ELectronics EXpress

LETTER

IEICE Electronics Express, Vol.11, No.1, 1–6

VLSI design of a reconfigurable S-box based on memory sharing method

Weiwei Shan[1a)], **Xiao Zhang**[2], **Xingyuan Fu**[1], **and Peng Cao**[1]

[1] *National ASIC System Engineering Research Center, Southeast University, Nanjing, China, 210096*

[2] *Shanghai Information Security Testing Evaluation and Certification Center, Shanghai, China, 200011*

a) *wwshan@seu.edu.cn*

Abstract: S-box is a core component of many block cipher algorithms. A reconfigurable S-box based on look-up table (LUT) with memory-sharing is proposed in this paper. It uses a sharing memory to support different S-box operation modes (4×4, 6×4, and 8×8) for most of the block cipher algorithms as well as reduce memory size. It also supports high-speed pipeline structure of DES and Serpent. This new type of S-box is applied in a reconfigurable cryptographic coprocessor under 0.18 μm CMOS process. It is also used in a DES circuit with 16 pipeline stages. Synthesis results show that it works at 100 MHz frequency with flexibility of different modes and a reduced area compared to non-memory-sharing LUT method with equivalent sizes of different S-boxes.

Keywords: S-box, cryptographic circuit, memory sharing, DES, AES

Classification: Integrated circuits

References

[1] D. Fronte, A. Perez and E. Payrat: International Conference on Reconfigurable Computing and FPGAs (2008) 438.

[2] W. Yan, K. You, J. Han and X. Zeng: IEEE 8th International Conference on ASIC (2009) 135.

[3] C. Wang and H. M. Heys: The 8th IEEE International NEWCAS Conference (NEWCAS) (2010) 101.

[4] R. R. Rachh, B. S. Anami and P. V. Ananda Mohan: IEEE Region 10 Conference of TENCON (2009) 1.

[5] S. Morioka and A. Satoh: Proc. CHES 2002, LNCS **2523** (2003) 172.

[6] Opencores AES, DES cores, http://opencores.org/project

1 Introduction

Cryptographic algorithms are the foundation of information security systems. Currently, many cryptographic chips are widely developed [1, 2, 3, 4, 5]. However, most of them are dedicated to one or a few fixed cryptographic algorithms, not flexible for different applications. On the

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014

other hand, reconfigurable cryptographic coprocessors [1, 2] greatly improve the flexibility and expandability by reconfiguring the hardware interconnections to realize different algorithms. Among all operations, S-box is the only non-linear module to complete the confusion function, thus it plays an important role in many typical block cipher algorithms, such as DES, AES, Serpent, MARS and so on.

S-box is usually built in two ways: logic and Lookup table (LUT):

(1) Logic-based implementation uses hardware logic circuits to achieve composite fields calculations [3, 4, 5, 6], i.e., multi-stage Positive Polarity Reed-Muller (PPRM) form architecture for AES S-box [5]. Logic-based approach consumes fewer resources, however, it needs complex calculations while does not support parallel work. Besides, for different types of S-box operation, it has no reusability.

(2) In LUT-based implementation the S-box substitution table is stored in a memory (such as MEM or ROM or registers). Its input is the memory address input and its output is the data stored in the corresponding address space. This way, the operation is fast and can be configured to apply a variety of S-box operation for different block ciphers. Besides, when the processor is not running, algorithm memory does not contain any information before configuration; therefore, it is a more secure way for the processor. However, this method takes up much more hardware resources than logic-based method, because of the used memory cells, especially when several different S-boxes are needed.

In this paper, a memory-sharing reconfigurable S-box is proposed, which uses a sharing memory to reduce hardware resources in cryptographic circuits, as well as support different operation modes for flexibility. It is especially applicable for reconfigurable cryptographic processors. This novel S-box is applied in a reconfigurable cryptographic circuit and a pipelined DES circuit under 0.18 μm CMOS process. Experimental and simulation results show that it is able to support three kinds of different S-box operation modes (4×4, 6×4, and 8×8). Compared with logic based method, it uses twice gates in pipelined DES/Serpent, but with advantages in convenient reusability and realization. Compared to non-memory-sharing method, our memory-sharing method uses only 1/4 resources.

2 Design of memory sharing reconfigurable S-box

2.1 Basic structure of reconfigurable S-box

Commonly used S-box substitutions include the following modes: 4×4, 6×4, 8×8, and 8×32, among which the 8×8 substitution mode for AES is most widely used, where sixteen 8×8 S-boxes are needed for a 128 bit to 128 bit substitution. And for DES algorithm a 48bit-to-32 bit S-box substitution is needed in each round, which is realized by eight 6×4 S-boxes. Here 6×4 S-box means 6-bit $\rightarrow$ 4-bit substitution. In order to design one S-box to support three different substitution modes with different inputs, outputs and memory sizes are shown in Table I, we choose the minimum memory size of 512×4 bits to build a reconfigurable S-box, which suits one 8×8 substitution and eight 4×4 or 6×4 substitutions.

The basic structure of reconfigurable S-box unit is shown in Fig. 1. It consists of a substitution element and a sharing common memory of eight

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014

Table I. S-box type and design details

S-box type	Meaning	Minimum memory size needed	Our design input	Our design output
4×4	4bit input to 4bit output	16×4bit	6bit*	4bit Aout0[3:0]~Aout7[3:0]
6×4	6bit input to 4bit output	64×4bit	6bit	
8×8	8bit input to 8bit output	256×8bit=512×4bit	8bit	8bit Bout[7:0]

* With first high two bits set as 2b'00

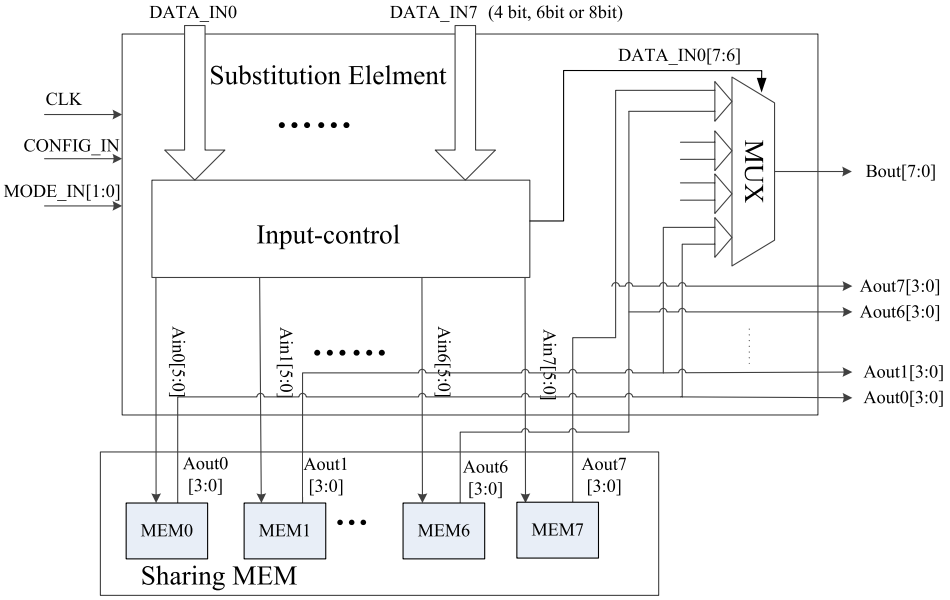

Fig. 1. Basic structure of reconfigurable memory-sharing S-box circuit

64 × 4 bit MEM blocks of MEM0, MEM1 to MEM7, standing for eight 6 × 4 S-boxes, realized by register arrays here.

2.2 S-box configuration

The input configuration signals control the status of the reconfigurable S-box unit to adapt to different block ciphers. There are two kinds of configurations, first one is the CONFIG_IN signal to determine whether S-box is in configuration or work state. The second configuration is about the substitution element mode, controlled by the MODE_IN signal with 2'b00 for 4 × 4 substitution, 2'b01 for 6 × 4 substitution and 2'b10 for 8 × 8 substitution.

2.3 Substitution element design

Substitution element is composed of input control and output control as shown in Fig. 1. First, for 4 × 4 and 6 × 4 modes, the width of store unit and output signal is 4 bit. The 4 × 4 mode is treated as a special 6 × 4 mode by setting the high two bits of the input signals DATA_IN0～ DATA_IN7 to 2'b00 through input control. And then the transformed input data Ain0 [5:0]～Ain7 [5:0] become the input address of sharing MEM to read the corresponding MEM unit, whose outputs are used as S-box outputs of Aout0 [3:0]～Aout7 [3:0] directly.

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014

Second, for the 8×8 mode, we need to make input signals to be DATA_IN0 = DATA_IN1 =……=DATA_IN7 by input-control. The input addresses of sharing MEM are: Ain0 [5:0], Ain1 [5:0]… and Ain7 [5:0]. The output control unit divides the eight groups of output data of sharing MEM to four groups with 8-bit width: (MEM0, MEM1), (MEM2, MEM3), (MEM4, MEM5), and (MEM6, MEM7). Then DATA_IN0 [7:6] decides which group to be chosen as the output from the four groups through a multiplexor.

Finally, In order to realize the 8×32 S-box operation, based on 8×8 S-box work mode, we need to add three more sharing MEM. In this way, the input is the same but the output is expanded to 32 bit for 8×32 S-box.

2.4 Multiple access memory design

The above S-box with one substitution and one sharing MEM can fulfill one 8×8 substitution or eight 6×4 (or 4×4) substitution, however, that is still not enough for a whole AES operation where sixteen 8×8 substitutions are needed. Conventional LUT method uses sixteen duplicated 8×8 S-boxes, making the memory size quite large. MEM-sharing method can reduce the memory size by multiple accesses to the memory realized by registers, as shown in Fig. 2.

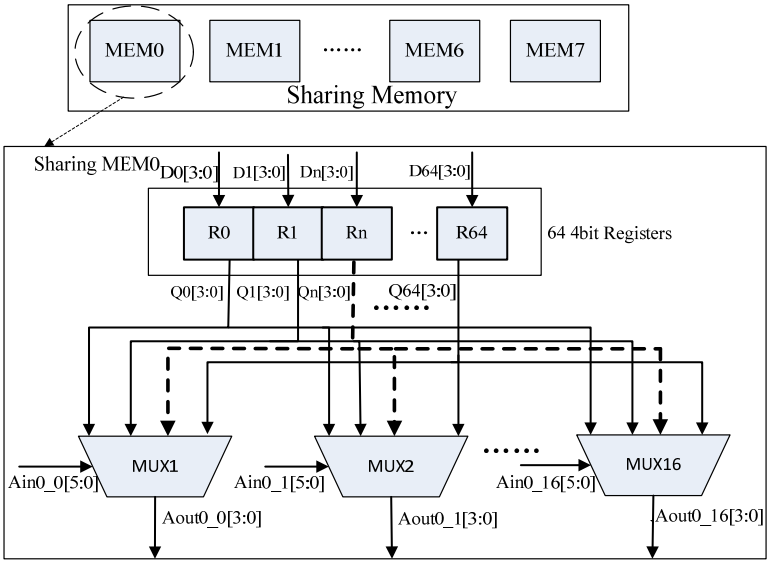

Fig. 2. The inner structure of sharing memory

The reading of the sharing MEM is actually realized by the multiplexors of the registers, where 16 MUXes are responsible for 16 S-boxes output chosen by the 6-bit Ain0_0 [5:0] to Ain0_16 [5:0]. The access of other MEM blocks is the same as MEM0. By this way we could achieve multiple outputs corresponding to multiple addresses at the same time, with the same one set of MEM, which made it possible for sixteen 8×8 S-boxes.

2.5 Pipeline design using memory-sharing method

The memory size of our reconfigurable S-box is much larger for one DES or Serpent algorithm; therefore, it can be used to configure the pipeline operation with N substitution elements and N multiplexors in sharing memory. Here N is the pipeline length, as shown in Fig. 3, where N is 16 for

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014

example to make full use of the memory. Therefore, the pipelined S-box is capable of be configured to be 16 same sized 8×8 S-boxes, and also could be configured to fulfill 16 DES S-boxes (16 groups of eight 6×4 bit S-boxes) or 16 Serpent S-boxes (16 groups of eight 4×4 bit S-boxes).

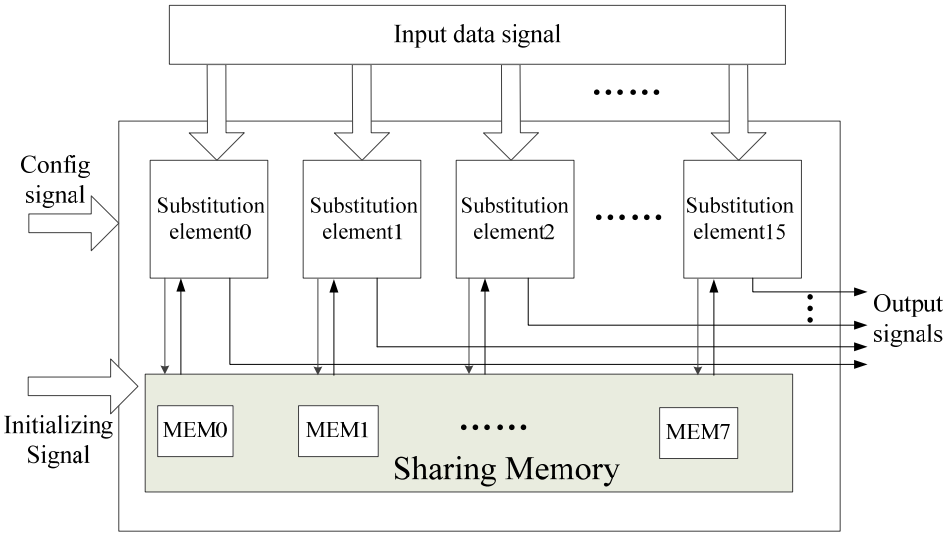

Fig. 3. Pipeline design of reconfigurable memory-sharing S-box structure

3 System application and simulation results

First, the proposed S-box is applied in a reconfigurable cryptographic coprocessor, which supports multiple block cipher algorithms. Besides, three other kinds of VLSI circuits application of S-boxes are designed in this paper for performance comparison, those are: (1) original DES circuit with eight 6×4 logic-based S-box [6], (2) original AES circuit with one 8×8 logic-based S-box [6]; and (3) pipelined DES circuit with our proposed memory-sharing S-box. They are all designed under 0.18 μm CMOS process with a working frequency of 100 MHz.

For a 16-stage pipelined DES, usually, 16 parallel 48bit-to-32 bit S-box units are required for ordinary LUT based S-boxes, using 16 times of larger memory size. In order to reduce the memory size, for our proposed MEM-sharing method, only one 512×4 bit MEM is needed to complete the 16 S-box units, as shown in Fig. 3, with some additional substitution elements and MEM multiplexors.

The synthesis results by Synopsys Design Compiler are shown in Table II. It can be seen that logic based S-boxes use very few logic gates, however, it has no reusability. In total, our pipeline S-box supporting one AES or 16 pipelined DES (or Serpent) uses 66,982 logic gates, about 4.4 times of non-pipeline method, instead of the 16 times of duplicated non-MEM sharing LUT pipeline method. The area of logic based pipeline method based on OpenCores AES and DES is estimated by 16 times of the area of S-boxes from the single Opencores cryptographic algorithm, without counting other connection parts needed in pipeline construction. By comparison, our method greatly reduces the memory size during pipeline operation, but with extra circuit area. When compared based on the same functions, our MEM-sharing S-box uses about twice gates of the logic-based

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014

Table II. DC synthesis results comparison for 0.18 μm CMOS process

Logic or LUT	S-box realization method	Application algorithms	S-box type and number	Memory size	Total area / gates
Logic: single S-box	**PPRM 1-stage [5]**	AES	One (8×8)	/	2242
	PPRM 3-stage [5]	AES	One (8×8)	/	701
	OpenCores-AES [6]	AES	One (8×8)	/	680
	OpenCores-DES [6]	DES	Eight (6×4)	/	908
	Open Cores-serpent	Serpent	Eight (4×4)	/	390
LUT: multiple S-box	**Our MEM-sharing**	AES, DES, and Serpent	one (8×8) Eight (6×4) Eight (4×4)	2056 bits	15,100
LUT: pipeline	**Our MEM-sharing**	AES, DES, and Serpent	16 groups of same (8×8)	2056 bits	66,982
LUT: pipeline	**Non-MEM-sharing**	AES, DES, and Serpent	16 groups of 8 different (6 × 4) -pipeline	32896	241,600
Logic: pipeline	***OpenCores with equivalent functions**	AES, DES, and Serpent	16 groups of 8 different (4 × 4) –pipeline	/	31,656

*: Estimated

method, but uses only about 1/4 gates of the non-MEM-sharing LUT method.

4 Conclusions

A reconfigurable S-box using MEM-sharing method is proposed with three typical work modes: 4×4, 6×4, and 8×8. It can also support pipeline structure circuits. It is applicable for a large number of block cipher algorithms with configurable parameters, resulting in convenience and security. What's more, the proposed S-box can save a lot of memory area compared to non-MEM-sharing LUT method. Therefore, it is very useful for the reconfigurable cryptographic circuits.

Acknowledgments

This work was sponsored by the National Natural Scientific Foundation of China (Grant No. 61006029) and Qing Lan Project.

DOI: 10.1587/elex.10.20130872
Received November 08, 2013
Accepted December 06, 2013
Publicized December 18, 2013
Copyedited January 10, 2014