ASIC design of High Speed Kasumi Block Cipher

Dilip kumar[1]
[1]M. Tech scholar,
Gyan ganga institute of technology and science Jabalpur
M.P.

Sunil shah[2]
Asst. Prof.
Gyan ganga institute of technology and science Jabalpur
M.P.

***Abstract* - The nature of the information that flows throughout modern cellular communications networks has evolved noticeably since the early years of the first generation systems, when only voice sessions were possible. With today's networks it is possible to transmit both voice and data, including e-mail, pictures and video. The importance of the security issues is higher in current cellular networks than in previous systems because users are provided with the mechanisms to accomplish very crucial operations like banking transactions and sharing of confidential business information, which require high levels of protection. Weaknesses in security architectures allow successful eavesdropping, message tampering and masquerading attacks to occur, with disastrous consequences for end users, companies and other organizations. The KASUMI block cipher lies at the core of both the f8 data confidentiality algorithm and the f9 data integrity algorithm for Universal Mobile Telecommunications System networks. The design goal is to increase the data conversion rate i.e. the throughput to a substantial value so that the design can be used as a cryptographic coprocessor in high speed network applications.**

Keywords— Xilinx ISE, Language used: Verilog HDL, Platform Used: family- Vertex4, Device-XC4VLX80

I. INTRODUCTION

Symmetric key cryptographic algorithms have a single key for both encryption and decryption. These are the most widely used schemes. They are preferred for their high speed and simplicity. However they can be used only when the two communicating parties have agreed on the secret key. This could be a hurdle when used in practical cases as it is not always easy for users to exchange keys. KASUMI is a block cipher used in UMTS, GSM, and GPRS mobile communications systems. In UMTS, KASUMI is used in the confidentiality (*f8*) and integrity algorithms (*f9*) with names UEA1 and UIA1, respectively. In GSM, KASUMI is used in the A5/3 key stream generator and in GPRS in the GEA3 key stream generator. KASUMI was designed for 3GPP to be used in UMTS security system by the Security Algorithms Group of Experts (SAGE), a part of the European standards body ETSI.[2] Because of schedule pressures in 3GPP standardization, instead of developing a new cipher, SAGE agreed with 3GPP technical specification group (TSG) for system aspects of 3G security (SA3) to base the development on an existing algorithm that had already undergone some evaluation.[2] They chose the cipher algorithm MISTY1 developed and patented by Mitsubishi Electric Corporation. The original algorithm was slightly modified for easier hardware implementation and to meet other requirements set for 3G mobile communications security.

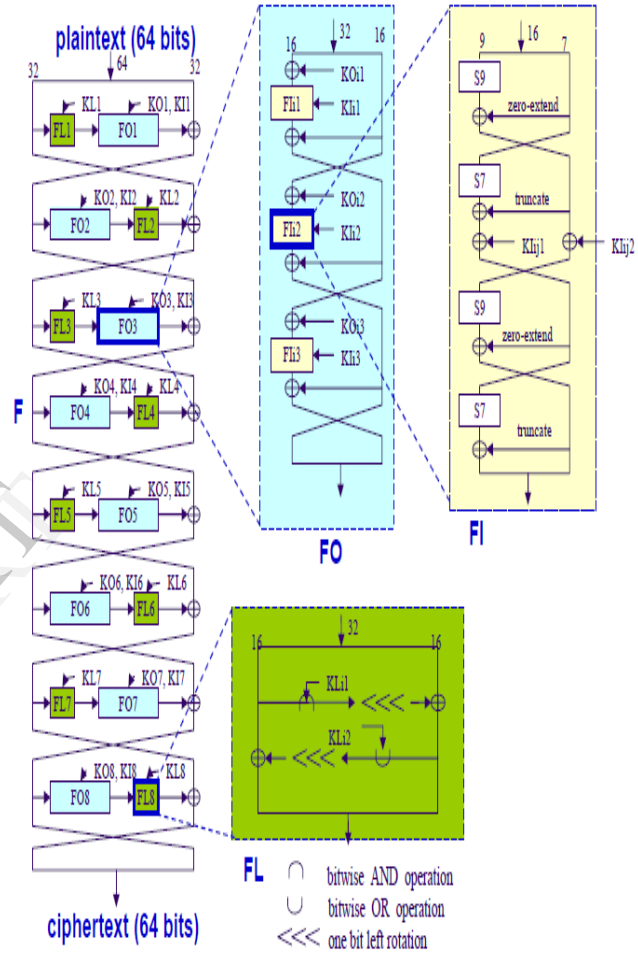

Figure 1 overall KASUMI cipher

II. KEY SCHEDULE

The key, K, is 128 bits long.
Each round of Kasumi uses 128 bit sub-key derived from K. Before generating the round keys, two 16-bit arrays, Kj, Kj' are derived as follows, K is split into eight 16 bit values. K1-K8. Thus, K = K1 || K2 || K3 ||…|| K8.
Kj' = Kj ⊕ Cj ,

for each j = 1 to 8 and Cj is a constant value as defined below.

C1=0x0123, C2=0x4567, C3=0x89AB, C4=0xCDEF, C5=0xFEDC, C6=0xBA98, C7= 0x7654, C8=0x3210

	Round 1	Round 2	Round 3	Round 4	Round 5	Round 6	Round 7	Round 8
$KLi_{,1}$	K1<<<1	K2<<<1	K3<<<1	K4<<<1	K5<<<1	K6<<<1	K7<<<1	K8<<<1
$KL_{i,2}$	K3′	K4′	K5′	K6′	K7′	K8′	K1′	K2′
$KO_{i,1}$	K2<<<5	K3<<<5	K4<<<5	K5<<<5	K6<<<5	K7<<<5	K8<<<5	K1<<<5
$KO_{i,2}$	K6<<<8	K7<<<8	K8<<<8	K1<<<8	K2<<<8	K3<<<8	K4<<<8	K5<<<8
$KO_{i,3}$	K7<<<13	K8<<<13	K1<<<13	K2<<<13	K3<<<13	K4<<<13	K5<<<13	K6<<<13
$KI_{i,1}$	K5′	K6′	K7′	K8′	K1′	K2′	K3′	K4′
$KI_{i,2}$	K4′	K5′	K6′	K7′	K8′	K1′	K2′	K3′
$KI_{i,3}$	K8′	K1′	K2′	K3′	K4′	K5′	K6′	K7′

Note: <<<n => Left Circular Rotation of the operand by n bits.

Table 1: KASUMI Key Generation

III. DESIGN METHODOLOGY

KASUMI encryption design have five design modules FI, FO, FL, Key-Generator and S-Box. FI, FO and FL have logical XOR and shifting operation and there is no way for further optimization.

Optimization in Area and speed possible only with Key-Generator and S-Box only. paper works on new optimized S-box though Key-Generator technique remains unchanged. Table 2 shows the relation between input and output for s7 box (f7).Observation from table 2 was that as for small size S-box (2-5 bit), memory based S-box is better area optimized and for bigger S box(more than 5 bit)

Input	output
000 0000	= 010 0000
000 0001	= 011 0000
000 0010	= 000 0000
000 0011	= 111 0000
000 1111	= 000 1011
001 0000	= 010 0000
001 0001	
001 1111	= 000 1011
010 0000	= 010 0000
010 1111	= 000 1011
111 1111	= 100 1100

Table 2: input/output relation S7 KASUMI

combinational architecture is better area optimized. Proposed work is a combination of memory and combinational architecture. The table show is relation between input and output for 7 bit S-box, here thesis proposed architecture divided the total range 0-127 into 8 sub-ranges (0-15,16-31,32-47,48-63,64-79,80-97,96-111,112-127) isolation shown by orange lines.For each sub-range, lower four LSB of output (separated by pink line) are generated using 4 input K-map and upper three MSB of output are generated using Memory architecture.Figure 2 shows the architecture of proposed work which reflects the idea behind the new logic for the architecture as explain above.

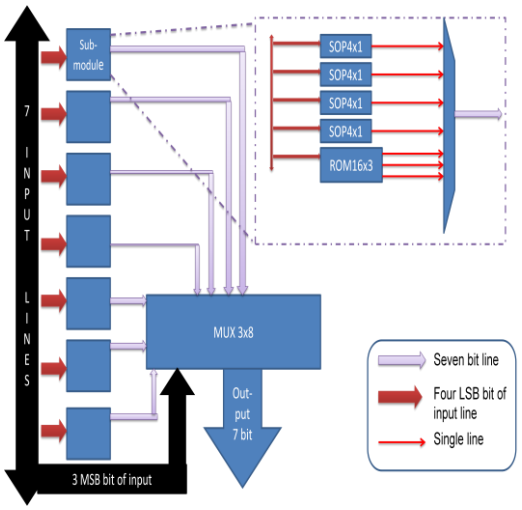

Figure 2: Proposed architecture S7 box

IV. TOOL PLATFORM AND LANGUAGE USED

Tool: Xilinx ISE : It is a software tool produced by Xilinx for synthesis and analysis of HDL designs. **Language used: Verilog HDL:** Verilog, standardized as IEEE 1364, is a hardware description language (HDL) used to model electronic systems. It is most commonly used in the design and verification of digital circuits at the register-transfer level of abstraction

Platform Used: family- Vertex4, **Device-**XC4VLX80, **Package-**FF1148. Target FPGA is a Vertex FGPA because the same platform is been used by base papers.

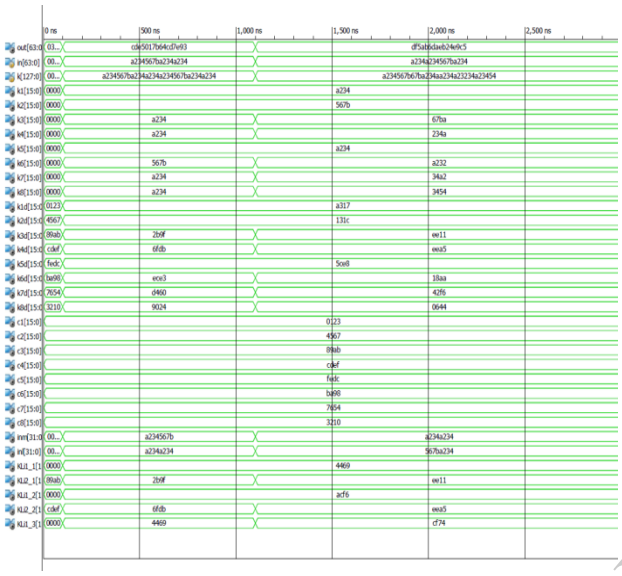

Figure 3: simulation and RTL schematic of proposed work

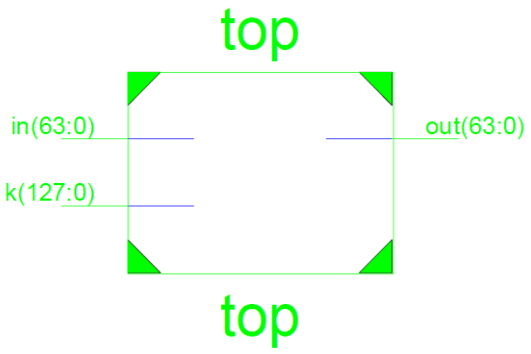

Figure 3: simulation and RTL schematic of proposed work

VI. RESULTS

From the simulation as shown in above slides

Key :

A234567ba234a234a234567ba234a234

Result:-1

Output: Cde5017b64cd7e93

Input: A234567ba234a234

Output^Input: 6fd15700c6f9dca7

Avalanche: **41 bit change/64 bit**

Result:-2

Output: Df5ab6daed24e9c5

Input: A234a234567ba234

Output^Input: 7d6e14eebb5f4bf1

Avalanche: **45 bit change/64 bit**

Parameters	Design of FI	Design of FO	Design of FL	Design of Sbox-7	Design of Sbox-9	Complete KASUMI module
No. of slice	429	1379	18	26	157	8401
No. of LUT's	782	2541	32	52	289	15468
No. of IOB's Logical Time delay	13.04 ns	11.216 ns	4.303 ns	6.067 ns	7.279 ns	33.64 ns

Table 3: Results for each module

Comparative Results

	Parameters	Base [1]		Base[2]		Proposed work	
S-box design		S-box 7 (S7)	S-box 9 (S9)	S-box 7 (S7)	S-box 9 (S9)	S-box 7 (S7)	S-box 9 (S9)
	No. of slice	34	169	-	-	26	157
	Logical Time delay (ns)	-	-	-	-	6.067	7.279
Overall Kasumi encryption design	No. of slice	8784		8770		8401	
	Logical Time delay (ns)	34.01		-		33.64	

The work is implemented of FPGA which makes proposed work a semicustom design as known semicustom design always lack behinds compare to full-custom design in term of Area, speed and power. In future proposed work can be implemented at transistor level (i.e. Full-custom)

Table 4 : comparative results

VI CONCLUSION

The huge number of potential subscribers and the advanced services to provide impose great challenges in terms of guaranteeing confidentiality and integrity of both data and signalling. An efficient and compact hardware design of the KASUMI algorithm was described in this thesis work, along with the results of its implementation in FPGA technology. these proposed S-box techniques might be utilized to design high performance compact implementations of Feistel-like block ciphers. Not only does this proposal achieve a good performance, but is one of the most economical designs in terms of area.

REFERENCES

[1]. Sima I., Tarmurean D., Greu V, Diaconu A.'XXTEA, an alternative replacement of KASUMI cipher algorithm in A5/3 GSM and f8, f9 UMTS data security functions' 9th International Conference on Communications (COMM), volume 1, pp 328-333

[2]. Ren fung, ying-jian, Fu Xiao-bing, 'A Small and Efficient Implementation of KASUMI', IEEE Explore, WASE International Conference on Information Engineering, volume 2, pp 377-380, 10-11 july, 2011

[3]. Hui Shi Yuanqing Deng Yu Guan Peng Jia Fengli Ma, Analysis of the Avalanche Property of the KASUMI Algorithm, Automatic Control and Artificial Intelligence (ACAI 2012), International Conference on, IEEE Explore, 3-5 March 2012

[4]. P. Kitsos, M. D. Galanis, and O. Koufopavlou,"High-speed hardware implementations of the kasumi block cipher" ISCAS 2004, ©2004 IEEE.

[5]. Tomas balderas-contreras, rene cumplido , claudia feregrino-uribe, "On the design and implementation of a RISC processor extension for the KASUMI encryption algorithm", T. Balderas-contreras et al. / Computers and electrical engineering 34 (2008) 531–546