ISSN 2320-9984

Volume 2 Issue 3 | September 2014

ISSN: 2320-9984 (Online)

International Journal of Modern Engineering & Management Research

Website: www.ijmemr.org

XXTEA an Optimized Encryption Design with High Feedback Substitution Box Architecture

Satish Kumar Vishwakarma
Research Scholar
Vindhya Institute of Technology & Science,
Jabalpur (M.P.) [INDIA]
Email: staishvits@yahoo.co.in

Prof. Shivam Khare
Head of the Department
Vindhya Institute of Technology & Science,
Jabalpur (M.P.) [INDIA]

Abstract—*With today's networks it is possible to transmit both voice and data, including e-mail, pictures and video. The XXTEA block encrypted documents founds at the core of both the f8 documents confidentiality algorithm and the f9 documents integrity algorithm for Universal Mobile Tele documents exchanges System networks. The design goal is to increase the rate of conversion of documents means the throughput to a substantial value so that the module can be used as a cryptographic coprocessor in very high speed (3G or 4G) network applications. basically XXTEA is an standard and one cannot modify its dataflow and operation of each module like FI, FO, FL and Sbox but one can produce same results with different approach, as FI, FO and FL used only XOR operation or shifting or addition which is been already optimised by many researcher, only Sbox can be optimised and as it is very frequent in use for XXTEA encryption generation we have design it in such a way so it reduce overall area and requires less time.*

1. INTRODUCTION

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 data, 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, firms and other organizations. Symmetric key cryptographic algorithms have a single key for both encrypted data using and deciphering. 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. In GSM, XXTEA is used in the A5/3 key stream generator and in GPRS in the GEA3 key stream generator. XXTEA was designed for 3GPP to be used in UMTS security system by Security Algorithms Group of Experts (SAGE), a division of the European standards body ETSI.[2] Because of planed pressures in 3GPP standardization, rather than of developing a new encrypted data, SAGE is in favour with 3GPP technical specification group (TSG) for module aspects of 3G security (SA3) to base the designing on an available methods that had already undergone some evaluation.[2] They chose the encrypted documents algorithm MISTY1 patented and developed by Mitsubishi Electric Corporation. The KCC core implements XXTEA encrypted data using in compliancy with the ETSI SAGE parameters. It executes 64-bit blocks using 128 -bit key. Normal core is very small (5,500 gates). Improved versions are available that support various encrypted documents modes (ECB, OFB, CFB, CBC, CTR. The module is fully synchronous and useful in both source and net list form. Test bench haves the XXTEA test vectors. The pioneer algorithm was somewhat modified for easier hardware implementation and to match other requirements set for 3G mobile documents transfer security.

2. KEY SCHEDULE

The key, K, is 128 bits long. Each round of XXTEA 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

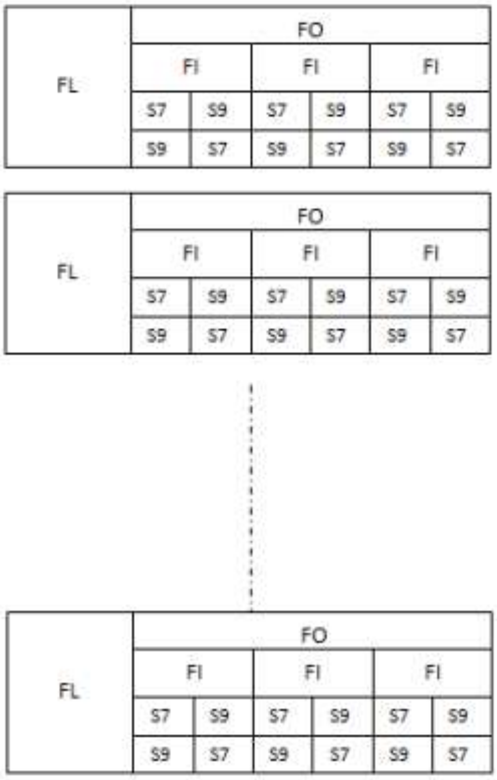


Figure 1: XXTEA encryption generator

$$
\begin{aligned}
KL_{i,1} &= \mathrm{ROL}(K_i, 1) \\
KL_{i,2} &= K'_{i+2} \\
KO_{i,1} &= \mathrm{ROL}(K_{i+1}, 5) \\
KO_{i,2} &= \mathrm{ROL}(K_{i+5}, 8) \\
KO_{i,3} &= \mathrm{ROL}(K_{i+6}, 13) \\
KI_{i,1} &= K'_{i+4} \\
KI_{i,2} &= K'_{i+3} \\
KI_{i,3} &= K'_{i+7}
\end{aligned}
$$

Figure 2: KASUMI key generator

3. TOOL PLATFORM AND LANGUAGE USED

Tool: Xilinx ISE : It is a EDA 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 digital systems. It is most generally used in the verification and design of digital circuits at gate and 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.

4. METHODOLOGY

KCC core is provided as portable VHDL thus allowing user to carry out an internal code cross check to ensure its security. The nature of the documents that flows throughout modern cellular documents exchanges networks has evolved noticeably since the early years of the first generation systems, when only voice sessions were possible. The method adopted for the proposed work is to design a Sbox not fully by memories or not fully by combinational design as both are related and so the present work shows architecture for the Sbox designing and it is basically the combination of two different methods that is memories and combinational, basically XXTEA is an standard and one cannot modify its dataflow and operation of each module like FI, FO, FL and Sbox but one can produce same results with different approach, as FI, FO and FL used only XOR operation or shifting or addition which is been already optimised by many researcher, only Sbox can be optimised and as it is very frequent in use for XXTEA encryption generation we have design it in such a way so it reduce overall area and requires less time.

Figure 3 shows the proposed s7 box and s9 box is also been designed in similar way as can be seen that proposed design is a feedback pipeline architecture and here two different module (combinational logic, EPROM) are been used total 8 times and at each time it stores the value in new buffer after eight iteration we have total 8 value in 8 different buffers then by using upper four bits of input we extract the final output.

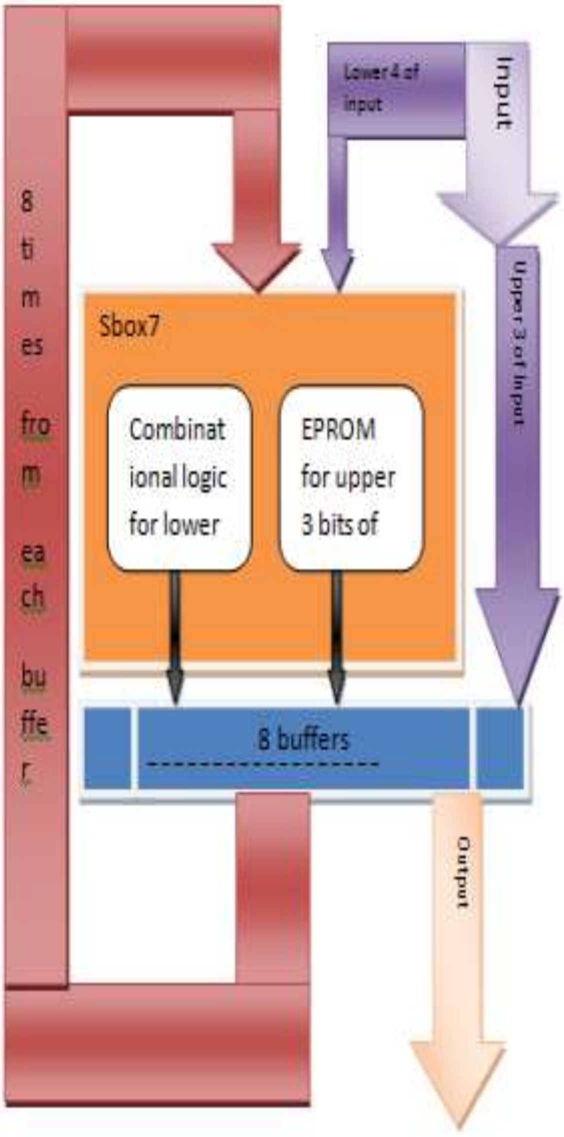

8 ti m es fro m ea ch bu ffe r
Lower 4 of input
Input
Sbox7
Combinat ional logic for lower
EPROM for upper 3 bits of
Upper 3 of input
8 buffers
Output

Figure 3: Proposed pipelined S7-box

5. SYNTHESIZE

The RTL schematic of proposed XXTEA encryption engine and as can be observed it has 128 bit key, 64 bit data input and 64 bit data output.

Figure 4 shows the synthesize summary results observed for the proposed work.

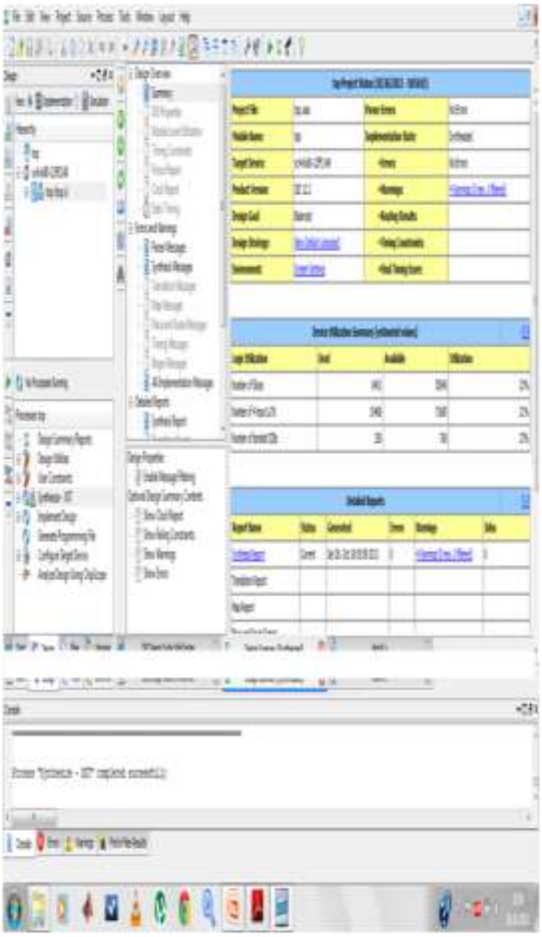


Figure 4: the synthesize summary

6. 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

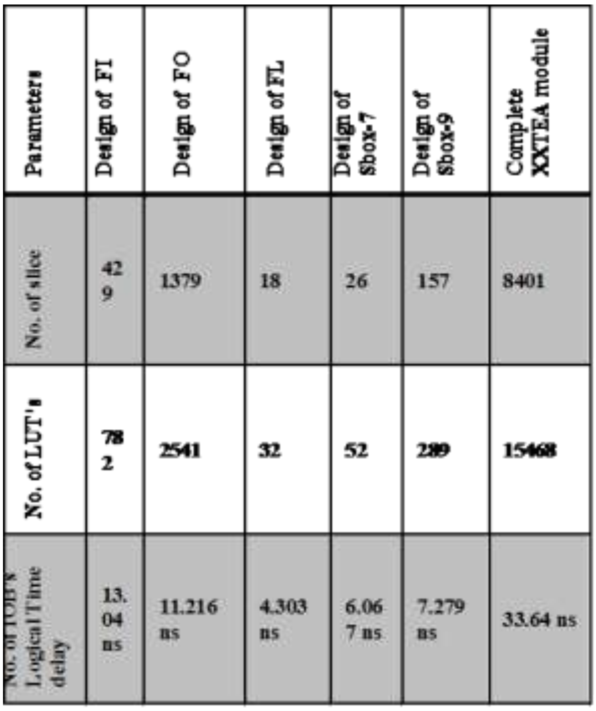
Input: A234a234567ba234

Output^Input: 7d6e14eebb5f4bf1

Avalanche:

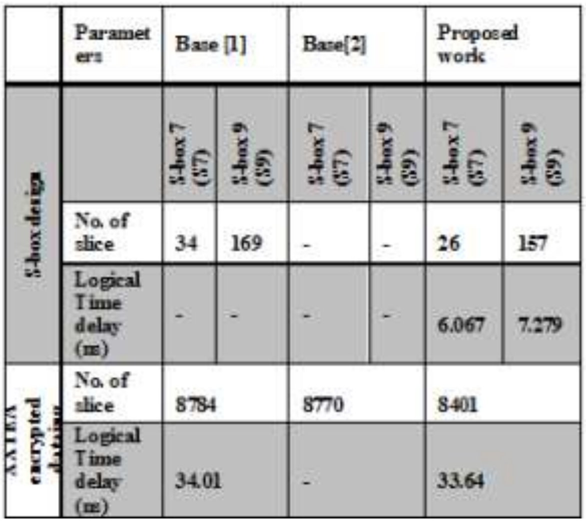
45 bit change/**64 bit**

Table 3: Results for each module



Parameters	Design of FI	Design of FO	Design of FL	Design of Sbox-7	Design of Sbox-9	Complete XXTEA 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 4 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
XXTEA encrypted data	No. of slice	8784		8770		8401	
	Logical Time delay (ns)	34.01		-		33.64	

7. CONCLUSION

The large number of potential subscribers and the advanced services to provide impose great challenges in terms of guaranteeing confidentiality and integrity of both documents and signalling. An efficient and compact hardware design of the XXTEA 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 encrypted datas. Not only does this proposal achieve a good performance, but is one of the most economical designs in terms of areaThe 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)

REFERENCES:

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

[2] Ren fung, ying-jian, Fu Xiao-bing, 'A Small and Efficient Implementation of XXTEA', IEEE Explore, WASE International Conference on Documents 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 XXTEA 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 XXTEA block encrypted data" 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 XXTEA encrypted dataing algorithm", T. Balderas-contreras et al. / Computers and electrical engineering 34 (2008) 531–546.