LOW POWER CRYPTOSYSTEM WITH KEY GENERATION UNIT

A.J.Bhuvaneshwari[1], S.Bhuvana[2], G.Ganga[3]

[1,2] PG Scholar, Raja College of Engineering and Technology, Madurai, Tamilnadu,(India)

[3]PG Scholar, Aanad Institute of Higher Technology, Chennai, Tamilnadu, (India)

ABSTRACT

The security based applications need sensitive data transfer between different nodes or destinations. In order to increase 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) which can be designed and implemented in VLSI to adapt with many real time constraints such as memory, high throughput and low delay. The additive feature of this proposed system is that it uses Key Generation Unit (KGU) to produce the random key to make it optimal for sensitive data transfer in many real-time applications. The proposed system achieved 1.5Mb/sec of throughput while compared with conventional throughput of 0.8758Mbits/sec and also the proposed system consumed 14.918ns of delay.

Keywords: Cryptosystem, Key Generation Unit , Tiny Encryption Algorithm.

I.INTRODUCTION

Secret key establishment is a fundamental requirement for private communication between two entities. Currently, the most common method for establishing a secret key is by using public key cryptography. However, public key cryptography consumes significant amount of computing resources and power which might not be available in certain scenarios (e.g., sensor networks). More importantly, concerns about the security of public keys in the future have spawned research on methods that do not use public keys. Quantum cryptography [7], [26] is a good example of an innovation that does not use public keys. It uses the laws of Quantum theory, specifically Heisenberg's uncertainty principle, for sharing a secret between two end points. Although quantum cryptography applications have started to appear recently [12], they are still very rare and expensive. Aless expensive and more flexible solution to the problem of sharing secret keys between wireless nodes (say Alice and Bob) is to extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them [6], [20], [18], [5], [24]. Essentially, the radio channel is a time and space-varying filter, that at any point in time has the identical 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. We use RSS as a channel statistic, primarily because of the fact that most of the current of-the-shelf wireless cards, without any modification, can measure it on a per frame basis. The variation over time of the RSS, which is caused by motion and multipath fading, can be quantized and used for generating secret keys. The mean RSS value, a somewhat predictable function of distance, must be filtered out of the measured RSS signal to ensure that an attacker cannot use the knowledge of the distance between key establishing entities to guess some portions of the key. These RSS temporal variations, as measured by Alice and Bob, cannot be measured by an eavesdropper (say Eve) from another location unless she is physically very close to Alice or Bob. However, due to nonideal conditions, including limited capabilities of the wireless hardware, Alice and Bob are unable to obtain identical measurements of the channel. This asymmetry in measurements brings up the challenge of how to make Alice and Bob agree upon the same bits without giving out too much information on the channel that can be used by Eve to recreate secret bits between Alice and Bob.

II.LITERATURE SURVEY

Azimi-Sadjadi et al. [6] suggested using two well-known techniques from quantum cryptography—information reconciliation and privacy amplification, to tackle the challenge caused by RSS measurement asymmetry. Information reconciliation techniques (e.g., Cascade [9]) leak out minimal information to correct those bits that do not match at Alice and Bob. Privacy amplification [15] reduces the amount of information the attacker can have about the derived key. This is achieved by letting both Alice and Bob use universal hash functions, chosen at random from a publicly known set of such functions, to transform the reconciled bit stream into a nearly perfect random bit stream. Most of the previous research work on RSS-based secret key extraction, including that of Azimi-Sadjadi et al. [6], is based on either simulations or theoretical analysis. Other than the recent work by Mathur et al. [20] that was performed in a specific indoor environment, there is very little research on evaluating how effective RSS-based key extraction is in real environments under real settings. We address this important limitation of the existing research in this paper with the help of wide-scale real life measurements in both static and dynamic environments. In order to perform our measurements and subsequent evaluations, we implement different RSS quantization techniques in conjunction with information reconciliation and privacy amplification. Eve can also measure both the channels between herself and Alice and Bob at the same time when Alice and Bob measure the channel between themselves for key extraction. We also assume that Eve knows the key extraction algorithm and the values of the parameters used in the algorithm. However, we assume that Eve cannot be very close (less than a few multiples of the wavelength of the radio waves being used [20]) to either Alice or Bob while they are extracting their shared key. This will ensure that Eve measures a different, uncorrelated radio channel [11].

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.

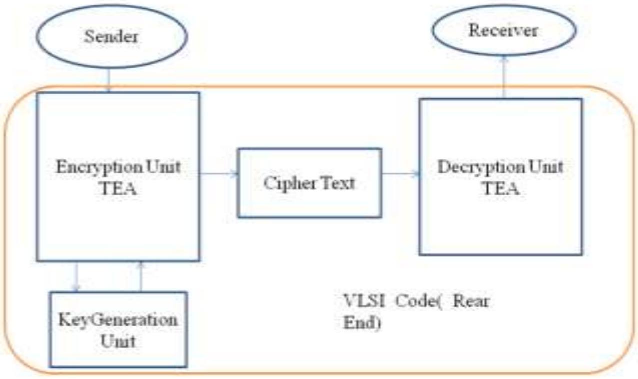

Fig.1: Block Diagram of Proposed System

3.1 TEA Algorithm

TEA is the Tiny Encryption Algorithm which 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.

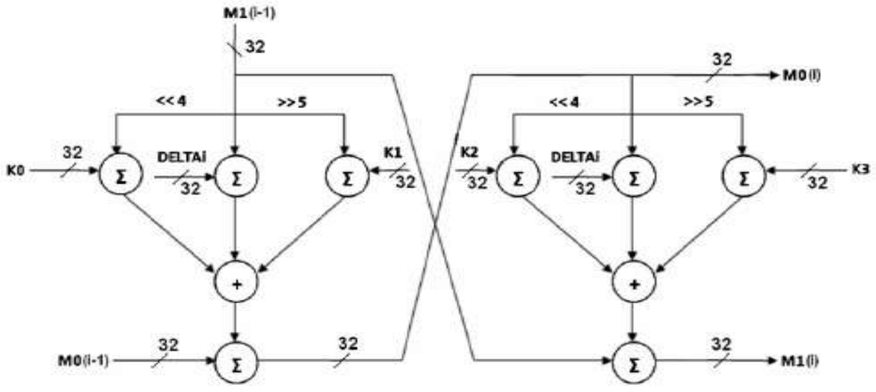

Fig.2: Encryption Architecture

3.1.1 Procedure for TEA Encryption

Step1:The one half M1[i-1] of the block cipher is Left shifted by 4 times and Right shifted 5 times.

Step2.:The left shifted block is added with the subkey K0 and right shifted block is added with the subkey K1.

Step3: It is also added with the constant delta value DELTA[i] which is the multiples of delta, where i represents the number of iterations.

Step4: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.

Step5: Similar operations are performed for the next half round function with the above result.

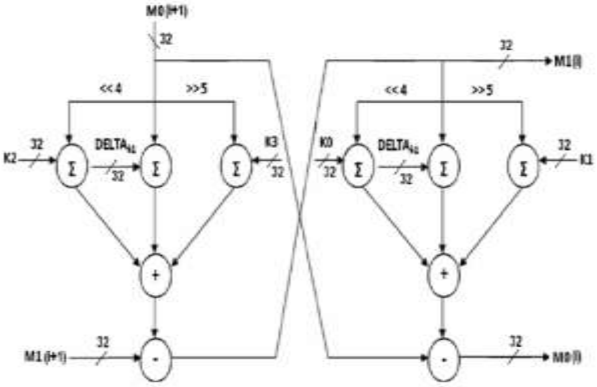

Fig.3: Decryption Architecture

Since, the TEA has a Feistel structure the reverse operation of encryption process is performed to obtain the plain text in the decryption process.

3.2 Key Generation Unit

In secret-key cryptography, two or more parties share the same key, which is used to encrypt and decrypt data. The key must be kept secret, and the parties who share a key rely upon each other not to disclose the key and to protect it against modification.It Provides the required key value.Key Generation unit generate the required 128 bit key.Single KGU generate 16bit key.Total 8KGU needed to generate four 32bit key values.Shifting, swapping & rearranging are the main functional transformations.In the Tiny decryption algorithm, there are 32 rounds of iterations. It get the 128bit key value from the Key generation unit. In each iteration, the delta value “9E3779B9” is subtracted with the constant delta value.

IV.SIMULATION RESULTS

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**.** By running the TEA Algorithm in ModelSim & Xilinx ,valuable results are obtained.

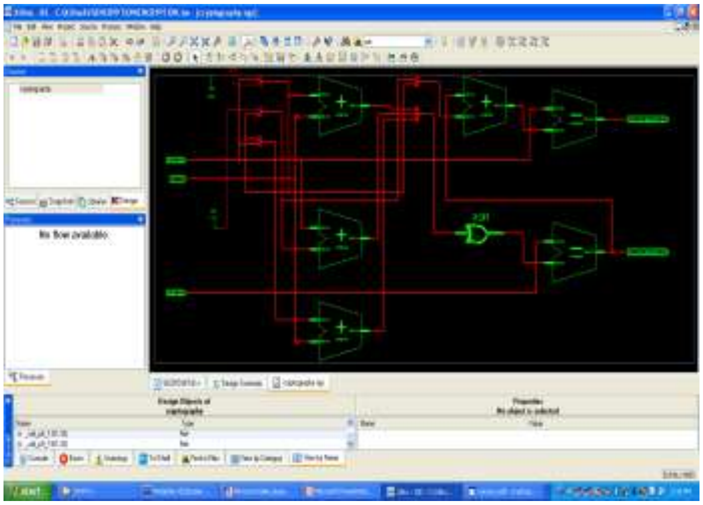

Fig.4: RTL Schematic view

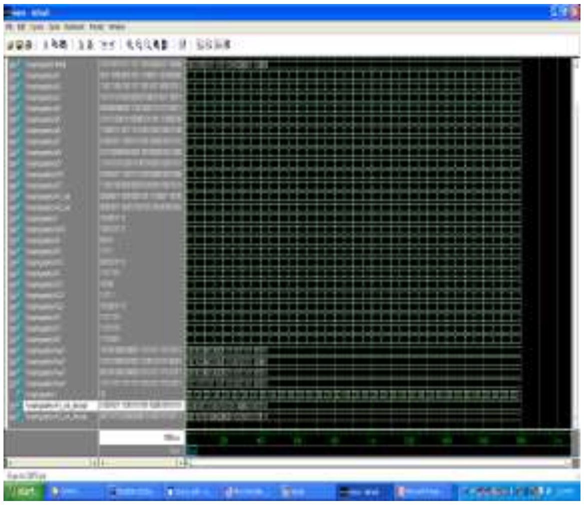

Fig.5: Simulation waveform

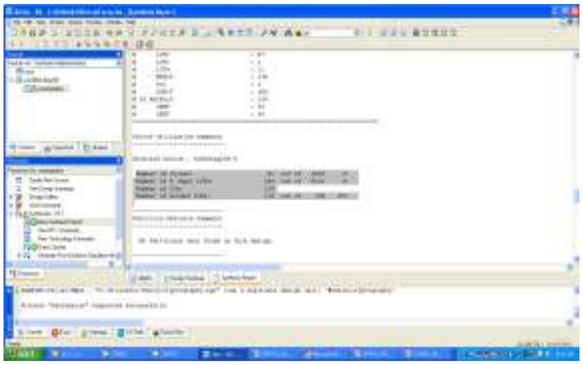

Fig.6: Harware Utilization report

Fig.7: Power Consumption Report

Performance Analysis

Parameters	Estimated Results
Power Consumption	81mW
Current Consumption	46mA
Delay	14.918ns

V.CONCLUSION & FUTURE WORK

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 which can be implemented in VLSI module. The system employs with a light-weight block cipher and offers low power and area consumption. The additional feature of this system is the usage of KGU to generate the 128bit key which still improves the security of data transfer with low power consumption & this can be needed for sensitive & secure data transfer**.** Systems design techniques can lower the computational complexity, effectively reduce the decomposing latency and Low Power Consumption is achieved. The proposed Cryptosystem achieves a higher throughput rate of 1.5Mbits/sec than that of other related works. Moreover, it resulted with Power consumption of 81mW, Current consumption of 46mA & Delay of 14.918ns. Therefore, the proposed Cryptosystem is very suitable for the area efficient cryptographic processor for speed-critical cryptographic applications.

ADVANTAGES

- Achieve sensitive & secure data transfer.
- 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.
- Significant application in RFID tags, Smart cards, Wireless sensor nodes.

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] “Radiotap,” 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-DomainScalar 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.

[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 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.

[21] U.M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," IEEE Trans. Information Theory, vol. 39, no. 3, pp. 733-742, May 1993.

[22] U.M. Maurer and S. Wolf, "Unconditionally Secure Key Agreement and the Intrinsic Conditional Information," IEEE Trans. Information Theory, vol. 45, no. 2, pp. 499-514, Mar. 1999.

[23]A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys through Multipath," Proc. IEEE Int'l Conf. Acoustics, Speech Signal Processing (ICASSP), pp. 3013-3016, Apr. 2008.

[24] M.A. Tope and J.C. McEachen, "Unconditionally Secure Communications over Fading Channels," Proc. IEEE Military Comm. Conf. (MILCOM), 2001.

[25] J.W. Wallace, C. Chen, and M.A. Jensen, "Key Generation Exploiting MIMO Channel Evolution: Algorithms and Theoretical Limits," Proc. Third European Conf. Antennas Propagation (EuCAP), Mar. 2009.