Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4737569, 9 pages
https://doi.org/10.1155/2022/4737569

Research Article

Architecture of Network-on-Chip (NoC) for Secure Data Routing Using 4-H Function of Improved TACIT Security Algorithm

N. Ashok Kumar[1], **G. Shyni**[2], **Geno Peter**[3], **Albert Alexander Stonier**[4], **and Vivekananda Ganji**[5]

[1]*Department of Electronics and Communication Engineering, Sree Vidyanikethan Engineering College, India*
[2]*Department of Electronics and Communication Engineering, Good Shepherd College of Engineering and Technology, India*
[3]*CRISD, School of Engineering and Technology, University of Technology Sarawak, Malaysia*
[4]*Department of Electrical and Electronics Engineering, Kongu Engineering College, India*
[5]*Department of Electrical and Computer Engineering, Debre Tabor University, Ethiopia*

Correspondence should be addressed to Vivekananda Ganji; drvivek@bhu.edu.et

Received 12 January 2022; Revised 1 February 2022; Accepted 16 February 2022; Published 9 March 2022

Academic Editor: Vinayakumar Ravi

In the technical world, NoC (network-on-chip) is a noticeable communication subsystem based on integrated circuits. It is mainly used in improving the performance of system-on-chip (SoC) by bridging the intellectual properties in the SoCs. But there is a need of protected architecture which is dealing with routing and processing data in the multicore system-on-chip (SoC). The recent issue with the above is there is still a drawback in enabling a better network routing system for accessing physical networks. The methodology of NoC mainly depends on the routing scheme, switching techniques, and structuring topologies. In this paper, we propose a new technique in implementing the chip in order to maintain the data privacy of NoC routers. There are many works with different algorithms that were evolved in enabling the secureness of NoCs, but due to the key size and block size, it is still not able to reach the expected effectiveness. Our proposed work is intended in designing a NoC architecture by means of embedding advanced TACIT security algorithm in Virtex-5 FPGA. Here, we used a hash function which is under a 4 hash function (4-H) scheme. The main advantage of this key generation scheme is it is applicable for block size and key size up to '*n*' bit. Thus, this TACIT security algorithm enables '*n*' bit using the software VHDL programming language in Xilinx ISE 14.2 and Modelsim 10.1 b which are applicable for 1024 bit and '*N*' bits of block size on Virtex-5 FPGA systems. This design system can be enhanced by improving the factors like timing parameters, supporting memory, higher frequencies, and utilized summaries.

1. Introduction

Various technical methodologies are being evolved in sharing the information either in wired or wireless networks. But the main motto or requirement to be attained in the system is that the privacy of the information should be maintained while passing over the various communication channels. But losing of information is in higher state even in the technically globalized industry [1, 2]. If we compare and discuss about any encryption algorithm, the important thing should be noticed as well as maintained is its processing speed with data privacy. Because when there is an increase in the sensitive of the information, the level of data privacy and speed are getting varied. In this concept, cryptography plays a vital role in achieving the data privacy [3, 4]. It is an art of expressing mathematical notation for encryption and decryption of data. When high sensitive data are stored or communicated, there is a possibility of privacy breach when those data are being passed through the unsecured networks. Cryptography is an art of data securing, and cryptanalysis is the concept of analyzing and damaging the secured communication systems [5]. Various kinds of cryptography techniques and algorithms used in the industry are DES, 3DES, AES, Kasumi Encryption Core, Blowfish,

RC4, and X-MODDES. Here, we compared the TACIT encryption algorithms based on the parameters like block size and key size. Next, the TACIT encryption algorithm was progressed on hardware description languages and it was analyzed with well commonly known encryption algorithms in the industry like AES as well as RSA.

1.1. Cryptography Overview. In cryptography [6, 7] the two factors involved are plain text and cipher text, in which the actual message or data to be viewed is known as plain text. Those texts which are encoded by means of key value are known as cipher text. This information is shared normally through the communication channels which are technically known as encryption. The reverse process of encryption which is being used in order to view the original text from encoding with key matching concept is known as decryption. The combination of these two processes is well known as cryptography which is involved in sharing the common or various keys in both ends. In technical factor, the sharing of the same key is called symmetric and by means of various keys is asymmetric key, respectively. Figure 1 is the pictorial representation of how the original text (X) which is getting encrypted with the (k) key value and communicated as cipher text with an expression $Y = E[K, X]$. The reverse process as mentioned above is shown by decryption algorithm with the expression $X = E[K, Y]$ and same key (K).

$$\mathbf{Y} = [\mathbf{E}, \mathbf{X}]\mathbf{X} = [\mathbf{E}, \mathbf{Y}]. \quad (1)$$

The important factor in the encryption algorithm is its secret key and key length. During the output, the key values vary by means of encryption algorithm.

According to the key values and exact substitutions, the algorithm produce varied outputs as per the key dependents. On discussing about the multiprocessor system-on-chip (MPSoC) and network-on-chip (NoC), the main drawback is maintaining the security channel. Network-on-chip is a well-known approach for designing any kind of subsystem that deals with the IP on system-on-chip. On the NoC communication architecture, the software and application layer are considered the crucial phases. If we get into a NoC template, it has a chip region and it is composed of chaining of chips. Those are physically isolated with the aid of regions through which they can communicate with each other. The switches in the architecture are composed of slots, which has computing and other resources. A resource can either be a memory, microprocessor, I/O, or FPGA resources. As the application layer is implemented by OSI layer, the resource connectivity among the network by means of switches and network interfaces. The networking services for the resources were gained by the network interfaces. The other layers implemented by network interfaces were presentation, session, and transport layers. Here, there is chain of connectivity between the switches and it is also connected to the network interfaces. The packet communication from source to destination is delivered by using the switches. The interconnection of network, data link, and physical layer is done by linking switches and metal wires. Figure 2 explains the NoC design which is structured by layer accordingly for transmitting the data. We can say a resource can be represented as fixed type or floating point. According to the presentation layer, it must be a same type for converting some process. The session layer will establish the connection between the variable resources. The transport layer undertook checking of packet loss during the transmission. The network layer is implemented by the switches, which took the responsibility of handling the network topology and handled the addressing scheme among them. The passing of data between the points are done by the data link layer and physical layer holds the electrical properties.

2. Related Works

Various research works are done in NoC architectures [5, 8] in which several gains were yielded over conventional bus architecture. Common NoC architecture is a topology-based structure especially 3D-mesh topology, which is proposed with stacked mesh in [9]. In paper [8], wormhole switching is proposed and it is suitable for dealing with high speed and low power, in which NoC structure has routing as final protocol but most of routing technique failed to design mainly on the basis of power awareness. According to the work on [10], the routing is created based on the programmable routing tables especially for dealing with the faulty links in the NoCs. In paper [11], during the communication, in order to reduce the power consumption, a three-step routing algorithm is evolved. Here, they discussed about some of the open problems in the task routing. The work on [12] is composed of dead-lock free routing and adaptive routing in minimizing the routing latency. From paper [13], they discussed about the complex dynamic routing protocol in order to shun the conflicts of data buffering raised in the networks. The deflection routing protocol is proposed in [14] which is mainly proposed for dealing with output connection problems. In addition to these, various algorithms were developed in order to improve the NoC architecture performance on various factors such as dead-lock, low power, high speed, buffer connection, and low latency. But the abovementioned algorithms failed to address the security breach among the routing packets. In architecture, during communication, if the data is not secured, it is vulnerable to various attacks. Paper [15] shows the works of proposing the TACIT algorithm for the purpose of secure data communications. It uses hash function for key selection and distributing keys. The TACIT algorithm is the well-known bit-reverse process that can be easily predictable by the attackers. In this paper, our proposed work enhanced the TACIT algorithm by using 4-H key distribution (4-types of hash function) to implement secure routing system. It is too hard for the invader to destroy advanced TACIT algorithm, because of the design used in four types of hash function while generating the keys.

3. Research Gap

The achievement of effectiveness in internetworks mainly depends on the freedom while implementing the

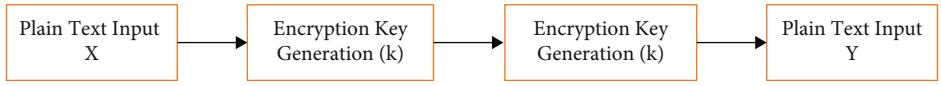

Figure 1: Symmetric encryption and decryption process.

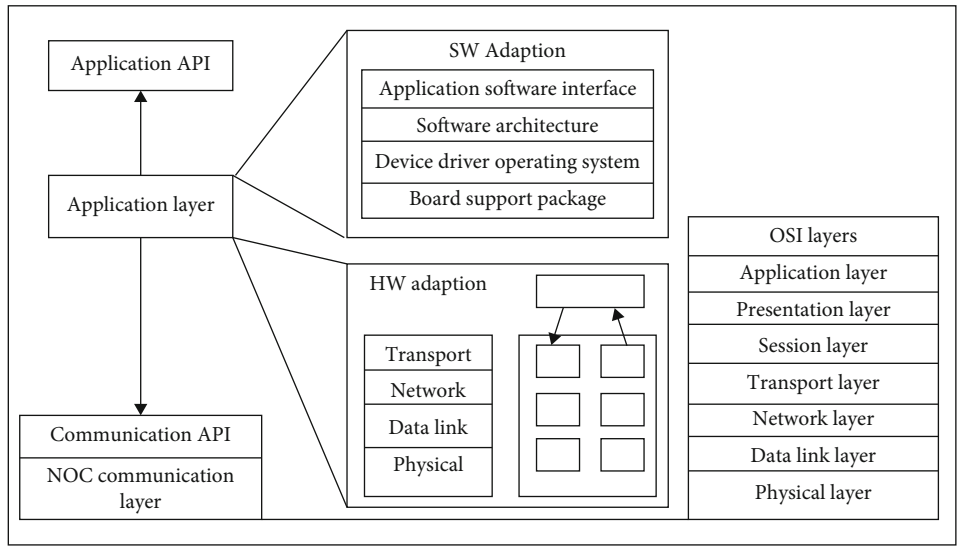

Figure 2: NoC architecture.

forwarding packets as well as routing. But traditional routing techniques have its own policies which restrict the routed traffic through specific paths for some administrative issues. These policies based routing intended the users to add policies which enable the packets selectively to pass through various paths. In a structured network, it is mainly required for a design to enable a route for secured data transmission till the destination. That is the reason for requirement in enabling secured policy based routing method. This paper analyses various methods in attaining security for networks. The methods discussed are DES, Triple DES, AES, Blowfish, RC4, Modes, and X-Modes but these have the limitation on block size and key size, in which the maximum size is 256 bits which is supported by AES algorithm. Finally, we proposed a new security algorithm known as TACIT. This TACIT is applicable for encryption and decryption on any network. The appreciable work of this proposed scheme is that it is designed to face '*n*' bits block size and '*n*' bits key size on any network. The implementation of hardware chip in the TACIT network security is proposed for future work with motto of achieving excellent result and even the key size is considered to be greater than the block size. The proposed algorithm is examined under various text files by implementing it on C, C++, C#, and Java programming languages. The TACIT can be used for encryption as well as decryption. It protects the theft of secret data in routers of network-on-chip by generating HASH key-based function. In case of proper right by the owner, the data protection unit does not create as problem to the unit. The main aim of the encryption and decryption algorithm is to provide the best secured database.

4. Proposed Key Generation Scheme

4.1. Procedure for Hash Function. We create streams A and B . Then, weexchange it. The above hash function has four cases are as follows:

Case 1: $(A = B = i_g)$ and take $'i' : x = H_1$ and $y = H_1$, where $i_g = i > (j, k, l)$

Case 2: $(A = B = j_g)$ and take $'i' : x = H_2$ and $y = H_2$, where $j_g = j > (i, k, l)$

Case 3: $(A = B = k_g)$ and take $'i' : x = H_3$ and $y = H_3$, where $k_g = k > (i, j, l)$

Case 4: $(A = B = l_g)$ and take $'i' : x = H_4$ and $y = H_4$, where $l_g = j > (i, j, k)$

Consider string A randomly at one end of transmitting such as source end and string B at receiving end. Here, both the strings were familiar among them and the hash table calculates the values between x and y. The value of random from the sender end is the range 0 to 9 with a code sequences in signifying the hash functions. It has four exist cases in order to break the key such as (i) $i_g = i > (j, k, l)$, (ii) $j_g = j > (i, k, l)$, (iii) $k_g = k > (i, j, l)$, and (iv) $l_g = j > (i, j, k)$. Table 1 shows the possible hash functions according to the proposed algorithms. In this, i_g represents the lower case alphabetic characters in the random sequence. If X and Y exchange between each other, value of 'i' is the first value which is under generated sequence. The value of x and y is generated by the value of 'i' to get the least prime numbers. This prime number is generated at both the ends by means of trial solution method. Thus, the biggest prime

Table 1: Hash table using the 4-H key.

j	Hash function			
	H_1 $i_g = i > (j, k, l)$	H_2 $j_g = j > (i, k, l)$	H_3 $k_g = k > (i, j, l)$	H_4 $l_g = l > (i, j, k)$
0	$i^j - i.j$	$j^k + j.k$	$k^l + k.l$	$l^i + l.i$
1	$i^k + (i + k)$	$j^l + (j + l)$	$k^i + (i + l)$	$l^j + (k + l)$
2	$i^l - (k + l)$	$j^i - (i + j)$	$k^j - (k + j)$	$l^k - (l + i)$
3	$j^k + (l.i)$	$i^l + (k.j)$	$k^j + (l.i)$	$l^i + (l.i)$
4	$j^l + (j.i)$	$i^k + (k.l)$	$k^j + (l.j)$	$l^i + (j.k)$
5	$j^i - i$	$i^j - j$	$k^l - l$	$l^k - k$
6	$k^i - i$	$l^j - j$	$i^k - k$	$j^l - l$
7	$k^j + (j + i - k)$	$l^i + (i + j - l)$	$j^l + (l - j - i)$	$i^k + (k - i - j)$
8	$k^l + (j + i + l - k)$	$l^k + (l + k + i - j)$	$i^j + (i + j + l - k)$	$j^i + (i + k + j - l)$
9	$i.j.l + (i.k)$	$j.k.l + (j.l)$	$i.j.k + (j.l)$	$k.l.j + (l.i)$

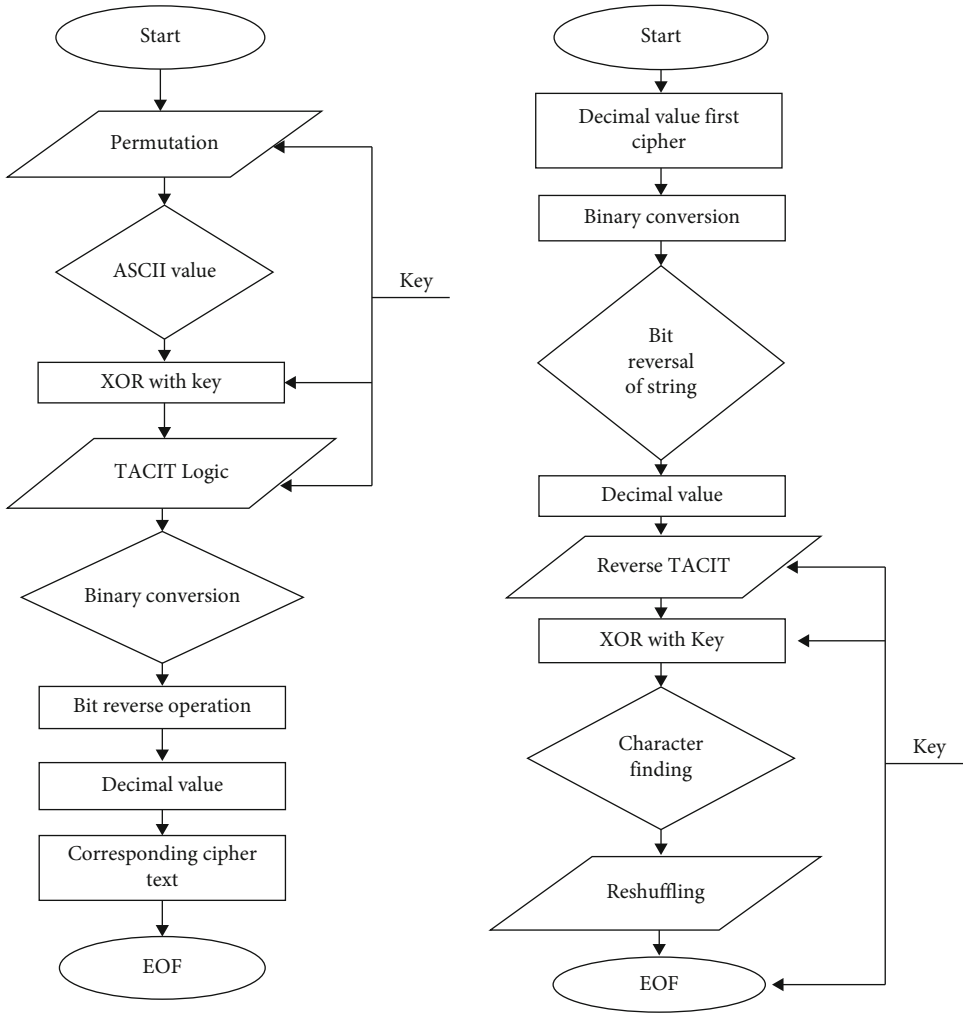

Figure 3: Encryption and decryption algorithm.

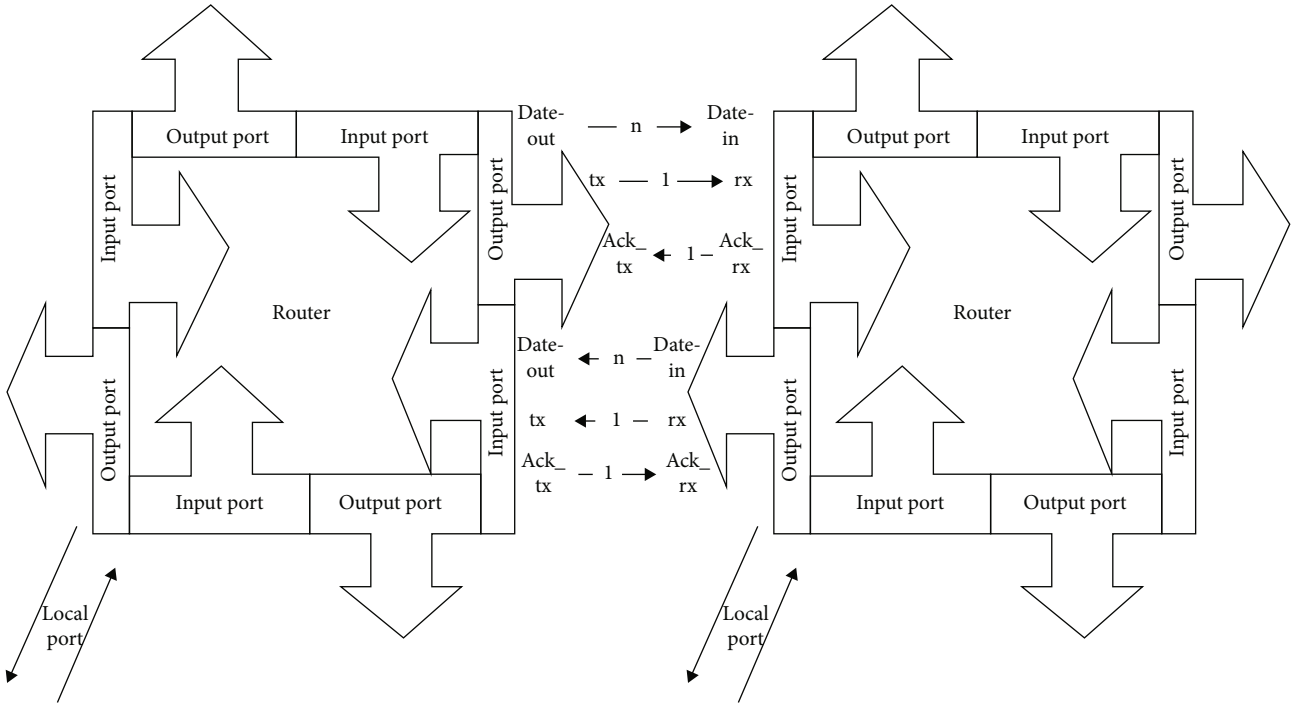

Figure 4: Router architecture of NOC.

number is between x and y with the average actual key. That generated key is proposed for processing the data encryption as well as decryption.

4.2. Key Generation

(1) Let $X = (4\text{mph}\#*\%\text{DH@897}\hat{}\text{jk\$})$ and $Y = (7\text{ln85 JZ41@!60\&gt})$

(2) For $X\{m = 4, n = 3, u = 2, v = 6\}$

(3) X satisfies V_g. Therefore, P should use hash table H4. Here $n = 4$

(4) Therefore, $P = V^m + (n.u) = >(6)^4 + (3 * 2)$

(i) $1296 + 6 = 1302$

(5) For $Y\{m = 4, n = 6, u = 2, v = 3\}$

(6) Y satisfies n_g. Therefore, Q should use Hash table H2. Here $n = 7$

(7) Therefore $Q = V^m + (m + n - v) = >(3)^4 + (4 + 6 - 3)$

(i) $81 + 7 = 88$. Key:

(8) Least prime number between 88 and $1302 = 89$. Largest prime number between 88 and $1302 = 1301$. Key = (Least Prime + Largest Prime)/2

(i) $(1301 + 89)/2.\text{Key} = 695$

4.3. TACIT Encryption Algorithm

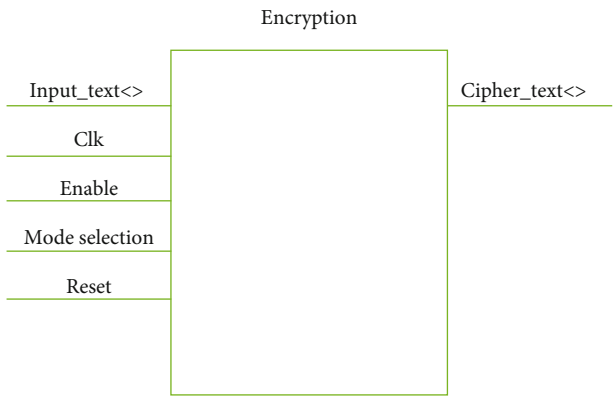

Figure 5: RTL view of developed encryption chip.

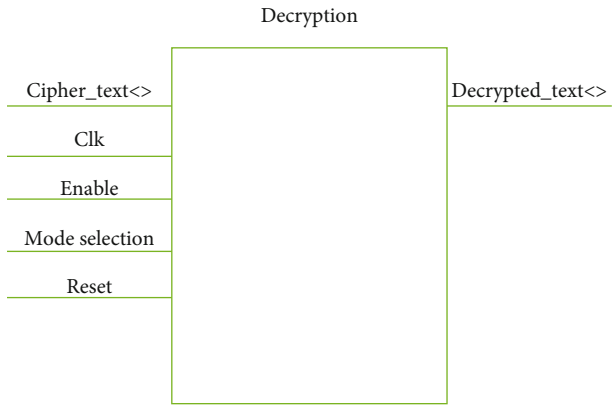

Figure 6: RTL view of developed decryption chip.

Table 2

Pins	Functional description
Reset	Used to reset sender and synchronized with clock of std_logic (1 bit)
Clk	Default input for sequential logic, rising edge of clock pulse of std_logic (1 bit)
input_text ($N-1:0$)	Input text of the encryption end it can be of 'N' bit. It is of std_logic_vector type
Decryption_text ($N-1:0$)	Decrypted text at receiving end, it is also of 'n' bit and of std_logic_vector type
Mode_Selection	1 bit input (std_logic) to select in a particular mode if mode_selection = '1' it is in encryption mode and mode_selection = '0', it is in decryption mode
Enable	1 bit input (std_logic) enable and disable the encryption logic. If enable = '1' encryption algorithms else decryption logic
Cipher_text ($N-1:0$)	Cipher text is the text which is encrypted with key at the transmitting end. It can be any garbage value and it is of std_logic_vector type

Step 1. initially the text file is viewed and process for permutation approach in order to get the shuffle position for the characters using the key value.

Step 2. the text file characters were analyzed, and ASCII values are generated accordingly by means of character.

Step 3. the corresponding text specified the n-bit key value as XORed.

Step 4. TACIT logic is applied for nkxorkk in order to perform some specified operations.

Step 5. the obtained resultant value is converted from Step 4 into binary one.

Step 6. reverse operation is applied on the resultant values from Step 5 on the binary string.

Step 7. the corresponding decimal value is to be analyzed.

Step 8. the decimal value according to the unicode character is formulated and that is the cipher text.

Step 9. perform all Steps from 1 to 7 for the remaining characters still the reaching the end of file (EoF).

The value for the first character and the key is generated using 4-H key function using ASCII table. This function is applied for doing the XOR operations. According to the TACIT logic (nk XOR kk), the value obtained is converted into binary forms by means of the preceding steps. In this stage, a modification is implemented in the TACIT logic that is the bit reverse operation which is processed after carrying out the bit XOR operations. As per [15], bit reverse operation is performed which the attacker can easily predict. To avoid this, the process is continuously performed based on the decimal value gained from the previous step. Those results involved the cipher text characters still its enciphered [16]. Visual cryptography technique allows visual information to be encrypted in such a way that the decrypted information appears as a visual image. Visual cryptography allows digital images to be separated into few shares called transparent shares. For security reasons, it ensures that hackers cannot find any clues about the secret image from a single cover image. Transforming a secret message to add some protection using cryptography technique is called as encryption algorithm [6]. The encryption algorithm is unique to the master user who in turn protects the data from attackers. Encryption technique is of two types symmetric and asymmetric encryption. In symmetric encryption, the secret data can be encrypted and decrypted using a single key, without which it is impossible to decrypt the secret data. In asymmetric encryption, the secret data can be encrypted and decrypted using two different keys; it is difficult to decrypt the secret data without those keys. For the decryption process, the first character's decimal value is in ciphered packets. Then, according to the advanced TACIT algorithm logic, it is inversed as shown in Figure 3. For character determination, these processes were reshuffled and this implementation further carried out for all packets still gets deciphered.

4.4. TACIT Decryption Algorithm

Step 1. the cipher text is the encoded text by means of encryption algorithm. The cipher text gives the approximate decimal value of the first character.

Step 2. reverse the corresponding binary values and examined

Step 3. according to the TACIT logic, inverse operation is processed.

Step 4. implementing XOR logical operation to the next key value or n-bit key value

Step 5. represent the corresponding character accordingly.

Step 6. by the help of key value reshuffle

Step 7. Steps from 1 to 6 is repeated still achieving EoF

Table 3: Device utilization summary of encryption and decryption.

Device part	Encryption		Decryption	
Block size	'1024' bit block size	'*N*' bit block size	'1024' bit block size	'*N*' bit block size
Number of slices	82 out of 1408, 6%	108 out of 1408, 8%	89 out of 1408, 6%	105 out of 1408, 8%
Number of slice flip-flops	134 out of 2816, 5%	184 out of 2816, 7%	147 out of 2816, 5%	187 out of 2816, 7%
Number of 4 input LUT's	48 out of 2816, 2%	72 out of 2816, 3%	144 out of 2816, 5%	168 out of 2816, 6%
Number of bonded IOB's	132 out of 140, 94%	132 out of 140, 94%	138 out of 140, 98%	138 out of 140, 98%
Number of GCLKs	1 out of 16, 6%	1 out of 16, 6%	1 out of 16, 6%	1 out of 16, 6%

Table 4: Timing parameters of encryption and decryption.

Device part	Encryption		Decryption	
Block size	'1024' bit block size	'*N*' bit block size	'1024' bit block size	'*N*' bit block size
Minimum period	1.56 ns	2.03 ns	1.442 ns	2.01 ns
Maximum frequency	786 MHz	793 MHz	754 MHz	768 MHz
Minimum input arrival time before clock	2.828 ns	2.915 ns	2.477 ns	2.545 ns
Maximum output required time after clock	5.807 ns	5.914 ns	5.112 ns	5.205 ns
Total memory usage	89943 kB	94248 kB	81175 kB	90298 kB

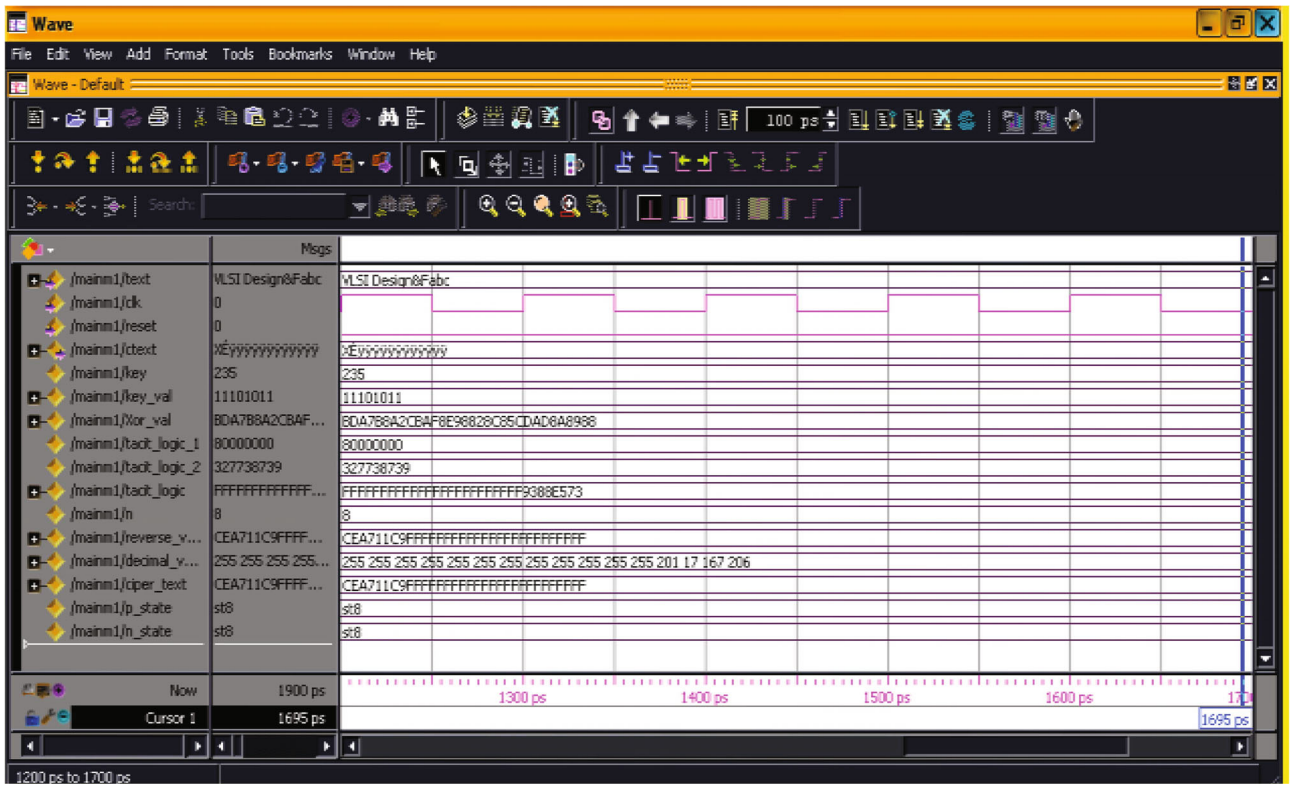

Figure 7: Modelsim simulation for data encryption.

4.5. Implementing Advanced TACIT in NoC Architecture. The developed network-on-chip (NoC) is successful for implementing in conventional bus architecture in an effective manner. The performance of NoC is improved by implementing some set of protocols. These protocols are mainly based on the working of topologies and routing and switching methodologies. This work is carried out by routing techniques [17] which are known to be deadlock free mechanism. The proposed advanced TACIT algorithm-based router architecture of NoC is shown in below Figure 4.

5. Result and Discussion

The proposed work is modeled and developed in VHDL as a finite state machine. As shown in Figures 5 and 6, the

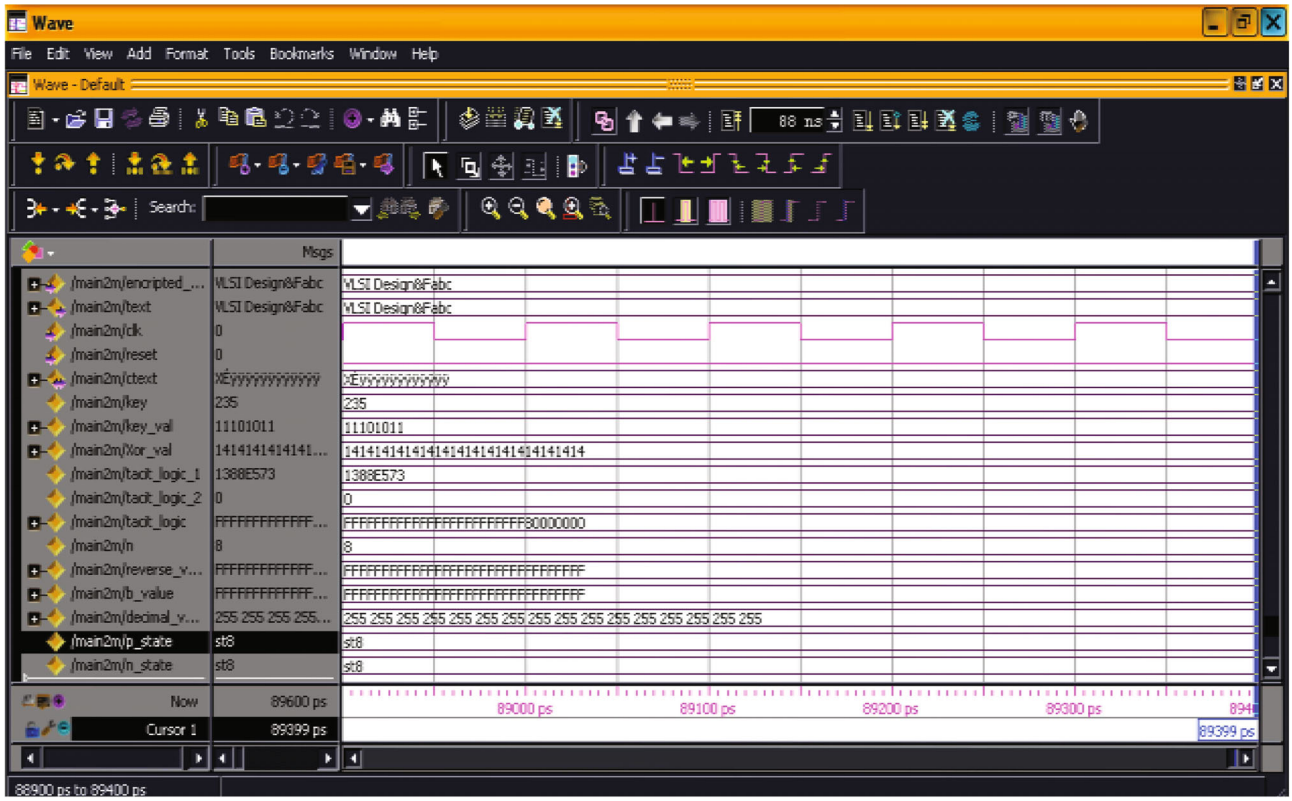

Figure 8: Modelsim simulation for data decryption.

register transfer level (RTL) is a developed view and Table 1 has the description of the chip.

Step input 1: reset = '1', the clk is for managing and run. At 50% duty cycle, every result was checked and rising edge is implied by clock pulse.

Step input 2: reset = '0', Select the input text and same clk is use for management.

Here, the Model_selection has two modes such as to select encryption and decryption mode. By which particular logic is done by enabling input. Table 2 has description of the pins and by means of Mode_selection is intended to perform the chip's functions [18]. There are two at Mode_selection 1 data encryption logic and at 0 decryption logic [8]. Thus, integrated chip differentiates the encryption and decryption logic in the system. In which, by enabling '1,' the encryption logic began, and at 0, the decription logic will be enabled by disabling the encryption logic. We force the mode selection and enable with input_text <*n* bit>.

5.1. Device Utilization and Timing Analysis. The chip implementations and hardware device utilization is analyzed by the device utilization report. The implementation design has the device hardware which is based on no. of flip flops, no. of bounded IOBs, no. of gated clocks (GCLKs), no. of slices, and no. of input LUTs. The important details like minimum period value, minimum input arrival time before clock, information of delay, maximum frequency value, and maximum output required time after clock were resulted at timing details [19]. But the design is still incomplete, and by means total memory utilization value, it will attain complete state. xc5vlx20t-2-ff323: it is the target device created with Virtex-5 FPGA. The simulated values of the design are tabulated in Tables 1, 3, and 4.

The achieved result is compared with existing work, and by means of ref. [5], the future work of chip development of TACIT cryptographic logic is proposed. On proposed work, the chip is designed and developed as per the logic. According to [2], the design is developed and created for 128 bit of block size. In the proposed work, it is designed to carry out for 1024 bit and *N* bits of block size with encryption maximum support frequency at 793 MHz.

The simulation output for data encryption and decryption using Modelsim is as shown in Figures 7 and 8 above. It is clearly evident that the proposed method has achieved its target with maximum security features.

6. Conclusion

In this paper, we proposed an advanced TACIT algorithm-based secured routing architecture for NoC (network-on-chip). In this mechanism, the key generation is based on the hash function (4-H key) scheme which is of four various types. According to this method, the intruder will not be able to break the key easily. This proposed scheme is simulated for the 'n' bit block size and key value. And the results are successfully implied on Virtex-5 FPGA for 1024 bit and 'N' bit of block size. Thus proving the efficiency of the proposed scheme compared to the other traditional approach in the industry. The flawless performance earns the remark for its achievement on being applicable for key size and block size

of 'n' bits. Based on the results the used memory and throughputs were tabulated and future work can be carried out for various NoC architectures.

Data Availability

The data is available upon request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] N. Ashok Kumar, P. Nagarajan, and P. Venkataramana, "Design challenges for 3 dimensional network-on-chip (NoC)," in *International Conference on Sustainable Communication Networks and Application*, vol. 39, pp. 773–782, Springer, 2020.

[2] N. Ashokkumar and A. Kavitha, "A novel 3D NoC scheme for high throughput unicast and multicast routing protocols," *Technical Gazette*, vol. 23, no. 1, pp. 215–219, 2016.

[3] A. Kumara, P. Kuchhal, and S. Singhal, "Secured network on chip (NoC) architecture and routing with modified TACIT cryptographic technique," *Procedia Computer Science*, vol. 48, pp. 158–165, 2015.

[4] A. Ambashanke and P. N. Kumar, "Modified TACIT algorithm based on 4H-key distribution for secure routing in NoC architecture," *IEICE Electronics Express*, vol. 11, no. 13, 2014.

[5] L. Benini and D. Bertozzi, "Network-on-chip architectures and design methods," *IEE Proceedings-Computers and Digital Techniques*, vol. 152, no. 2, pp. 261–272, 2005.

[6] P. P. Pande, C. Grecu, M. Jones, A. Ivanov, and R. Saleh, "Performance evaluation and design trade-offs for network-on-chip interconnect architectures," *IEEE Transactions on Computers*, vol. 54, no. 8, pp. 1025–1040, 2005.

[7] P. Guerrier and A. Greiner, "A generic architecture for on-chip packet-switched interconnections," in *DATE '00: Proceedings of the conference on Design, automation and test in Europe*, pp. 250–256, Paris, France, 2000.

[8] P. Gope, A. Singh, A. Sharma, and N. Pahwa, "An efficient cryptographic approach for secure policy based routing (TACIT encryption technique)," in *2011 3rd International Conference on Electronics Computer Technology*, vol. 5, pp. 359–366, Kanyakumari, India, 2011.

[9] X. Zhang and K. K. Parhi, "High-speed VLSI architectures for the AES algorithm," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 12, no. 9, pp. 957–967, 2004.

[10] B. S. Ferro and P. P. Pande, "Networks-on-chip in a three-dimensional environment: a performance evaluation," *IEEE Transactions on Computers*, vol. 58, no. 1, pp. 32–45, 2008.

[11] Y. U. Ogras and R. Marculescu, "Analytical router modeling for networks-on-chip performance analysis," in *2007 Design, Automation & Test in Europe Conference & Exhibition*, pp. 1096–1101, Nice, France, 2007.

[12] A. Shahabi, N. Honarmand, H. Sohofi, and Z. Navabi, "Degradable mesh-based on-chip networks using programmable routing tables," *IEICE Electronics Express*, vol. 4, no. 10, pp. 332–339, 2007.

[13] S. Saeidi, A. Khademzadeh, and A. Mehran, "SMAP: an intelligent mapping tool for network on chip," in *2007 International Symposium on Signals, Circuits and Systems*, vol. 1, pp. 1–4, Iasi, Romania, 2007.

[14] M. Palesi, R. Holsmark, S. Kumar, and V. Catania, "Application specific routing algorithms for networks on chip," *IEEE Transactions on Parallel and Distributed Systems*, vol. 20, no. 3, pp. 316–330, 2009.

[15] H. Moussa, A. Baghdadi, and M. Jezequel, "Binary de Bruijn interconnection for a flexible LDPC/turbo decoder," in *2008 IEEE International Symposium on Circuits and Systems*, pp. 97–100, Seattle, WA, USA, 2008.

[16] S. A. Alexander, T. Manigandan, M. D. Kumar, and R. V. Vardhan, "A comparison of simulation tools for power electronics," in *Proceedings of International Simulation Conference*, Institute for Applied Physics, Italian National Research Council, 2012.

[17] P. Geno Peter and M. Rajaram, "An enhanced Z-source inverter topology-based permanent magnet brushless DC motor drive speed control," *International Journal of Electronics*, vol. 102, no. 8, pp. 1289–1305, 2015.

[18] Y. S. Jeong and S. E. Lee, "Deadlock-free XY-YX router for on-chip interconnection network," *IEICE Electron Express*, vol. 10, no. 20, pp. 1–5, 2013.

[19] G. Peter, J. Livin, and A. Sherine, "Hybrid optimization algorithm based optimal resource allocation for cooperative cognitive radio network," *Array*, vol. 12, article 100093, 2021.