International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:2, No:5, 2008

A Low-cost Reconfigurable Architecture for AES Algorithm

Yibo Fan, Takeshi Ikenaga, Yukiyasu Tsunoo, and Satoshi Goto

***Abstract*—**This paper proposes a low-cost reconfigurable architecture for AES algorithm. The proposed architecture separates *SubBytes* and *MixColumns* into two parallel data path, and supports different bit-width operation for this two data path. As a result, different number of S-box can be supported in this architecture. The throughput and power consumption can be adjusted by changing the number of S-box running in this design. Using the TSMC 0.18μm CMOS standard cell library, a very low-cost implementation of 7K Gates is obtained under 182MHz frequency. The maximum throughput is 360Mbps while using 4 S-Box simultaneously, and the minimum throughput is 114Mbps while only using 1 S-Box.

***Keywords*—**AES, Reconfigurable architecture, low cost.

I. Introduction

ADVANCED Encryption Standard (AES) [1] was selected by the National Institutes of Standards and Technology (NIST) as a new encryption standard to replace the Data Encryption Standard (DES) in Oct. 2000. The AES algorithm is a symmetric block cipher that processes data blocks of 128 bits. The data is operated by 10, 12 or 14 rounds of transformations with key length equal to 128, 192 or 256 bits.

A lot of hardware implementations of AES algorithm already have been proposed. They can be classified into two types: high speed designs and low- cost designs. Because of the increase of personal security requirement and mobile device usage, the low-cost design is the trend for AES implementation.

Among the existing low-cost designs, some focus on architecture design, such as Satoh's work in [2]. Some focus on S-Box design, such as Canright's work in [3]. Some focus on ultra low power AES design which can be used in RFID, which can be found in [4]. However, there are few proposals on reconfigurable design, which can be configured for different throughput up to the requirement of system. For power-limited system, reconfigurable design which can provide different performance and power consumption is much more attractive than fixed architecture design.

In this paper, a very low-cost reconfigurable architecture for AES algorithm is proposed. This architecture can be configured into different modes which has different throughput and power consumption. The ability of reconfiguration is achieved by changing the number of S-box running in the data path. While using more S-box, the performance is increased, and the power consumption also be increased.

This paper is organized as follows. AES algorithm is introduced in Section 2. The reconfigurable architecture is presented in Section 3. The experimental results and comparison are given in Section 4. Finally, conclusion is provided in Section 5.

Y. Fan, T. Ikenaga and S. Goto are with Graduate School of Information, Production and Systems, Waseda University, Japan (e-mail: fanyibo@ruri.waseda.jp).

Yukiyasu Tsunoo is with Internet Systems Research Laboratories, NEC Corp., Japan.

II. AES Algorithm

AES, also known as Rijndael, is the most popular algorithm used in symmetric key cryptography. AES operates on a 4×4 array of bytes termed the *State*. For encryption, it implements a round function 10, 12, 14 times (depends on the key length). The encryption and decryption flow of AES algorithm are shown in Fig. 1 (a) and (b). Four transformations including Subbytes, ShiftRows, MixColumns and Addroundkey are performed in the encryption process, and the other four inverse transformations are performed in the decryption process. A separate KeyExpansion unit is used to generate keys for each round of AES algorithm. In order to simplify the hardware implementation and support both of encryption and decryption, a hybrid dataflow is proposed, which is shown in Fig. 1 (c). This data flow adjusts the order of some transformations. The advantage of this dataflow is that it reduces the number of MixColumns module from 2 to 1. (Normally, 2 MixColumns module are needed in AES, such as Satoh's work in [2]).

Fig. 2 shows the operations in AES algorithm. The briefly introduction is listed as below:

1) SubBytes: The SubBytes operation is a non- linear byte substitution that operates on each byte of the *State* using a substitution table.
2) ShiftRows: In the ShiftRows operation, the bytes in the last three rows of the *State* are cyclically shifted over different numbers of bytes.
3) MixColumns: Mixing operation which operates on the columns of the *State* using a linear transformation.
4) AddRoundKey: A Round Key is added to the *State* by a simple bitwise XOR operation.

The detailed description of these operations can be found in [1]. There are a lot of proposals about hardware design of these sub-modules. Especially the hardware reuse methods are proposed very much, which can be found in [2-6]. These

methods are valuable for low-cost implementation of AES algorithm.

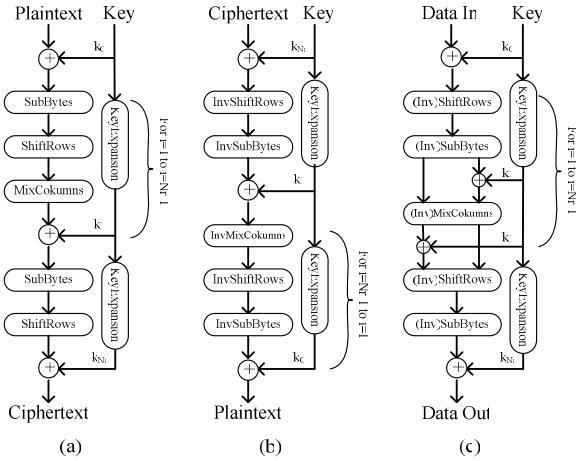

Fig. 1 Data flow (a) Encryption (b) Decryption (c) Proposed hybrid dataflow for encryption & decryption

III. Reconfigurable Architecture for AES Algorithm

A. Reconfigurable Architecture

The proposed reconfigurable architecture is shown in Fig. 3. This architecture is different from all of the existing designs, and some new ideas are introduced in this architecture.

Parallel Data Path with Different Bit-Width: There are two data paths in parallel in this design: a) SubBytes data path (8-bit, 16-bit and 32-bit). b) MixColumns data path (32-bit). The advantage of this design includes two points:

Firstly, it provides much more flexibility than serial data path. Most of the low-cost designs use serial data path which connects SubBytes, MixColumns in serial. In this way, all of the operations of AES algorithm should use the same bit width. This is not efficient. Different from serial design, our architecture separates the SubBytes and the MixColumns into two data paths. It can support different bit width operation for SubBytes and MixColumns.

Secondly, it achieves good performance. As the SubBytes module and MixColumns module in parallel data path, the critical path of our design is shorter than the serial data path design.

Reconfigurable S-box: Our architecture supports different bit width for SubBytes, so the number of S-box can be configured in the data path. As shown in Table I, SubBytes is an 8-bit operation. Every S-box in Fig. 3 executes one SubBytes operation. There are totally 4 S-boxes in our architecture, so it can support 4 SubBytes simultaneously. Since the S-box module consumes a lot of power, the power-aware ability can be achieved by adjusting the number of S-box running in the data path. While using less S-box in the data path, the throughput becomes lower and the power consumption also can be reduced.

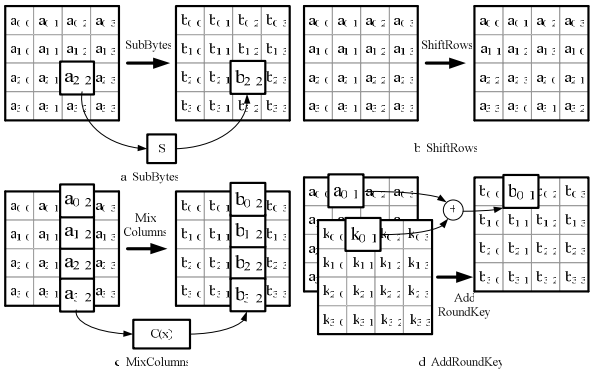

Fig. 2 Transformations in AES Algorithm

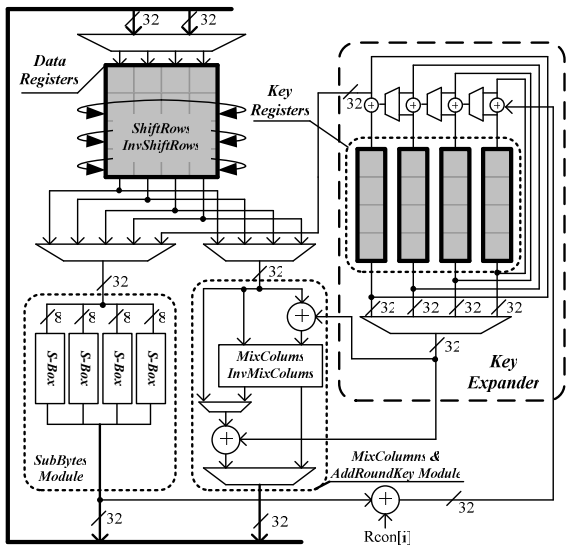

Fig. 3 Reconfigurable Architecture

TABLE I
Bit Width for Each Operation in AES Algorithm

Operations	*Min. bit width for operations*
(Inv)SubBytes	8-bit
(Inv)ShiftRows	-
(Inv)MixColumns	32-bit
AddRoundKey	1-bit
KeyExpansion	8-bit

32-bit MixColumns & AddRoundKey Module: From table 1, the bit width for MixColumns is 32-bit. We implement this module by using 32-bit I/O-width. The structure of this module is based on proposed hybrid dataflow in Fig. 1 (c). Only one MixColumns module is needed in this design.

Different from Satoh's work in [2] and Feldhofer's work in [4], our implementation achieves lower hardware cost than Satoh's work with same performance, and higher performance than Feldhofer's work with extra hardware cost.

B. Mode Configurations

There are three mode configurations in our design. Each configuration uses different number of S-box in the data path, so the throughput and power consumption of each configuration are also different. Fig. 4 shows these 3 configurations. Config.a only uses 1 S-box in the data path, and the bit-width for SubBytes module is 8-bit. It has lowest power consumption and speed. Config.b and Config.c use 2 and 4 S-boxes. Config.c uses 32-bit bit-width for SubBytes, it has highest throughput and highest power consumption.

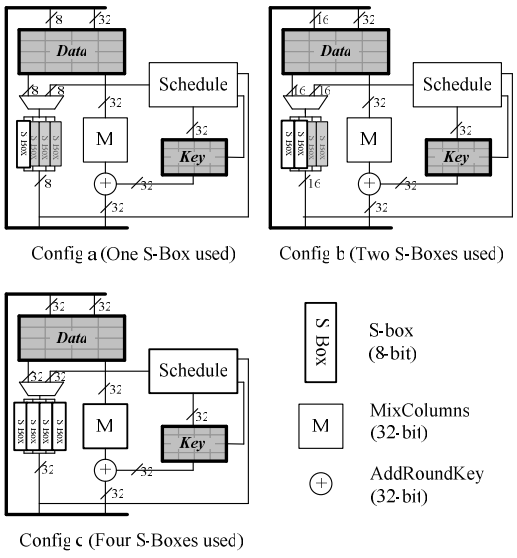

Fig. 4 Mode configurations

C. Dataflow

The cycle accurate dataflow of 3 configurations is shown in Fig. 5. The round function of AES algorithm is divided into 3 steps: First Round, Round Loop and Last Round. As our architecture has parallel data path, some operations of AES can be executed in parallel, such as {Subbytes & MixColumns} and {KeyExpansion & MixColumns}.

Table II shows the number of clock cycles consumed in each round and the total number of clock cycles needed for AES encryption with 128-bit key length. From Table II, the config.a which only uses 1 S-box needs much more clock cycles than other two configurations. The config.c uses 4 S-boxes simultaneously, so it can save a lot of clock cycles.

By using the proposed reconfigurable architecture, mode configurations and dataflows, different performance and power consumption can be achieved. This design is very suitable for power-limited systems, such as mobile phone. The performance and power consumption of AES can be adapted to the bandwidth condition or the throughput of top-level system.

IV. Experimental Results

Using the TSMC 0.18 μm CMOS standard cell library and the Sysnopsys Design Compiler Tools, the implementation results are shown in Table III. The total hardware cost for our design is 6986 Gates, and the frequency is 182 MHz. The power consumption of these 3 mode configurations is directly measured by synthesis result without doing power optimization. All of these data is got under 182 MHz system clock and 1.62V system voltage.

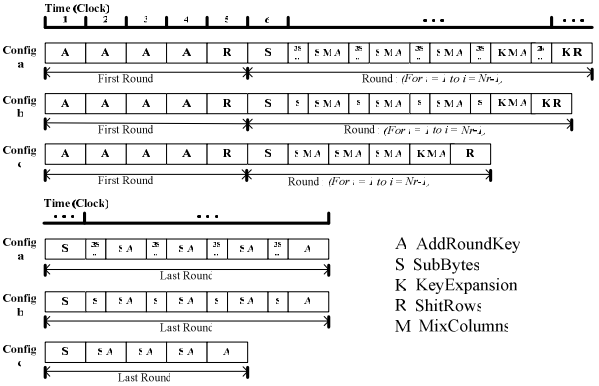

Fig. 5 Cycle Accurate Data Flows

TABLE II
Bit Width for Each Operations in AES Algorithm

	Number of Cycles		
	Config.a	Config.b	Config.c
First Round	5	5	5
Round Loop	20	10	6
Last Round	17	9	5
Total (AES 128-bit Encryption)	202 (5+20*9+17)	104 (5+10*9+9)	64 (5+6*9+5)

Table IV shows the comparison of our design with other low-cost implementations. Satoh's design in [2] is a 32-bit serial data path design. We implement his design by ourselves to compare the serial data path design with parallel data path design under the same condition. Zhao's design in [6] is a 32-bit pipelined serial data path design. Feldhofer's design in [4] is 8-bit parallel data path design, and Pramstaller's design in [7] is 32-bit parallel data path design.

Compared to other's design, our design achives both low hardware cost and resonable throughput. Moreover, our design has 3 mode configurations which can provide different throughput and power consumption. In order to achieve lower power consumption, other power optimization technologies such as clock gating also can be used in this design.

V. Conclusion

In this paper, we introduced a low-cost VLSI design of AES algorithm. A reconfigurable architecture which can support different number of S-box running in the data path is proposed, and it achieves performance configurability and power consumption configurability. This design is very suitable to be used in the power-limited mobile systems.

TABLE III
EXPERIMENTAL RESULTS @ 182MHZ, 1.62V

AES Components		Area		Config.a Power		Config.b Power		Config.c Power	
		Gates	%	mW	%	mW	%	mW	%
ShiftRows+ Data Registers		1380	19.8%	2.03	24.6%	2.50	19.4%	2.88	13.8%
S-Box	S-Box 0	618	8.8%	0	0%	0	0%	3.38	16.2%
	S-Box 1	643	9.2%	0	0%	0	0%	3.88	18.6%
	S-Box 2	651	9.3%	0	0%	3.45	26.8%	3.40	16.3%
	S-Box 3	693	9.9%	3.25	39.5%	3.56	27.7%	3.46	16.6%
MixColumns/InvMixcolumns		576	8.2%	0.83	10.1%	0.82	6.4%	0.73	3.5%
Key Expander+Key Registers		1590	22.8%	1.34	16.3%	1.49	11.6%	1.75	8.4%
Controller		250	3.6%	0.26	3.2%	0.33	2.6%	0.40	1.9%
Others		585	8.4%	0.52	6.3%	0.71	5.5%	0.98	4.7%
Total		6986	100%	8.24	100%	12.87	100%	20.87	100%

TABLE IV
COMPARISON WITH OTHER'S WORK

Ref	Tech	Gates	Freq.	Throughput	Configurations
[*]	0.18μm	7226	138MHz	327Mbps	-
[4]	0.35μm	3595	100KHz	12.6Kbps	
[6]	0.25μm	12000	100MHz	256Mbps	
[7]	0.6μm	8541	50MHz	70Mbps	
Ours	0.18μm	6986	180MHz	114Mbps	*Config.a*
				221Mbps	*Config.b*
				360Mbps	*Config.c*

[*] 32-bit serial design using Satoh's architecture in [2]

ACKNOWLEDGMENT

This research was supported by ``Ambient SoC Global COE Program of Waseda University'' of the Ministry of Education, Culture, Sports, Science and Technology, Japan.

REFERENCES

[1] National Institute of Standards and Technology (U.S.). Advanced Encryption Standards (AES). FIPS Publication 197, 2001.
[2] A. Satoh, S. Morioka, K. Takano, S. Munetoh, "A Compact Rijndael Hardware Architecture with S-Box Optimization," Advances in Cryptology - ASIACRYPT 2001, 7th International Conference on the Theory and Application of Cryptology and Information Security, Gold Coast, Australia, December 9-13, 2001, pp.239 – 254.
[3] D. Canright, "A Very Compact S-Box for AES," Cryptographic Hardware and Embedded Systems – CHES, September, 2005, pp.441 – 455.
[4] M. Feldhofer, S. Dominikus, J. Wolkerstorfer, " Strong Authentication for RFID Systems Using the AES Algorithm," Cryptographic Hardware and Embedded Systems - CHES 2004, Volume 3156, pp.357-370.
[5] S. Morioka, A. Satoh, "An Optimization S-Box Circuit Architecture for Low Power AES Design", CHES 2002, LNCS 2523, pp. 172-186.
[6] Jia Zhao, Xiaoyang Zeng, Jun Han, Jun Chen, "Very Low-cost VLSI Implementation of AES Algorithm", IEEE Asian Solid-State Circuits Conference, 2006, pp. 223 - 226.
[7] Norbert Pramstaller, Stefan Mangard, Sandra Dominikus, and Johannes Wolkerstorfer, "Efficient AES Implementations on ASICs and FPGAs", Proceedings of the Fourth Workshop on the Advanced Encryption Standard, AES4- State of the Crypto Analysis, LNCS vol- 3373 2005, pp. 98 – 112.