International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

EFFICIENT VLSI ARCHITECTURE FOR 4G CRYPTO PROCESSOR USING MILENAGE AND ZUC ALGORITHM

Dr. R.Latha[1] ,Dr. C.Thiripura sundari[2], V.Agalya[3,] D.Sandhiya[4] , P.Sankari[5]
[1]. Professor, [2].Associate professor. [3-5].Final year students
Department of ECE, KSK College of Engineering and Technology, Kumbakonam India
rlatha@gmail.com, .c_thiripurasundari@yahoo.co.in, agalyaeceksk@gmail.com,
santhiyaeceksk@gmail.com

Abstract

The whole security architecture of LTE (long term evolution) consists of two main cryptographic algorithms: MILENAGE algorithm and ZUC algorithm. This paper shows a security architecture crypto processors for 4G LTE consists of two ciphers algorithm enables each one on demand which is based on novel design principles .The crypto processor reduce the covered area and increase the speed better than the other crypto processors.
Keywords - 4G LTE security, block cipher and stream cipher , mobile communication system, network level security, symmetric key cryptosystem.

Introduction

The recent expansion of new wireless network technologies has led many of their supported protocols to become realized into the new demanding 4 g wireless era. One of the such recently deployed standards is the course LTE/SAE. One of the key aspects of these next generation wireless communication network will be their speed, operability as well as security [3]. Security plays a vital role in this world. hence ,it is important to make wireless network , like LTE , secure by protecting data and resources from malicious acts , thus crypto algorithms should be the core of their security mechanisms it is easy to implement crypto algorithms in software ,but such algorithms are proven to slow for real time application .for this reason , it becomes necessary to implement crypto algorithm as hardware module or crypto processors [2],[4],[5]. In modern mobile embedded system along with high security demand constraints such as power consumption and chip covered area are very strict while the performance requirements are crucial. almost all today's hardware implemented cipher have a major drawback the slowness of the operation due to mathematical and logical transformation therefore several architecture design novelties are being proposed in bibliography to ensure mode performance with less resource consumption the experts deals with weakness of security service found on UMTS system as well as to introduce new improvements [6] [7] [11] the modern technology such as network demand on private and secure communication for number of everyday transaction approaches on silicon high throughput [10] the 128 bit data path is in AES is more suitable for LTE terminal [7] .the area optimization is observed by using multi codes in VLSI implementation [2] the key used in this crypto processor is symmetry key algorithm[8]

4G LTE SECURITY TECHNOLOGY

Recently the LTE protocol has been prototyped with (3gpp) , together with its future development , the system architecture evolution (SAE), as for LTE to become evolved into 4g standard security plays a key role for effective and reliable implementation although the 3g security architecture does not really

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

require standardisation of crypto analytic algorithm needs for authentication and key agreement for protocol The first set of algorithm is MILENAGE one form of AES algorithm[1]. 3G Technology security features that have proven to be both robust and secure the improvement of any weakness found on 3G security, the resulting algorithm is based on stream core algorithm named ZUC inside the vital improvement cipher algorithm still need to be included to confront some keys issues like AKA(authentication and key agreement) during this transactions the cipher keys are needed to be transported securely protection of data plane originated by those entities needs crypto algorithm [3]. The pseudorandom generator is used for key generation [9].

STRUCTURAL CONSIDEARATION FOR THE PROPOSED ARCHITECTURE

I. S-BOX OPTIMIZATION

It includes large amount of area consumption inside the chip , nevertheless in most published academic architectures S BOX are being manufactured using static blocks of SRAM or RO M by lookup tables or by Boolean gates. The hexadecimal value is included inside 0x64, memory cell address, AES S-BOX should be treated as normal S-BOX we simply selected as index address (x=6,x=4)in his they are treated as their common S-BOX, since we simply select as index address for two registers files y=0x06 ,y=0x04 ,or simply the AES S-BOX refer table1

II.OVERALL ARCHITECTURE

The authentication and key agreement unit function as the operating unit for MILENAGE main core algorithm, Two data buses of 32 bit and 64bit address bus are used for internal data transfer purpose the storage for algorithm key to be stored and loaded in RAM blocks finally in order to communicate efficiently with the external environment as I/O interface has been added (refer figure1) as it is illustrated in next figure (refer figure2),the universal security architecture encryption unit (USAEU) in corporate S-BOX optimizations. By using the MUX the MILENAGE and ZUC algorithm can be selected from the crypto processor.

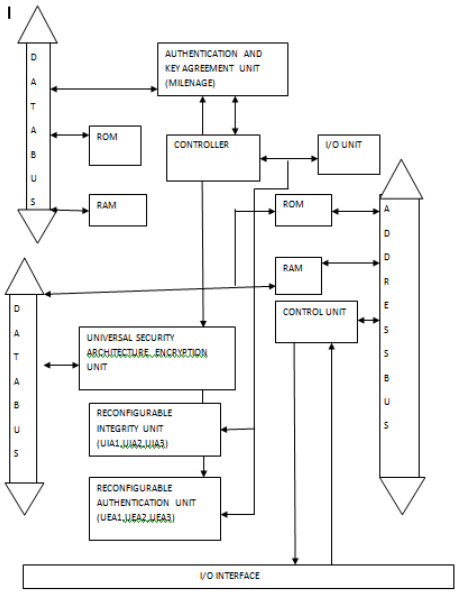

Fig1. OVERALL ARCHITECTURE OF THE CRYPTO PROCESSOR

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

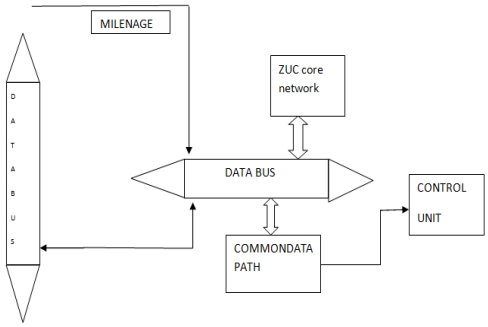

FIG 2: UNIVERSAL SECURITY ARCHITECTURE

III MILENAGE ALGORITHM

For the MILENAGE case ,five concurrent 128bit rotation of five new variable instead of mapping them in fixed S-BOX (refer table 1) value like in the ROM case, we could easily exploit the modified previous circuit into extending it to a 32bit shifted output so to be 4 time deployed for 128 bit value rotations the plain text is converted into cipher text by dividing them into blocks .The block size and key size is 128 bits and rounds takes place in MILENAGE 10rounds the key are processed in terms of words the sub key generated is 44 in very brief speculations we could notice that the previous ROM average access time or read latency in terms of authentication and key generation MILENAGE was specified into function . one strong design benefit from the decision was their ability to offered to UMTS operators to personalized utilization of function instead of own algorithm one example algorithm for instant that could be used in well-known AES [1] E[x]k define the result of applying block cipher encryption algorithm like AES to the input value x using key k the 128 bit value OP is operator variant algorithm configuration field with the task force asked to include in order to provide separation between functionality of algorithm as mentioned a before the selection of kernel cipher for MILNAGE algorithm was flexible Rijindael was choose has being one of the file AES was well studied and could easily implemented in wireless system offering 128bit security (refer figure3).The key generation includes 11 partial rounds the expansion key from 0 to 43 bits 3words in the position of multiples of 4 calculated by the applying rot word and sub bytes transformation to previous words finally XOR with RCON table

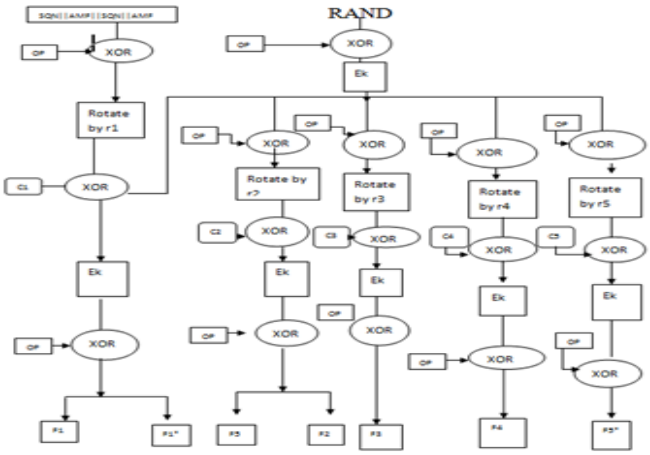

FIG3: MILENAGE ALGORITHM

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

IV ZUC ALGORITHM

ZUC stream cipher that can be encrypt and decrypt 1bit message at a time it mainly consists of linear feedback shift register, bit reorganisation and nonlinear functions LFSR as four 32bit words the bit reorganisation extracts from state of LFSR, nonlinear functions the mixing operation are the XOR takes Place l1 and l2 are both consists of linear transformations according to ZUC specifications [5] LFSR has two modes of operation initialization mode and working mode

Middle layer of ZUC bit reorganisation it founds 32bit words in accordance with algorithm the first three words are passed to next bottom layer therefore, BR procedure should mix with nonlinear function F operation together to save the clock cycles there are two 32 bit memory cells R1 ,R2 in the nonlinear function F procedure . the input of F is X0,X1,X2 , which are the first three words of output of BR procedure, and its output 32 bit words W .(refer figure 4)

$\oplus$ L1(X)$\oplus$1(X) ($\oplus$<<<10) (X<<<18) (X<<<24),

$\oplus$ L2(X)$\oplus$L2(X) ($\oplus$<<<14) (X<<<22) (X<<<30).

The key loading proc3dure will expand the initial key and initial vector in to 16 (31bit) integers has the initial state of LFSR. let the 128 but initial key and the 128 bit initial vector IV K=K0||K1||K2||.....||K15 and IV =IV0||IV1||IV2||....||IV15 separately where ki and ivi are bytes . The ki and ivi are loaded into the cells si as SI=KI||DI||IVI. Where DI is known as constant. Several researches from 2011 till now tried to enhance and the security in ZUC algorithm this section present the contribution has been done to improve the efficiency of ZUC cryptography algorithm. Some by optimising the structure of ZUC and some by modifying the algorithm itself from about the throughput with less consuming area

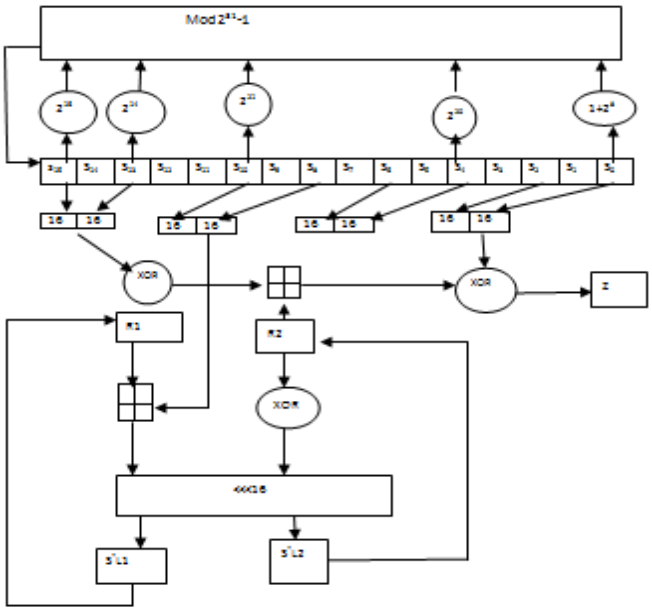

FIG 4:ZUC ALGORITHM

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

IV.RESULTS OF HARDWARE IMPLEMENTATION

The proposed system architecture (see figure 1) was captured by using vhdl with structural description logic the code was synchronised, placed, and routed by using FPGA device of Xilinx. The proposed system implementation is compared with each one of the most efficient ciphering function in individual implementation found in the research in bibliography in the different hardware device (FPGAs) the synthesis result for this implementation are also shown in the table2. Concerning the MILENAGE cipher mechanism benchmark results are depicted in table (refer table 2). Due to the more flexibility in selecting the desire kernel cipher function as well as the better achieved data path the ZUC outer performed in terms of sped and bandwidth percentage. the frequency is increased by 156MHZ Whereas the utilise the hardware area space lowered at above 214 slices the MILENAGE algorithm performs the speed and frequency increased from 109MHZ and area are lowered by the 438CLBS due to the lowest power consumption of all investigated solution, the universal common S-BOX design the concept combined with a 128 bit common data path in AES architecture proves to be benefit for ciphering LTE terminals

X1 / Xo	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

T ABLE 1:S-BOX

IMPLEMENTATION	COVERED AREA	FREQUENCY
MILENAGE	1154 CLBS	109 MHZ
PROPOSED MILENAGE	438 CLBS	92.199MHZ
ZUC	840 SLICES	49MHZ
PROPOSED ZUC	214 SLICES	156.178 MHZ

TABLE 2: DEVICE UTILIZATION TABLE

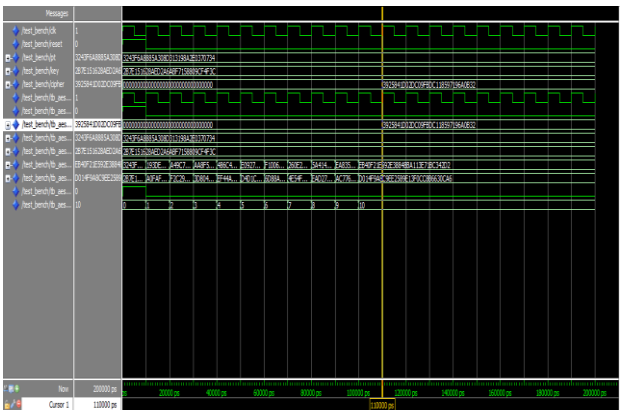

FIGURE 4: MILENAGE SIMULATION OUTPUT

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

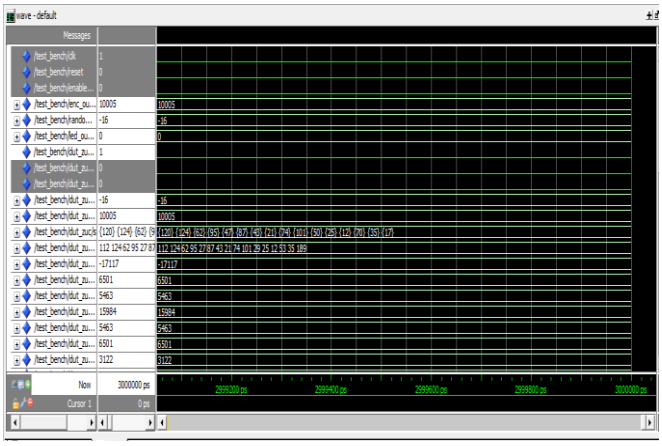

FIGURE5: ZUC SIMULATION OUTPUT

V.CONCLUSION AND FUTURE ENHANCEMENT

Network operators an chip manufactures have great marketing outlook toward the usage of 4G network in the upcoming decades the vast increase of mobile subscribes creates challenges in terms confidentiality and integrity of both data and signalling transmission an efficient and compact full rolling architecture crypto processor described in this document to convert the total asset of 4G LTE security panel, along with the result of this implementation in FPGA technology. The design techniques and novel reconsideration imposed in building the security processor have proved to be a very useful. Not only does this proposal achieve a higher performance and throughput area /delay improvement but is one of the advanced most novel design in terms of unifying the S-BOX of 4G Crypto processor in to only one in addition it manages to emulate the operation complicated processors the left shift bit stream into a ready circuit , the future enhancement is the algorithm set can be modified and can be implemented any other hardware oriented algorithm such as KASUMI AND SNOW 3G etc…. they can also provide a secured services with the system. The simulated output of MILENAGE is shown in fig 4 and the simulated output of ZUC algorithm is shown in fig5.

REFERENCES

[1] Specification and evaluation of THE MILENAGE Algorithm set, ETSI/SAGE Specification ,Version :1.0 Date:22nd November 2000
[2] G.Selimis, N.Sklavos, O.Koufopavlou, “area optimized architecture and VLSI Implementation of Multicoder Processor for the WTLS “ proceeding of 46th IEEE Midwest symposium on circuits &systems (IEEE MIDWEST’03),PP.24-27,December 27-30,Cairo,Egypt ,2003.
[3] Bikos Anastasios N.Sklavos Nicloas, “LTE/SAE Security Issues on 4G Wireless Networks,”Security &privacy ,IEEE,Vol.11,no2,pp55,62, March-April 2013
[4] P.Kitsos,N.Sklavos and O.Koufopavlou.2007.UMTS Security: System Architecture and hardware implementation : research articles wireless commun.mob.comput.7,4 (May 2007), 483-494.
[5] Paris Kitsos, N.Sklavos, George Provelengios, Athanassios N.Skodras.2013.FPGA – based perfomance analysis of stream cipher ZUC,snow3g, grain VI ,mickey V2, trivium and E0 Microprocess,Microsyst. 37,2 (March 2013), 235-245.

International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN : 2456-172X | Vol. 3, No. 4, Dec. - Feb, 2019
Pages 36-42 | Cosmos Impact Factor (Germany): 5.195
Received: 16.02.2019 Published : 28.02.2019

[6] Sourav Sen Gupta ,Anupam Chattopadhyay, Ayesha khalid "Designing integrated accelerator for stream cipher with structural similarities ", Journal on Cryptography ad Communication ,2013, vol.5,no.1,pp.19-47.
[7] Ho Won Kim ; Sunggu Lee ,"Design and implementation of private and public key crypto processor and its application to a security system," Consumer Electronics .IEEE Transaction on, vol 50,no .1 pp 214 ,224,frb 2004.
[8] A.Bikos, N.Sklavos, A.Furnaris, "on the optimization of S-BOX functionality in 4G LTE security ciphers", joint MEDIAN-TRUDEVICE Workshop ,co-located with international symposium on defect and fault toleranc in VLSI and Nanotechnology Systems (DFT"14), amstredam the netherlandS ,2-3 OCTOBER 2014.
[9] Taylor and Francis , "On the hardware implemented cost of crypto processors architectures ", Information security Journal: A global perspective; 19.53-60,2010.
[10] Ricardo Chaves , Shivam Basin, "Challenges in designing trustworthy cryptographic co-processors", Tru device cost action ref . IC(204) The ARTEMIS joint undertaking under grant agreement no.621429,and UID/CEC/50021/2013