A Highly Efficient AES Cipher Chip

Chih-Pin Su, Tsung-Fu Lin, Chih-Tsun Huang, and Cheng-Wen Wu
Laboratory for Reliable Computing
Department of Electrical Engineering
National Tsing Hua University
Hsinchu, Taiwan 30013
ROC

Abstract—We present an efficient hardware implementation of the AES (Advanced Encryption Standard) algorithm, with key expansion capability. Instead of the widely used table-lookup implementation of S-box, the proposed basis transformation technique reduces the hardware overhead of the S-box by 64% and is easily pipelined to achieve high throughput rate. Using a typical 0.25μm CMOS technology, the throughput rate is 2.977 Gbps for 128-bit keys, 2.510 Gbps for 192-bit keys, and 2.169 Gbps for 256-bit keys with a 250MHz clock. Testability of the design is also considered. The area of the core circuit is about $1,279 \times 1,271 \mu m^2$.

I. Introduction

The large and growing number of Internet and wireless communication users has led to an increasing demand of security measures and devices for protecting the user data transmitted over the insecure media. The symmetric-key cryptography such as DES and AES [1], is one of the major components in a robust security system. Unlike the public-key cryptography, the symmetric-key cryptography uses an identical key between the sender and receiver, both to encrypt the message text and decrypt the cipher text. The characteristic of the high speed computing makes it more suitable for the encryption and decryption of a large amount of data. The AES algorithm, which was announced by the National Institute of Standards and Technology (NIST) of the United States, has been widely accepted for replacing DES as the new symmetric encryption algorithm.

The AES encryption is considered to be efficient both for hardware and software implementations. Some works have been presented on hardware implementations of the AES algorithm using FPGA [2] and ASIC [3]. Most of them used the ROM/RAM-based look-up table (LUT) to implement the S-box operation in the AES algorithm. It is cost-effective for SRAM-based FPGAs, but may not be a good choice for ASIC implementation. In this work, we present a more efficient hardware design for the AES algorithm [4]. The S-box is implemented using a basis transformation in the finite field, resulting in a much more cost-effective hardware than previous works. Furthermore, design-for-testability has been considered. With a 64% area reduction in S-box and about 50% total area reduction as compared with the best previous result, the speed also is enhanced. Using the TSMC 0.25μm CMOS technology, a 250MHz clock is easily achieved, and the throughput rate is 2.977 Gbps for 128-bit keys, 2.510 Gbps for 192-bit keys, and 2.169Gbps for 256-bit keys. The overall core size is $1,279 \times 1,271 \mu m^2$.

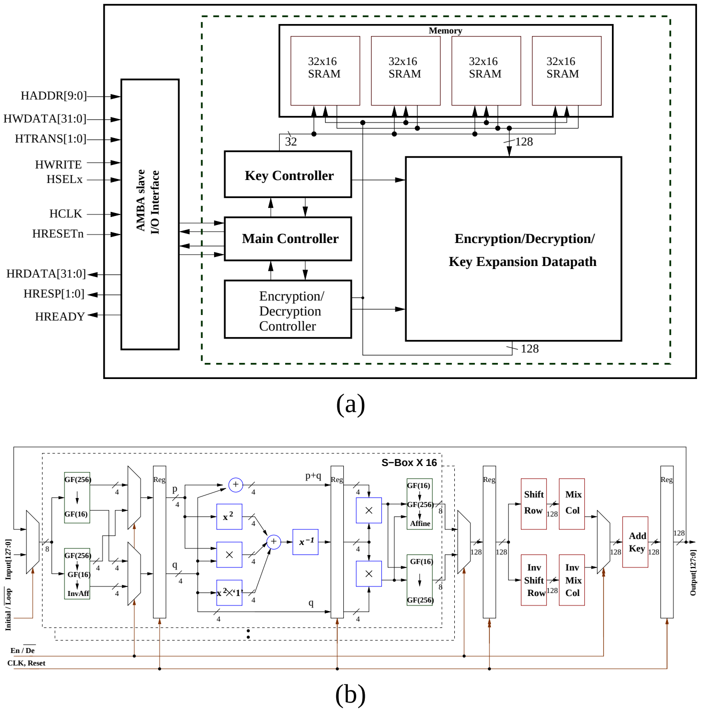

Fig. 1. (a) The block diagram of our AES design, and (b) the architecture of the encryption/decryption datapath [4].

II. Hardware Implementation

Figure 1(a) shows the block diagram of our AES chip and the architecture of our cost-effect en/decryption datapath [4]. The *Main Controller* generates control signals for data transportation, key expansion, encryption, and decryption. The initial key is gathered in the slices of word via the AMBA I/O Interface initially. The *Key Controller* then executes the key expansion routine. It controls the datapath to generate all the necessary round keys and stores them in four 32×32-bit SRAM

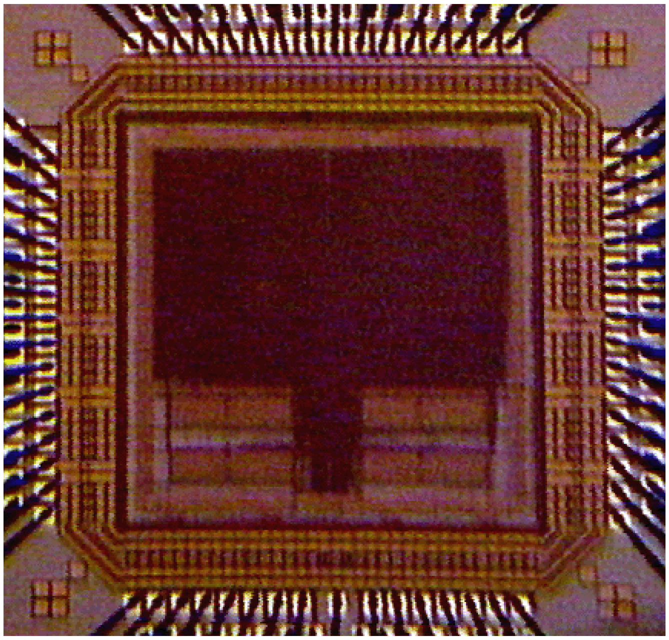

Fig. 2. Die photo of our AES chip.

modules that will be retrieved during the encryption or decryption phase. Once the round keys are ready, the *En/Decryption Controller* will take over the control and perform the encryption or decryption whenever a new 128-bit data block is ready from the I/O Interface. The AES round function will then be applied for 10, 12, or 14 iterations depending on the key size. Finally, the processed data will be exported through I/O interface.

Figure 1(b) depicts a 4-stage pipeline architecture of the AES datapath. The first three stages implement the proposed SubBytes() architecture, while the last one implements ShiftRows(), MixColumns() and AddRoundKey(). By choosing proper basis transformation, the area of S-box can be greatly reduced and the circuit is easily pipelined. DFT is also considered in our work. Four scan chains are implemented in our controllers. The fault coverage is 97.1% with 89 test patterns. Memory blocks are directly multiplexed out in the test mode. Due to the regular structure of our S-boxes, a BIST circuit is implemented to apply pseudo-exhaustive patterns. The fault coverage is about 99.8% reported by a commercial fault simulator with 512 test patterns (the 8-bit exhaustive patterns are applied twice to cover the faults in the multiplexers).

III. Experimental Results

Our design has been implemented on an Altera EP20K FPGA as well as an ASIC. Figure 2 shows the die photo of our AES chip with an area of $1,279 \times 1,271 \mu m^2$ (about $63.4K$ gates) using the TSMC $0.25\mu m$ CMOS technology by cell-based design flow. Although the packaged chip has a limited clock rate due to external loading, post-layout simulation showed that the circuit can function correctly at 250MHz for the typical case (see Fig. 3), achieving over 2 Gbps throughput. Some important facts of the chip are listed in Table I.

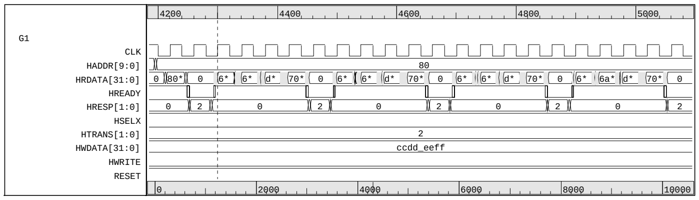

Fig. 3. The encryption waveform at 250MHz with a post-layout simulation.

TABLE I
Test chip characterization.

Technology	TSMC $0.25\mu m$ CMOS
Package	12CQFP
Core Size	$1,279 \times 1,271 \mu m^2$
Gate Count	63.40K
Max. Freq.	250MHz
Throughput	2.977 Gbps (128-bit key)
	2.510 Gbps (196-bit key)
	2.169 Gbps (256-bit key)

IV. Conclusions

We have presented a high throughput, area efficient implementation of the AES algorithm. The complexity of the S-box is greatly reduced by a basis transformation from $GF(2^8)$ to $GF(2^4)$. There is a 64% area reduction in S-box and about 50% total area reduction as compared with the previous LUT approaches. The pipelined AES chip provides a very high throughput while keeping the area small. In addition, our design can also perform key expansion on-line. With the standard on-chip bus interface, the AES cipher can be plugged into the system chip easily. Finally, testability has been stressed in the proposed design.

References

[1] National Institute of Standards and Technology (NIST), *Advanced Encryption Standard (AES)*, National Technical Information Service, Springfield, VA 22161, Nov. 2001.

[2] A. J. Elbirt, W. Yip, B. Chetwynd, and C. Paar, "An FPGA-Based performance evaluation of the AES block cipher candidate algorithm finalists", *IEEE Trans. VLSI Systems*, vol. 9, no. 4, pp. 545–557, Aug. 2001.

[3] H. Kuo and I. Verbauwhede, "Architectural optimization for a 1.82 Gbits/sec VLSI implementation of the AES Rijndael algorithm", in *Cryptographic Hardware and Embedded Systems (CHES) 2001*, Ç. K. Koç, D. Naccache, and C. Paar, Eds. 2001, number 2162 in LNCS, Springer-Verlag.

[4] T.-F. Lin, C.-P. Su, C.-T. Huang, and C.-W. Wu, "A high-throughput low-cost AES cipher chip", in *Proc. 3rd IEEE Asia-Pacific Conf. ASIC*, Taipei, Aug. 2002, pp. 85–88.