Volume 9, No. 5, May - 2018 (Special Issue)
International Journal of Mathematical Archive-9(5), 2018, 7-12
Available online through www.ijma.info ISSN 2229 – 5046

VLSI DESIGN OF LOW POWER CRYPTOSYSTEM WITH MODIFIED LOPEZ–DAHAB KEY GENERATION ARCHITECTURE

A. J. BHUVANESHWARI*,
Assistant Professor/Dept of ECE,
Kamaraj College of Engg. & Tech, Virudhunagar, Tamilnadu, India.

M. SAROJINI,**
Assistant Professor/Dept of ECE,
Kamaraj College of Engg. & Tech, Virudhunagar, Tamilnadu, India.

E-mail: erbhuvana.me@gmail.com* and sarojiniece@kamarajengg.edu.in**

ABSTRACT

Sensitive data transfer between different nodes should be kept secret & secure. The communication system which requires sensitive data transfer uses secured cryptographic algorithms to convert the data into an unrecognizable format. With the intention of increasing the speed and to reduce the hardware complexity, this proposed system focuses on the VLSI implementation of light weight security algorithm such as Tiny Encryption Algorithm (TEA) with MLD.VLSI design of TEA is to adapt with many real time constraints such as memory, high throughput and low delay. Modified Lopez Dahab (MLD) Key Generation Architecture is the main additive feature of this proposed system .The proposed system focused on the Modified Lopez–Dahab key generation architecture for low power applications. To achieve the maximum architectural and timing improvements, we reorganize and reorder the critical path of the Lopez–Dahab scalar point multiplication architecture. The proposed system achieved 2Mb/sec of throughput while compared with conventional throughput of 0.8Mb/sec and also the proposed system consumed 11.123ns of delay with efficient power consumption of 52mwatts.

Index Items*- Encryption, Latency, Power, MLD, Security, TEA.*

I. INTRODUCTION

The Secret key establishment is a fundamental requirement for private communication between two parties [1]. At Present, the universal method for generating a secret key is by using public key cryptography. Conversely Asymmetric key cryptography [2] consumes significant amount of computing resources and power which might not be available in certain scenarios (e.g., sensor networks). Quantum cryptography [7] & is a good example of an innovation that use private keys. It utilize the terms of Quantum hypothesis, particularly Heisenberg's uncertainty principle, for exchanging a top secret between different entities. Even though quantum cryptography applications have started to appear recently [12], they are still very rare and pricey. Effectively, the radio channel is a time and space-varying filter, which has the unique filter response for signals sent from Alice to Bob as for signals sent from Bob to Alice. Received signal strength (RSS) is a popular statistic of the radio channel and can be used as the source of secret information shared between a transmitter and receiver [8], [9]. We exercise RSS as a channel gauge, mainly due to the fact that nearly all the current of-the-shelf wireless cards [10], [11], exclusive of any variation, can measure it on a per frame basis. These RSS chronological variations, as calculated by Alice and Bob, might not be considered by an eavesdropper (say Eve) from another location unless she is physically very close to Alice or Bob. Still, due to non ideal state of affairs, including limited capabilities of the wireless hardware, Alice and Bob are incapable to obtain identical proportions of the channel.

II. RELATED WORK

The two familiar techniques from quantum cryptography [6] —information reconciliation and privacy amplification, to undertake the challenge caused by RSS measurement irregularity. Information reconciliation techniques (e.g., Cascade [9]) reveal out negligible information to correct those bits that do not equal at Alice and Bob. Confidentiality amplification [15] reduces the quantity of information the attacker can have about the obtained key. The majority of the

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

earlier research work on RSS-based secret key mining, including that of Azimi-Sadjadi et al. [6], is due to either simulations or hypothetical investigation. Except the recent work by Mathur *et al.* [20] that was achieved in a particular indoor environment, there is only little research on evaluating how effective RSS-based key extraction is in genuine environments under valid settings. We address this important inadequacy in the existing research in this paper with the assist of wide-scale real life measurements in both static and dynamic environments. In order to achieve our measurements and subsequent evaluations, we execute different RSS quantization techniques in conjunction with information reconciliation and privacy amplification. Eve can also compute both the channels between herself and Alice and Bob at the same time when Alice and Bob evaluate the channel between themselves for key mining. We also believe that Eve knows the key extraction algorithm and the values of the parameters used in the algorithm. On the other hand, we assume that Eve cannot be very close (less than a few multiples of the wavelengths of the radio waves being used [14]) to either Alice or Bob while they are extracting their shared key. This will guarantee that Eve measures a different, uncorrelated radio channel [20].

III. PROPOSED SYSTEM

The proposed system implements the above statements using the light-weighted, secure and efficient block cipher TEA in VLSI. It focuses on the block cipher which allows feasibility for the key generation and these generated keys are used for Cryptographic applications with reduced hardware complexity. The programming work for the encryption & decryption techniques and Key generation code are writen using verilog module.

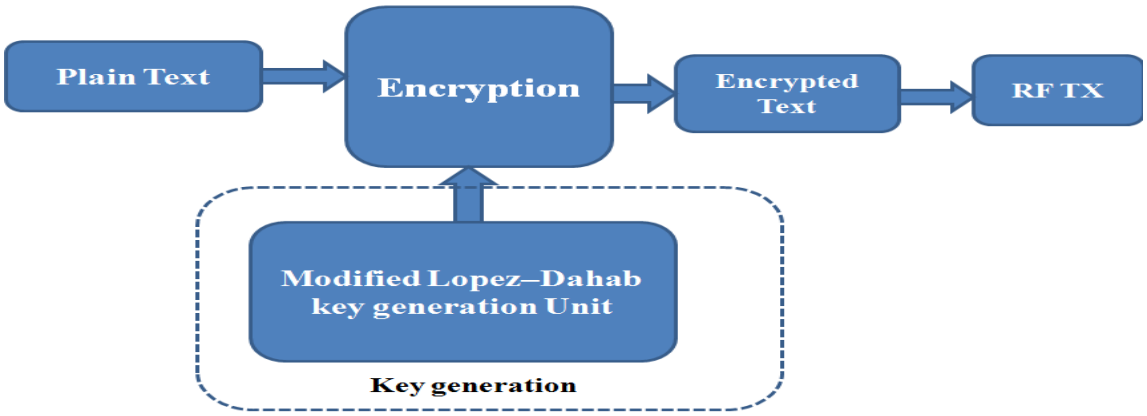

Figure-1: Block Diagram of Proposed System

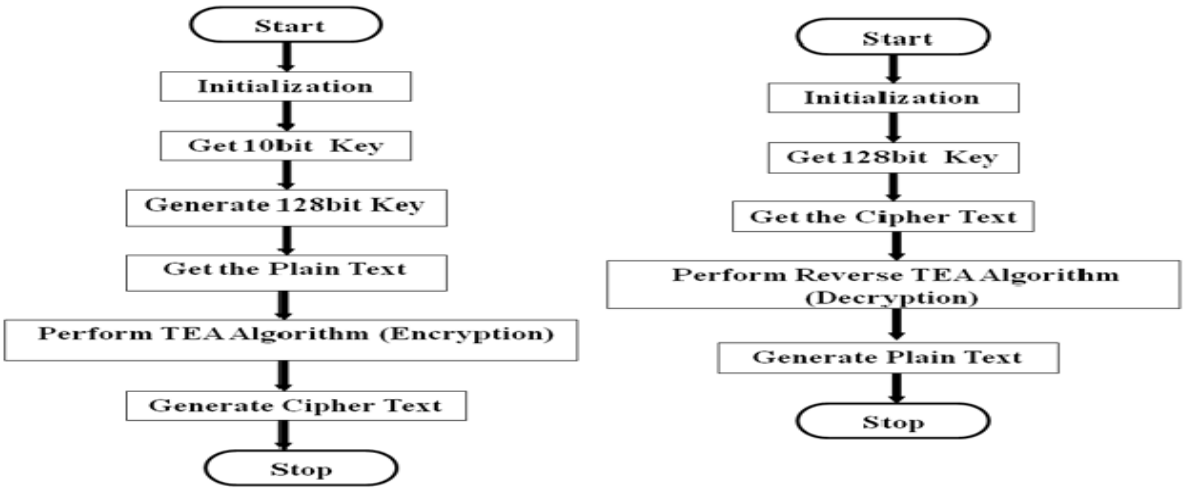

Figure-2&3: Flow Chart for Encryption & Decryption respectively

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

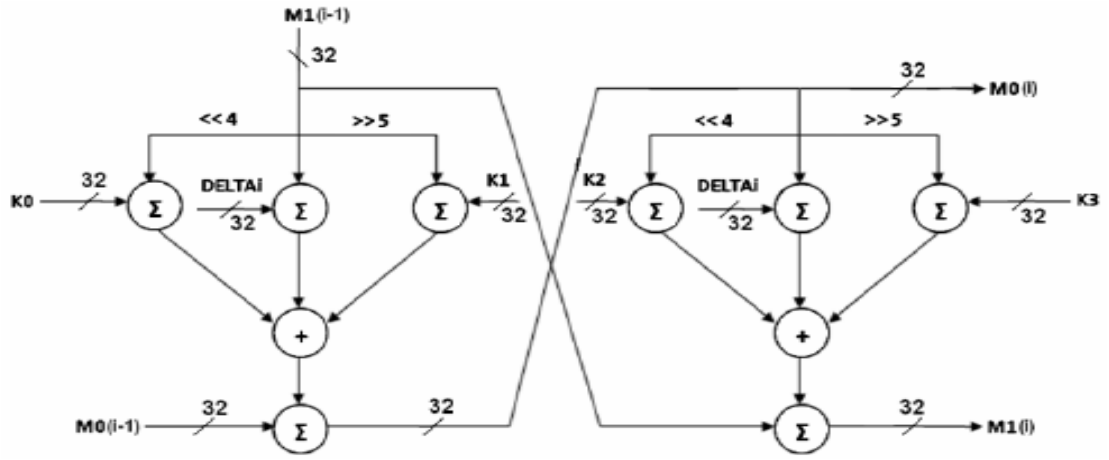

Figure-4: Encryption Architecture

TEA operates on 64 (block size) data bits at a time using a 128-bit key with 32 rounds. TEA is an iteration cipher, where each round i has inputs M0 [i-1] and M1 [i-1], which is derived from the previous round. The sub key K[i] is derived from the 128 bit overall K.

A. Procedure for TEA Encryption& Decryption

Step-1: The one half M1[i-1] of the block cipher is Left shifted by 4 times and Right shifted 5 times.

Step-2: The left shifted block is added with the subkey K0 and right shifted block is added with the subkey K1.

Step-3: It is also added with the constant delta value DELTA[i] which is the multiples of delta, where i represents the number of iterations.

Step-4: The results are then Ex–ORed and added with the other half of the block cipher M0 [i-1] which produces one half of the block cipher M0 for next iteration.

Step-5: Similar operations are performed for the next half round function with the above result.

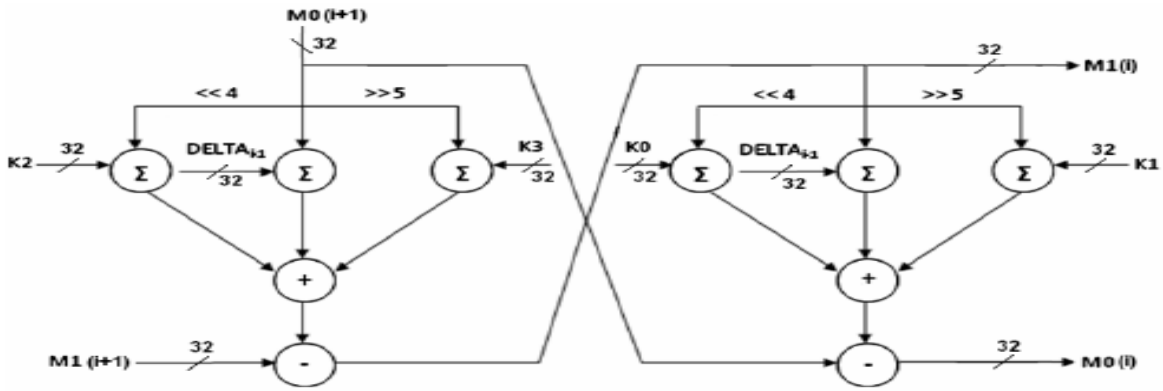

Figure-5: Decryption Architecture

It does Shifting (Left & Right), Summation & Xoring functions. It makes use of the generated 128 bits key by KGU. Subtraction is there instead of addition function at the end. The plain text is retrieved from cipher text by Tiny Decryption algorithm.

B. Features

- Achieve sensitive & secure data transfer.
- Light weight security algorithm: Tiny Encryption Algorithm (TEA) is used in the proposed method.
- Key Generation Unit (KGU) is the special additive feature which is meant for sensitive data transfer in many real-time applications.
- Implementing TEA with VLSI in order to achieve Low Power Consumption.
- Real time constraints such as memory, area, data loss and low cost are properly managed.

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

C. Key Generation Unit

Safe and sound management of the cryptographic keys is vitally important, in view of the fact that the security and reliability of cryptographic processes based on the strength of the keys, the usefulness of the protocols associated with the keys, and the refuge given to the keys. In the secret-key cryptography, two or more entities carve up the same key, which is meant for encryption and decryption of data. The key should be kept secret, and the parties who share a key trust each other not to reveal the key and to defend it against variation. It affords the required key value. Key Generation unit generate the required 128 bit key.

D. MLD Algorithm

Modified Lopez–Dahab key generation architecture for low power applications.MLD algorithm has 2 projective coordinates,where Affine to projective coordinates & Projective to affine coordinates.

Affine variables : x_p ,y_p and b.

Projective variables: X1,X2,Z1 and Z2.

The algorithm consists of three stages:

- ✓ Conversion of P from affine coordinate to projective coordinate;
- ✓ Computation of Q = kP in projective coordinate; and
- ✓ Conversion of Q from projective coordinate back to affine coordinate.
- For the design of the architecture for ECSM, two different parts are considered: the first part involves calculations in the projective coordinate system(X1,X2,Z1 and Z2), and the other part involves the calculations for converting projective coordinates to affine coordinates(x_p, y_p).
- According LD algorithm, in the the first stage, three multiplications X1 Z2, X2 Z1, and T Z_2 (T → X2) are performed in parallel by using three multipliers, and then three other multiplications x p Z1, X1X2T Z_2 (T ← Z1), and bz_2^4 are accomplished in parallel in the second stage,
- Hence, the delay of each iteration is reduced from six field multiplication delays to two field multiplications delays.

IV. STIMULATION RESULTS

The programming work for the encryption & decryption techniques and Key generation code are writen using verilog module i.e. Behavioral or Algorithmic Level Modeling. The execution of code requires the Software - Modelsim 5.8e and Xilinx Project Navigator 9.2i.

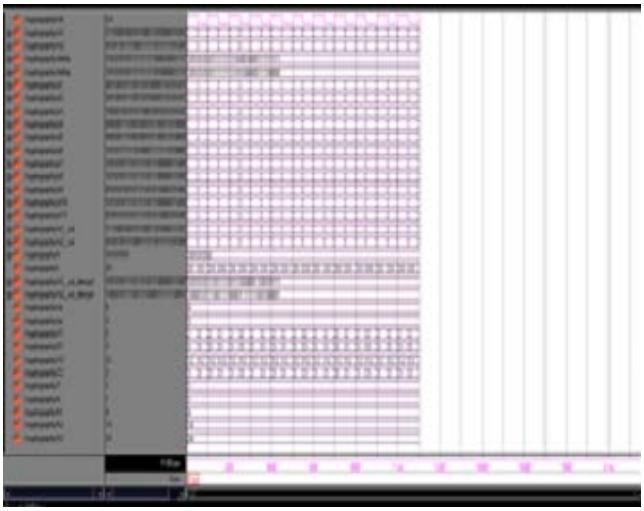

Figure-6: Simulation Screenshot

The *Fig.6* shows the stimulation result of entire algorithm. The *Fig.7* shows the Register transfer level representation of designed IC.The *Fig.8* shows the Hardware Utilization report. The hardware resources used for this proposed system are listed below.

- Number of slices used : 92
- Number of 4 input LUT : 184
- Number of IOB : 139
- Number of bounded IOB : 139 out of 158

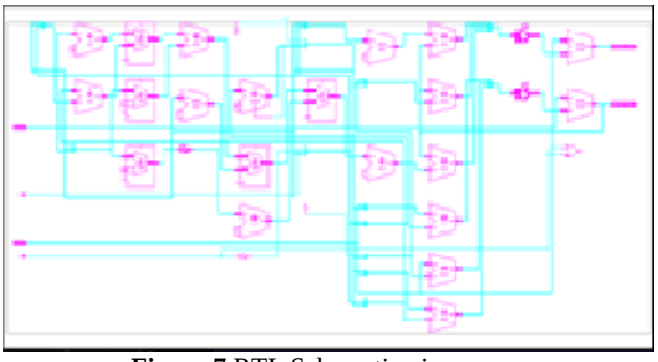

Figure.7 RTL Schematic view

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

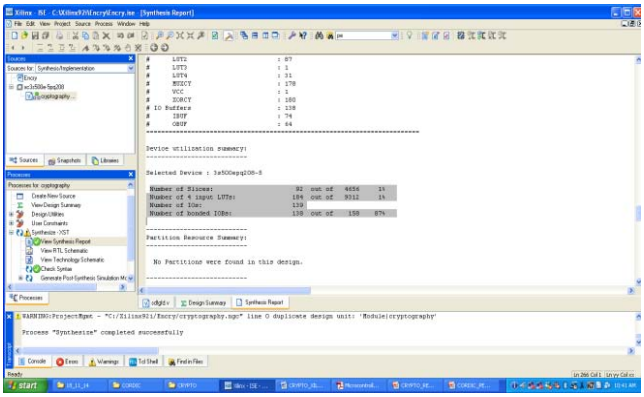

Figure-8: Hardware Utilization report

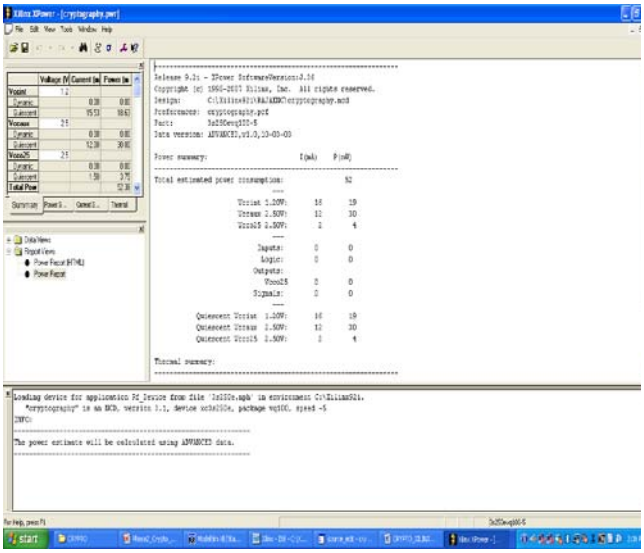

Figure-9: Power Consumption Report

The *Fig.9* shows the overall Power Consumption of the designed Cryptosystem.In order to increase the throughput and to reduce the hardware complexity & power, this proposed system focuses on the light weight security algorithm Tiny Encryption Algorithm TEA which can be implemented in VLSI module**.** The performance of our secure cryptosystem is analyzed and the results are discussed in the following tables 1 & 2.

Table-1: Performance Analysis

Parameters	Estimated Results
Obtained Power	52mWatts
Current	30mA
Latency	11.123ns

Table-2: Performance Comparison

Parameters	Conventional	Proposed
Throughput	0.8Mb/s	2Mb/s
Execution Time	115.248ms	11.123ns
Power	3W	52mW

V. CONCLUSION

Thus the design of the low power consumption architecture for cryptographic processor is achieved. The proposed system focused on the Modified Lopez–Dahab key generation architecture for low power applications. In order to increase the throughput and to reduce the hardware complexity & power, this focuses on the light weight security algorithm Tiny Encryption Algorithm this can be implemented in VLSI module. The Cryptosystem achieves a higher throughput rate of 2Mbits/sec than that of other related works. Moreover, it resulted with Power consumption of 52mW, Current consumption of 30mA & Delay of 11.123ns. Therefore, the proposed Cryptosystem is very suitable for the area efficient cryptographic processor for speed-critical cryptographic applications.

REFERENCES

1. "NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," http:// csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501. pdf, 2001.
2. "ipwraw," http://homepages.tu-darmstadt.de/~p_larbig/wlan, 2012.
3. "Radio tap," http://www.radiotap.org, 2012.
4. "Converting Signal Strength Percentage to dBm Values," http:// www.wildpackets.com/elements/whitepapers/Converting_Signal_Strength.pdf, 2012.
5. T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless Secret Key Generation Exploiting Reactance-Domain Scalar Response of Multipath Fading Channels," IEEE Trans. Antennas and Propagation, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.
6. B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks," Proc. 14th ACM Conf. Computer and Comm. Security (CCS), 2007.
7. C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," J. Cryptology, vol. 5, no. 1, pp. 3-28, 1992.

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

8. M. Bloch, J. Barros, M.R.D. Rodrigues, and S.W. McLaughlin, "Wireless Information-Theoretic Security," IEEE Trans. Information Theory, vol. 54, no. 6, pp. 2515-2534, June 2008.
9. G. Brassard and L. Salvail, "Secret Key Reconciliation by Public Discussion," Proc. Workshop Theory and Application of Cryptographic Techniques on Advances in Cryptology, pp. 410-423, 1994.
10. V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. ACM MobiCom, 2008.
11. G.D. Durgin, Space-Time Wireless Channels. Prentice Hall PTR, 2002.
12. L. Greenemeier, "Election Fix? Switzerland Tests Quantum Cryptography," Scientific Am., Oct. 2007.
13. A.A. Hassan, W.E. Stark, J.E. Hershey, and S. Chennakeshu, "Cryptographic Key Agreement for Mobile Radio," Elsevier Digital Signal Processing, vol. 6, pp. 207-212, 1996.
14. J.E. Hershey, A.A. Hassan, and R. Yarlagadda, "Unconventional Cryptographic Keying Variable Management," IEEE Trans. Comm., vol. 43, no. 1, pp. 3-6, Jan. 1995.
15. R. Impagliazzo, L.A. Levin, and M. Luby, "Pseudo-Random Generation from One-Way Functions," Proc. 21st Ann. ACM Symp. Theory of Computing (STOC), pp. 12-24, 1989.
16. S. Jana and S.K. Kasera, "On Fast and Accurate Detection of Unauthorized Access Points Using Clock Skews," Proc. ACM MobiCom, 2008.
17. S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari, and S.V. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," Proc. ACM MobiCom, 2009.
18. Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing Wireless Systems via Lower Layer Enforcements," Proc. Fifth ACM Workshop Wireless Security (WiSe), 2006.
19. M.G. Madiseh, M.L. McGuire, S.W. Neville, and A.A.B. Shirazi, "Secret Key Extraction in Ultra Wideband Channels for Unsynchronized Radios," Proc. Sixth Ann. Comm. Networks Services Research Conf. (CNSR), May 2008.
20. S. Mathur, W. Trappe, N.B. Mandayam, C. Ye, and A. Reznik, "Radio-Telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," Proc. ACM MobiCom, 2008.

Source of support: Proceedings of National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics (RAPAM - 2018)", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.

CONFERENCE PAPER
National Conference March 1st - 2018, On "Recent Advances in Pure and Applied Mathematics", Organized by Department of Mathematics, Arul Anandar College (Autonomous), Madurai. Tamilnadu, India.