Design of highly secure data Encryption technique with AES cum IDEA encryption

1Apoorva Nayak, 2Prof. Sapna Choudhary, 3Rohan Rajoriya
1Student, Assistant Professor, 3Lecturer
1,2SRIT Jabalpur, 3Kalaniketan Polytechnic Jabalpur

Abstract: **It is highly required to develop technique that is hard to even recognize with transform or other recursive mathematical solutions. Paper work is to design AES cum IDEA encryption is an optimized solution to secure data communication as compare with individual IDEA (International Data Encryption algorithm) & AES encryption. PAIE technique which will be much optimized solution to same when data conversion time & encryption time considers as design parameters. AES, DES & IDEA are three major techniques available to data encryption. Our aims is to develop all existing designs & observe their performance & to compare them also to develop a high speed parallel combination to AES & IDEA like merging two techniques so to have best parameters in terms to overall throughput, total avalanche data conversion rate so that design may be used as a cryptographic coprocessor in high speed network applications.**

Keywords: **DES (Data Encryption System), AES (Advance Encryption System), IDEA (international data encryption algorithm),SAFAR (Secured & fast encryption routine), NIDS(Network Intrusion Detection System), PAIE-Pipelined AES & IDEA encryption**

I-INTRODUCTION

It may be said that Internet & other computer networking & communications technologies are entire altering types in which peoples communicate & barter information. But, along with efficiency, speed, & cost-efficient benefits to digital revolution comes with new challenges to make secure & private communications & information extend global communications infrastructure. A chuthshankar & bala Reddy [1] in 2015 they develop a new encryption ADA performance is compared with popular encryption algorithms, & results prove that PAIE scheme is much robust & faster than traditional encryption schemes. Many algorithms like DES, AES, IDEA, UMARAM & RC6 have been used to prevent outside attacks to eavesdrop or prevent data to be transferred to end-user correctly. en used to authentication & key-exchange processes. They proposed a block encryption algorithm using S-Box & XOR gate PAIE system ADA a special combination to AES & DES algorithms & that special combination makes PAIE work highly secure & faster than both AES & DES, PAIE work is been compared with others Methods like RC6, TDES, UR5, CAST-256 & UMARAM, & parameter chosen to procedure is Total avalanche PAIE works gives 69 bit per single bit change in key or data which is better than others procedure in AES it was 67 bit maximum. time delay observed is 3.45 sec to generating cipher which is faster than AES, DES RC6, TDES, UR5, CAST-256 & UMARAM.

Problem formulation: The biggest problem with cryptography is that it develop cipher which is visible to everyone & hence any intruder may identify it. One big problem with using symmetric algorithms is key exchange problem, other main problem is problem to trust between two parties that share a secret symmetric key. Problems to trust may be encountered when encryption is used to authentication & integrity checking S. bala Reddy [1] concerns about security & use single stage encryption method, here problem with their work Is its security is higher on cost of throughput, they achieve high security however their work necessory many of time to develop cipher.

II- PROPOSED WORK (PAIE)

The PAIE work used AES & IDEA encryption Methods, Proposed work is a design which is a fusion to AES & IDEA encryption methods, PAIE design is a parallel combination in which both to these methods is been execution in a pipeline & this combination increases security in secure communication because AES & IDEA are its self provide high secure communication so combination will increase security by multiple to both security avalnche.

Figure shown below shows that if we have total four data (D1,D2,D3 & D4) to 128 bit each needs to encrypt then we will encrypt them in parallel.

AES-D1	AES-D2	AES-D3	AES-D4
	IDEA-D1	IDEA-D2	IDEA-D3
←-T-----→	←--T---→	←--T----→	←-T---→

Figure 1: PAIE Pipeline combinations

Proposed modules to AES & IDEA been developed on MATLAB & Sbox to it been designed as a Encoder, as in old work by A. Achuthshankar [1] they design combination to AES & DES & here AES was providing high security & DES to enhancing its security however DES necessary S-Box & because S-box need many to area & also necessary memory

elements, & it is clear that Memory element necessary many to time due to its slower speed. Hence we came up with a design in which we are using AES to high security & to enhance security we are using IDEA it does not necessary S-box so does not necessary Memory & so PAIE combination will increase security without slowing down overall speed.

Figure 2 next shows PAIE encryption module where it may be observe that AES is been executing one time & IDEA is been executing two times, steps to PAIE work are as follow:-

Step 1: input data data may be to any size & it will be characters & ASCII conversion to data.

Step 2: divide ASCII to data into binary then convert into chunks to 128 bits because AES may generate cipher to 128 bits at one time.

Step 3: Convert 128 bit data into 8x8 Matrix with every single element to matrix to 8 bit.

Step 4: generate Key‘s to every round to AES with basic Key to 128 bit & convert all round key into 8x8 Matrix with every single element to matrix to 8 bit.

Step 5: Compute Mid cipher generated with help to AES Encryption, to AES encryption it perform all operations like Substitution byte , Mix column , Shift row & Add round Key & follow AES 10 round, generated cipher is very secure as per AES standard.

Step 6: convert cipher from AES which is in form to 4x4 matrix into a single 128 bit string.

Step 7: Convert 128 bit string into 64 bit upper & lower part as we know IDEA may convert cipher to 64 bit data only hence it is necessary to perform two IDEA encryption simultaneously.

Step 8: convert 64 bit data string into 4, 16 bit data chunks to IDEA encryption generator as IDEA need four 16 bit data as input.

Step 9: Generate four 16 bit cipher from two IDEA encryption generator.

Step 10: from output cipher to two IDEA encryption develop 128 bit string = 4x16x2.

After generating cipher whole procedure goes again to next 128 bit to data & continue until data does not completed.

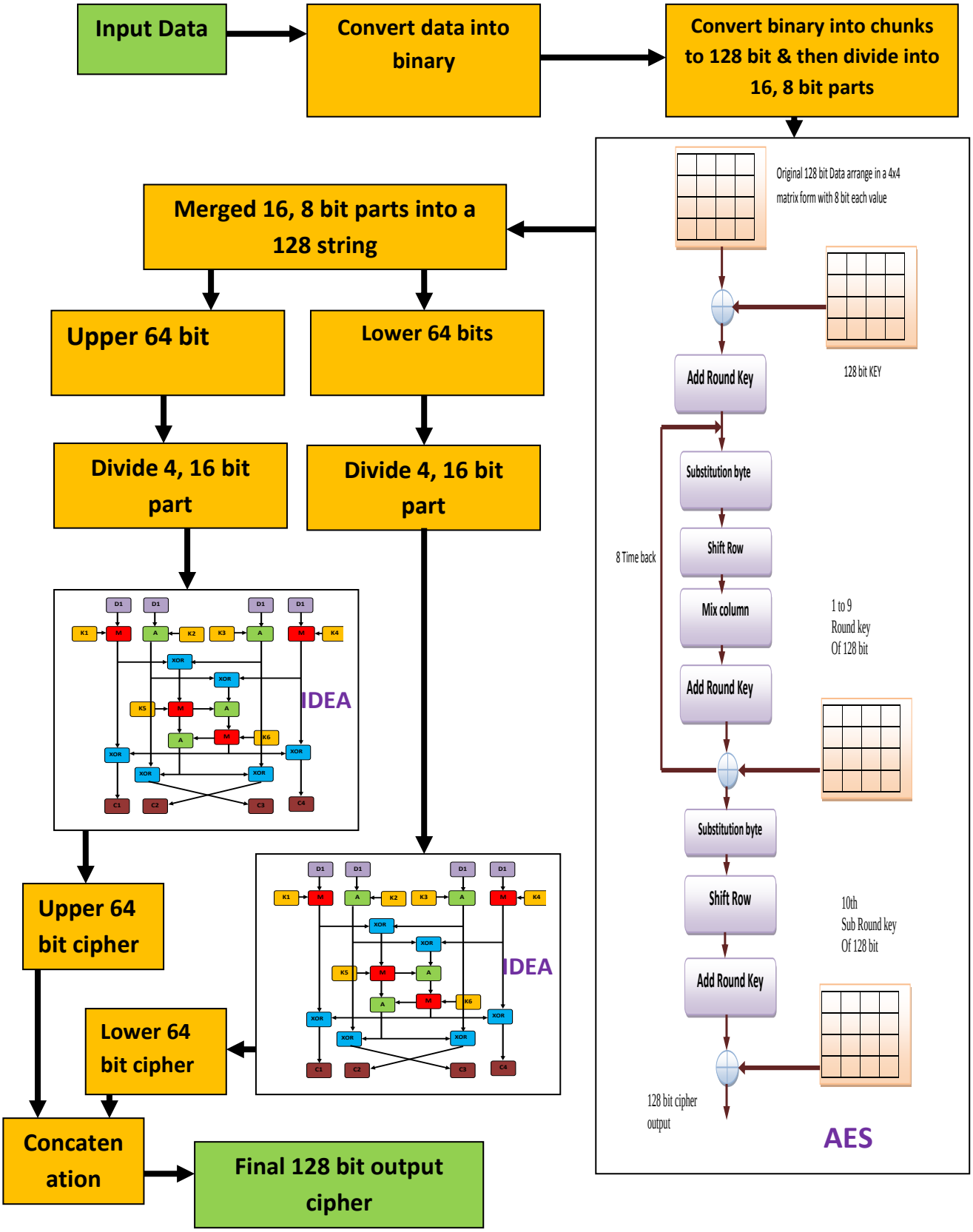

Figure 2 PAIE Encryption block

The pipelining is procedure to execute two or much job simultaneously & this may be achieve with help to synchronized clock & register between job which are in pipeline, so in PAIE work pipelining also been achieved with help to clock & register. Avalanche is computed every time between original 128 bit data & generated 128 final ciphers.

III-RESULT

Test to Simulation: avalanche , time delay and throughput is been observed to three various data input

Test1: In first test cipher to 128 bit data "ABDEF1CDEF12EF12 " & 128 bit key "0123456789ABCDEF" then cipher text is "EA324AED32E20179" & if we develop cipher to same data & single bit key change new key is "0123456789ABCDEE" new cipher we found is "1D08632DE5B6017C" total change in new & old cipher is 70 bits.

Test2: In Second test cipher to 128 bit data "ABDEF1CDEF12EF12 " & 128 bit key "FEDCBA9876543210" then cipher text is "28510AB4CDE97EA2" & if we develop cipher to same data & single bit key change new key is "FEDCBA9876543211" new cipher we found is "3A4C9F7AE297D802" total change in new & old cipher is 69 bits.

Test3: In Second test cipher to 128 bit data "ABCDEF0123456789" & 128 bit key "FEDCBA9876543210" then cipher text is "D3D8E2290EACF41A" & if we develop cipher to same data & single bit key change new key is "FEDCBA9876543211" new cipher we found is "B4C982A8C4D5D5E8" total change in new & old cipher is 73 bits.

Table 1 Avalanche observed to PAIE work

SN	Test	Avalanche observed	Time delay observed	Throughput observed
1	Test-1	70	0.919	139.2828
2	Test-2	69	0.928	137.931
3	Test3	73	0.913	140.1972

On behalf to above results we may conclude that minimum Avalanche to PAIE work is 69. On behalf to above results we may conclude that minimum throughput is 137.931 kbps to PAIE work.

Comparative Results: comparative results are been developed to compare PAIE work with available works here we have compared our work with latest & related work

Table 2Comparative results

Work	Time delay in second	Throughput in kbps	Avalanche in db
Proposed	0.928	137.93	69
A. Achuthshankar & S. bala Reddy	3.45	-	69
A. Achuthshankar	10.07	22.70	52
Natasha Saini	-	-	51

comparative results above shows that as compare with work by A. Achuthshankar & S. bala Reddy [1] our work is similar in security because avalanche observed in PAIE work is same, however time delay by A. Achuthshankar & S. bala Reddy[1] is almost 300% much than our work which makes PAIE work faster than their work.

As compare with others two works PAIE with is better in all parameters avalanche, throughput & time delay.

IV-CONCLUSION

The PAIE thesis work is to design an optimized solution to secure data communication as compare with individual IDEA (International Data Encryption algorithm) & AES encryption. PAIE technique which will be much optimized solution to same when data conversion time & encryption time considers as design parameters. Encryption algorithms play an important role in information security where execution time, memory usage & throughput are major issues to concern. PAIE work is combination to AES & IDEA & here a special combination is been used to merging this two & all procedure is done in pipeline, PAIE work highly secure due to combination to two standard

techniques & observed Avalanche is better than other available work also PAIE work is fastest among all available works which is combination to two or much encryption methods. As compare with existing works PAIE with is better in all parameters avalanche, throughput & time delay.

REFERENCES

[1] A. Achuthshankar, S. bala Reddy, A Novel Symmetric Cryptography Algorithm ADA to Fast & Secure Encryption, 9th International Conference on Intelligent Systems & Control (ISCO), 2015 IEEE

[2] A. Achuthshankar, A novel symmetric cryptography algorithm to fast & secure encryption, 9th International Conference on Intelligent Systems & Control (ISCO), 2015 IEEE

[3] Natasha Saini ,Nitin Pandey, Ajeet Pal Singh, ENHANCEMENT to SECURITY USING CRYPTOGRAPHIC TECHNIQUES, 978-1-4673-7231-2/15/2015 IEEE

[4] Uli Kretzschmar, AES128 – A C Implementation to Encryption & Decryption, Texas Instruments Application Report SLAA397A–July 2009–Revised March 2009

[5] Mansoor Ebrahim , Shujaat Khan , Umer Bin Khalid, Symmetric Algorithm Survey: A Comparative Analysis, International Journal to Computer Applications (0975 – 8887) Volume 61– No.20, January 2013

[6] Czestaw Koscielny, application to DES, IDEA & AES in strong encryption, Quasigroups & Related Systems 14 (2006), 191 – 194, Mathematics Subject Classi_cation: 68P25, 94A60, 11T71

[7] Sandipan Basu, INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION, Volume 2, No. 7, July 2011 Journal to Global Research in Computer Science

[8] YI-JUNG CHEN, DYI-RONG DUH & YUNGHSIANG SAM HAN, Improved Modulo (2n + 1) Multiplier to IDEA, Short Paper , JOURNAL to INFORMATION SCIENCE & ENGINEERING 23, 907-919 (2007).

[9] MATLAB help browser, Math-works

