNoC) interconnect architecture, as it has low latency and high throughput and occupies less silicon in comparison to existing cryptography techniques such as DES, and AES due to incorporated pipelining, re-trimming, and clock gating techniques in the design.

References

1 Adhinarayanan S G V & Shabeer H A, ASIC implementation of one level 2DDWT and 2D DWT in hybrid wave-pipelining & pipelining, *J Sci Ind Res*, **74** (2015) 609–613.

2 Sivanantham S & Tresa T, Built-in self-test methodology for system-on-a-chip testing, *J Sci Ind Res*, **76** (2017) 149–153.

3 Lin G T R & Lee Y-C, Evaluation and decision making in Taiwan semiconductor industry through silicon via technology," *J Sci Ind Res*, **73** (2014) 456–460.

4 3D IC and TSV interconnect market expects a drastic growth, Taiwan Semiconductor Manufacturing Company Ltd., Samsung Electronics Co. Ltd., Toshiba Cor among Others, Tech Rep, (2020).

5 Lee Y-C & Chou C, Technology evaluation and selection of 3DIC integration using a three-stage fuzzy MCDM, *Sustainability*, **8** (2016) 114.

6 Kumar C & Ibrahim A, VLSI design of energy efficient computational centric smart objects for IoT, **09** (2018).

7 Ravichandran V & Venkatesan G K D P, Network on chip with CDMA technique, *J Sci Ind Res*, **73**, (2014) 209–213.

8 Indrusiak L S, Harbin J, Reinbrecht C & Sepazlveda J, Side-channel protected MPSoC through secure real-time networks-on-chip," *Microprocess Microsyst*, **68** (2019), 34 – 46.

9 "IoT security is essential, ARM, Tech Rep, (2020).

10 Nagori T K, Robust and reconfigurable verification platform for NoC in IoT soc design, *J Emerg Technol Innov Res*, **3(8)**, (2016), 16–17.

11 Patil V P N & Bhairi P, Reconfigurable NoC for IoT based SoCs, *Int J Electr Comput Sci Eng*, (2016).

12 Sharma G, Ellinidou S, Anand R, Kuchta V, Markowitch O & Dricot J-M, Secure communication on NoC based MPSoC, (2018).

13 Fiorin L, Silvano C & Sami M, Security aspects in networks-on-chips: Overview and proposals for secure implementations, *10th Euromicro Conf on Digital System Design Architectures, Methods and Tools (DSD 2007)*, (2007), 539–542.

14 Diguet J, Evain S, Vaslin R, Gogniat G & Juin E, NoC-centric security of reconfigurable SoC, *First International Symp on Networks-on-Chip (NOCS'07)*, (2007), 223–232.

15 Saeed A, Ahmadinia A & Just M, Secure on-chip communication architecture for reconfigurable multi-core systems, *J Circuits Syst Comput* (2016).

16 Yang Y S, Bahn J H, Lee S E & Bagherzadeh N, Parallel and pipeline processing for block cipher algorithms on a network-on-chip, *Sixth Int Conf on Inf Technol: New Generations*, (2009), 849–854.

17 Kerakalamatti B S & Nagraj P, Design and implementation of NoC based parallel AES computation, *IJCA Proc on National Conf on Power Systems and Industrial Automation*, NCPSIA 1, (2015), 1–4.

18 Fettweis G P, 5G and the future of IoT, *ESSCIRC 42nd European Solid-State Circuits Conf*, (2016), 21–24.

19 Tatas K, Siozios K, Soudris D & Jantsch A, *Designing 2D and 3D Network-on-Chip Architectures*. Springer Publishing Company, Incorporated, (2013).

20 Michelogiannakis G, Jiang N, Becker D & Dally W J, "Packet chaining: Efficient single-cycle allocation for on-chip networks," *44th Annual IEEE/ACM Int Symp on Microarchitecture (MICRO)*, (2011), 83–94.

21 Shahane P & Pisharoty N, "Modified x-y routing algorithm for mesh topology based noc router on FPGA," *IET Circuits, Devices Syst*, **13** (2019).

22 Gabriel I, Anghelescu P & Serban G, RSA encryption algorithm implemented on FPGA, *Int Conf on Appl Electronics*, (2011).

23 Kundi D, Zaka S, Qurat-Ul-Ain & Aziz A, "A compact AES encryption core on XILINXFPGA," *2nd Int Conf on Comput, Control and Commun*, (2009), 1–4.

24 Ghosal M B P & Biswas M, A compact FPGA implementation of triple-des encryption system with IP core generation and on-chip verification, *Int Conf on Ind Eng and Operat Manag* Dhaka, Bangladesh, (2010).

25 Crope F, Sharma A, Singh A & Pahwa N, An efficient cryptographic approach for secure policy-based routing: (TACIT encryption technique), *3rd Int Conf on Electron Comput Technol*, 5, (2011), 359–363.

26 Verma J S & Chatterjee A, A methodology for designing LVDS interface system, *Sixth Int Symp on Embedded Computing and System Design (ISED)*, (2016), 284–288.

27 Jayshree & Seetharaman G, "Design and analysis of novel interconnects with network-on-chip LVDS transmitter for low delay," in *2018 NASA/ESA Conf on Adaptive Hardware and Systems (AHS)*, (2018), 204–209.

28 Kumar S, Jantsch A, Soininen J, Forsell M, Millberg M, Oberg J, Tiensyrja K & Hemani A, A network on chip architecture and design methodology, in *Proc IEEE Computer Society Annual Symp. on VLSI. New Paradigms for VLSI Systems Design*, (2002), 117–124.

29 Gabis A B & Koudil M, NoC routing protocols - objective-based classification, *J Syst Archit*, **66–67** (2016) 14 – 32.

30 Elgeldawi E, Mahrous M & Sayed A, A comparative analysis of symmetric algorithms in cloud computing: A survey, *Int J Comput Appl*, **182** (2019) 7–16.