Low Area Memory-free FPGA Implementation of the AES Algorithm

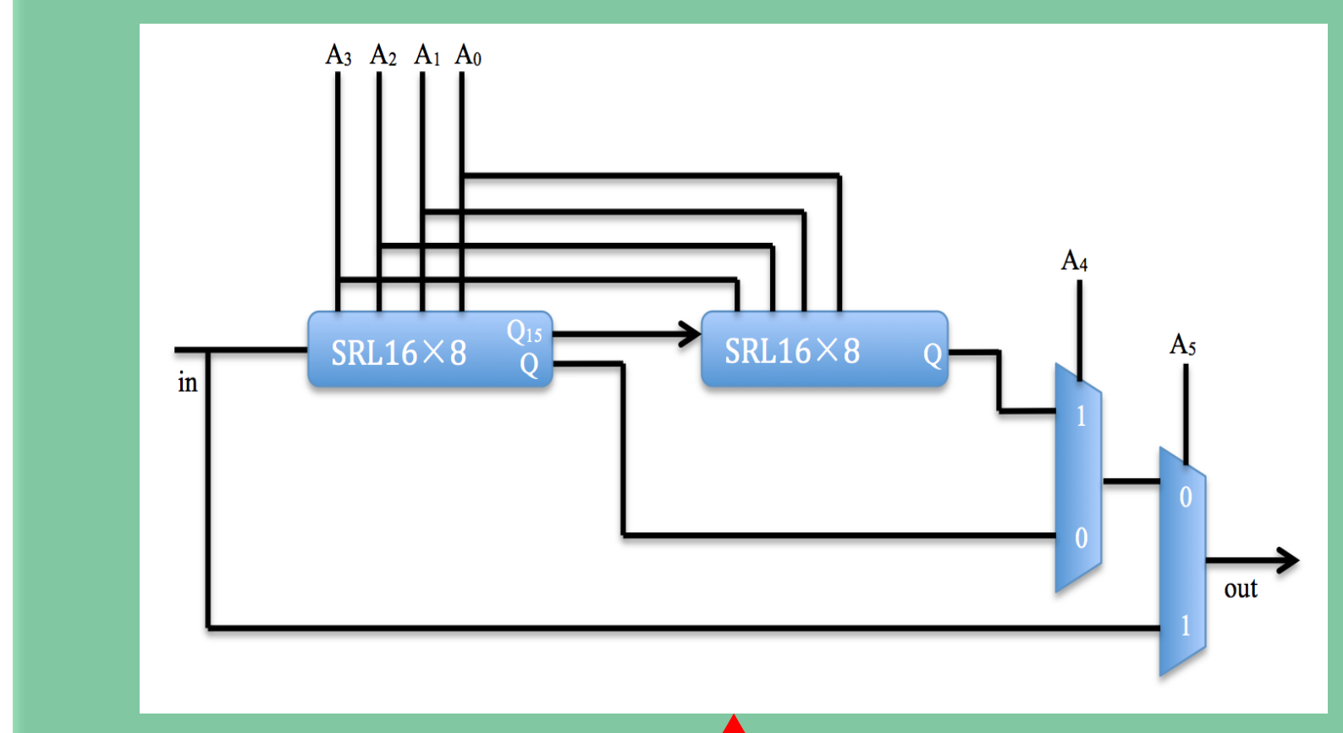
Abstract

A new FPGA design for the Advanced Encryption Standard (AES) is presented. This design is believed to be the smallest memory free FPGA implementation of the AES encryption only requiring 184 slices on a Xilinx Spartan 3 (XC3S50) device, and 80 slices on a Spartan 6 (XC6SLX4) device while achieving throughputs of 36.5Mbps and 58.13Mbps respectively. This FPGA design adopts an 8-bit architecture and exploits the specific fabric in Spartan 3 and Spartan 6 generation FPGAs to optimize the implementation of the shifting operations.

The AES

The AES is a symmetric block cipher, which uses the same key for both encryption and decryption. It has been broadly used for different applications, including smart cards, cellular phones, website servers and automated teller machines etc. Similar to other symmetric ciphers, the AES applies round operations iteratively to the plaintext to generate the ciphertext. There are four transformations in a round operation: SubBytes, ShiftRow, MixColumn and AddRoundKey. Derived from the cipher key, each round key is generated by an extra key expansion function.

Design Details



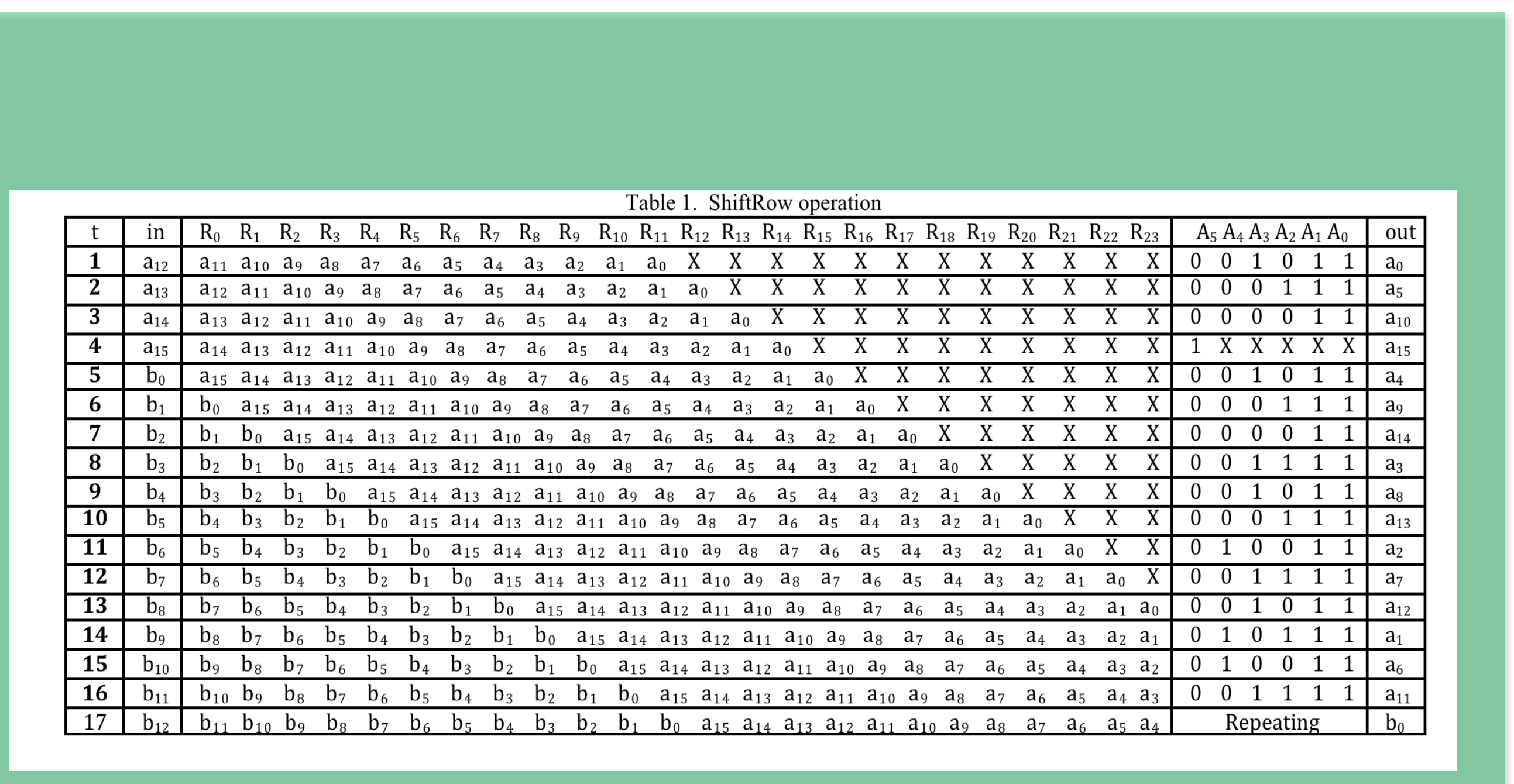
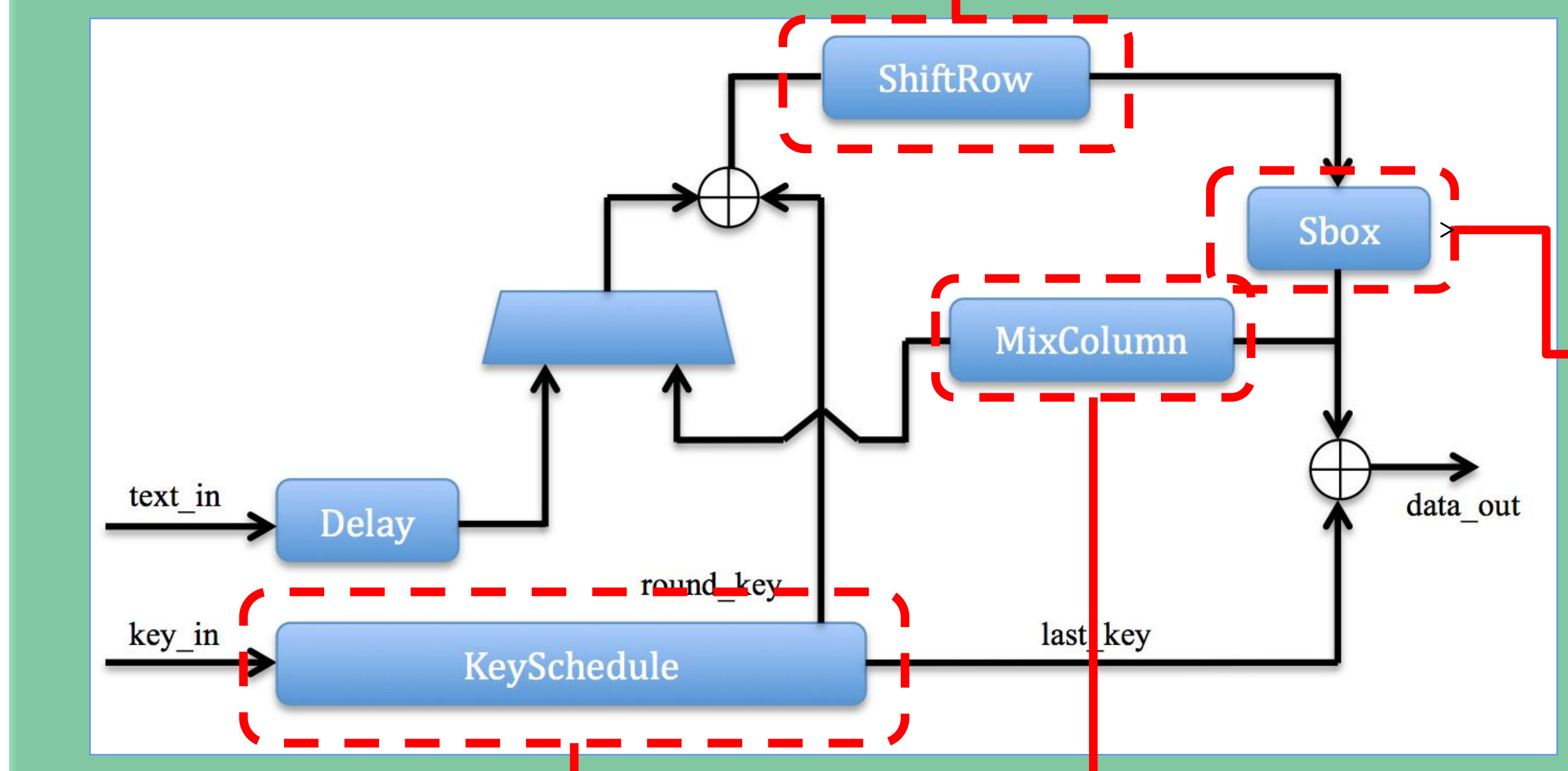
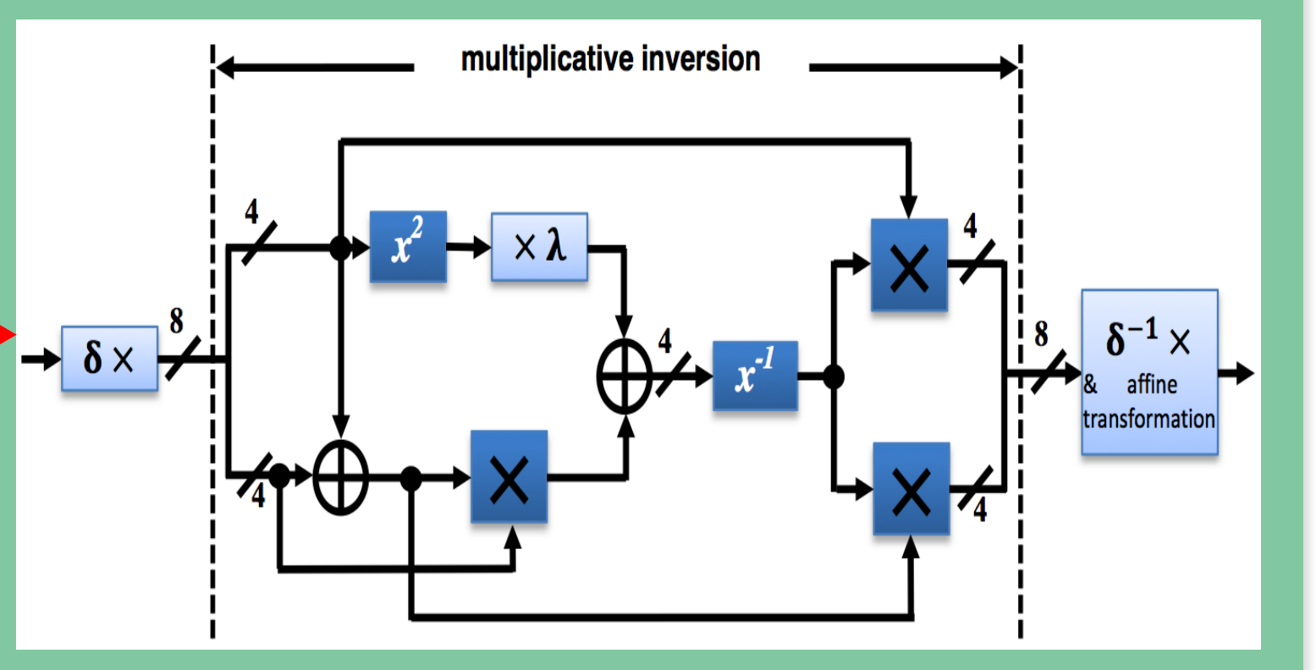
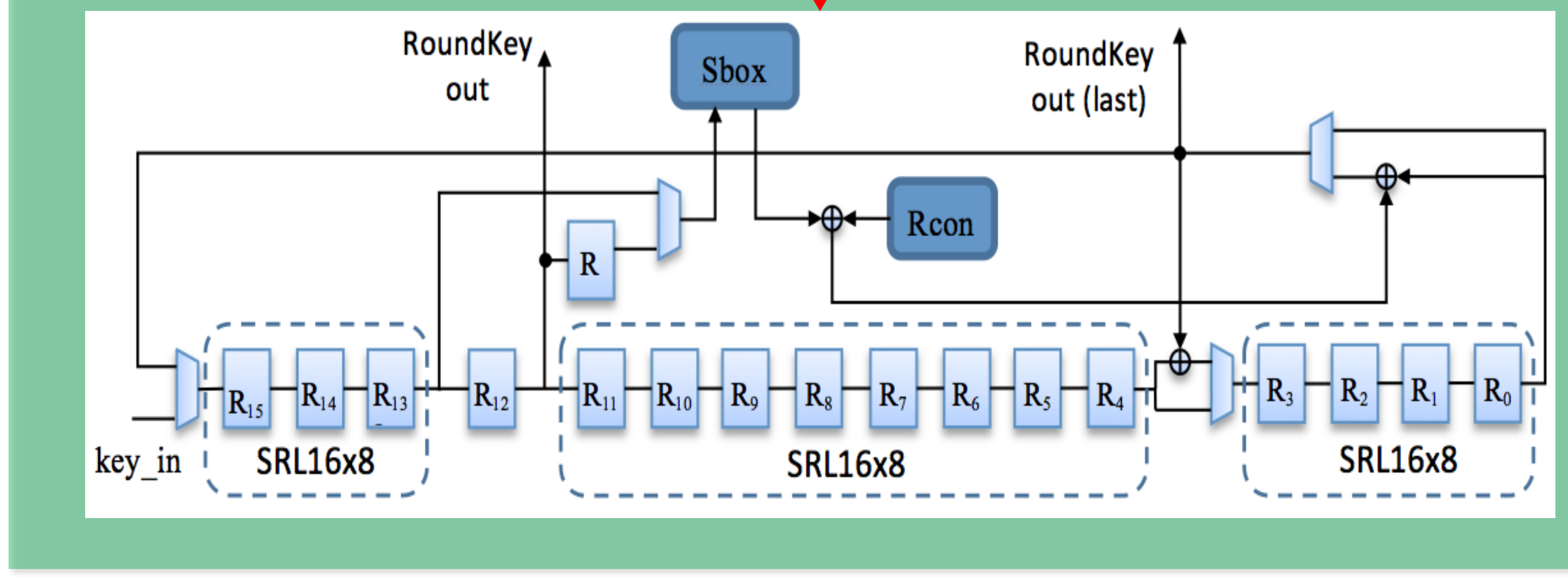


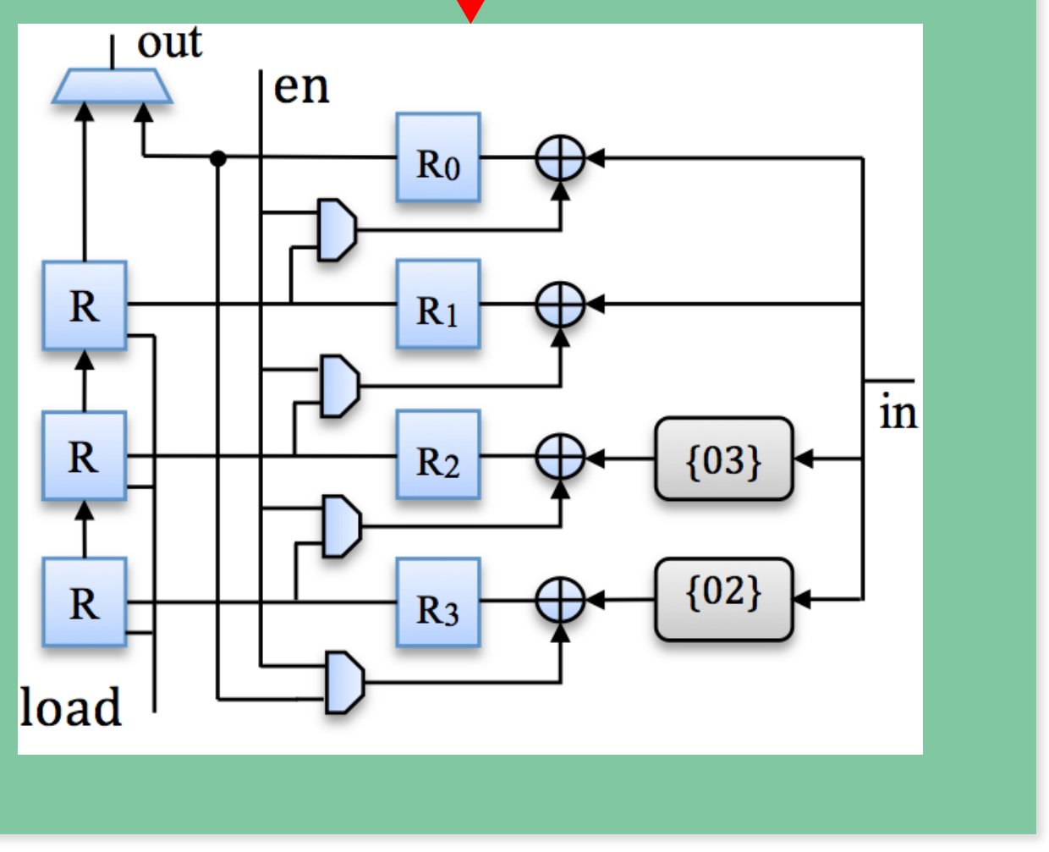
Table 1. ShiftRow operation

t	in	R_0	R_1	R_2	R_3	R_4	R_5	R_6	R_7	R_8	R_9	R_{10}	R_{11}	R_{12}	R_{13}	R_{14}	R_{15}	R_{16}	R_{17}	R_{18}	R_{19}	R_{20}	R_{21}	R_{22}	R_{23}	A_5	A_4	A_3	A_2	A_1	A_0	out
1	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	X	X	X	X	X	0	0	1	0	1	1	a_0
2	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	X	X	X	X	0	0	0	1	1	1	a_5
3	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	X	X	X	0	0	0	0	1	1	a_{10}
4	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	X	X	1	X	X	X	X	X	a_{15}
5	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	X	0	0	1	0	1	1	a_4
6	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	X	0	0	0	1	1	1	a_9
7	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	X	0	0	0	0	1	1	a_{14}
8	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	X	0	0	1	1	1	1	a_3
9	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	X	0	0	1	0	1	1	a_8
10	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	X	0	0	0	1	1	1	a_{13}
11	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	X	0	1	0	0	1	1	a_2
12	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	X	0	0	1	1	1	1	a_7
13	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0	0	0	1	0	1	1	a_{12}
14	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	0	1	0	1	1	1	a_1
15	b_{10}	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	a_2	0	1	0	0	1	1	a_6
16	b_{11}	b_{10}	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	a_3	0	0	1	1	1	1	a_{11}
17	b_{12}	b_{11}	b_{10}	b_9	b_8	b_7	b_6	b_5	b_4	b_3	b_2	b_1	b_0	a_{15}	a_{14}	a_{13}	a_{12}	a_{11}	a_{10}	a_9	a_8	a_7	a_6	a_5	a_4	Repeating						b_0









Introduction

A compact AES FPGA encryption core is proposed based on an iterative round-looping architecture as in [7] where the shifting operations are re-designed to exploit the FPGA fabric in Spartan 3 and Spartan 6 generations (Look-up-table based shift registers) to reduce overall area and improve speed. Since most useful modes (OFB, CTR and CFB) can all provide data encryption and decryption using only an encryption-primitive, it was decided to implement a design that performs AES encryption only, as this is the minimum requirement for three useful modes. To the authors' knowledge, this design is the smallest memory free FPGA implementation of the AES encryption to date.

Results Comparison(*with industrial products*)

Table 3. Synthesis results comparisons with industry products

	FPGA	MAX Throughput	Slices	Block RAM
Tiny AES cores [6]	Spartan 3E	30 Mbps	166	1
	Spartan 6	29 Mbps	91	0
Our work	**Spartan 3**	**36.5** Mbps	**184**	**0**
	Spartan 6	**58.13** Mbps	**80**	**0**

Results Comparison

Table 2. Synthesis results comparisons

	Chodowiec & Gaj [1]	Rouvroy et al [2]	Pramstaller et al [3]	T.Good & M.Benaissa [4]	Picoblaze based [4]	Yong Sung Jeon et al [5]	**This design**
FPGA	Spartan II XC2S30-6	Spartan III XC3S50-4	Virtex-E XCV1000E	Spartan II XC2S15-6	Spartan II XC2S15-6	Spartan II XC2S30-6	**Spartan III XC3S50-5**
Clock Frequency (MHz)	60	71	161	67	90	66	**45.642**
Data path	32	32	32	8	8	8	**8**
No. of Clock Cycles	44	46	92	3691	13546	352	**160**
Slices	222	163	1125	124	119	258	**184**
No. of Block RAMs	3	3	0	2	2	0	**0**
Block RAM Size (kbits)	4	18	0	4	4	0	**0**
Bits of block RAM used	9600	34176	0	4480	10666	0	**0**
Total Equivalent Slices	522	1231	1125	264	452	258	**184**
Throughput (Mbps)	166	208	215	2.2	0.71	24	**36.5**
Throughput/slice (kbps/slice)	318	169	191	8.3	1.9	93	**198**
Summary	Best speed/area	-	Fastest	ASIP	Software	-	**Smallest**

References

[1] P. Chodowiec, K. Gaj, Very Compact FPGA Implementation of the AES Algorithm, Cryptographic Hardware and Embedded Systems (CHES 2003), LNCS Vol. 2779, pp. 319 – 333, Springer-Verlag, October 2003.

[2] G. Rouvroy, F. X. Standaert, J. J. Quisquater, J. D. Legat, Compact and efficient encryption/decryption module for FPGA implementation of the AES Rijndael very well suited for small embedded applications, Proceedings of the international conference on Information Technology: Coding and Computing 2004 (ITCC 2004), pp. 583 – 587, Vol. 2, April 2004.

[3] N. Pramstaller, S. Mangard, S. Dominikus, and J. Wolkerstorfer. Efficient AES implementations on ASICs and FPGAs. In Proc. 4th Conf. on the Advanced Encryption Standard (AES 2004), pp. 98–112, Bonn, Germany, May 10–12, 2005.

[4] T. Good and M. Benaissa, "AES on FPGA from the Fastest to the Smallest,"LectureNotesinComputerScience,vol.3659,pp.427-440, Sep. 2005.

[5] Y. S. Jeon, Y. J. Kim, and D. H. Lee, "A Compact Memory-Free Architecture for the Aes Algorithm Using Resource Sharing Methods," Journal of Circuits, Systems, and Computers, vol. 19, no. 5, p. 1109, 2010.

[6] Helion. Tiny AES Cores. Available from: http://www.heliontech.com/aes_tiny.htm

[7] P. Hämäläinen, T. Alho, M. Hännikäinen, and T.D. Hämäläinen, "Design and Implementation of Low-Area and Low-Power AES Encryption Hardware Core", in Proc. DSD, 2006, pp.577-583.

The University Of Sheffield.

Electronic and Electrical Engineering

Junfeng Chu, Mohammed Benaissa