VLSI ARCHITECTURE DESIGN AND IMPLEMENTATION FOR TWOFISH BLOCK CIPHER

Yeong-Kang Lai[†], *Liang-Gee Chen*[‡], *Jian-Yi Lai*[‡], *and Tai-Ming Parng*[‡]

[†]Department of Electrical Engineering
National Chung Hsing University
Taichung, Taiwan, R.O.C.

[‡]Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan, R.O.C.

ABSTRACT

In this paper, a novel VLSI architecture of the TWOFISH block cipher is presented. Based on the loop-folding technique combined with efficient hardware mapping, the architecture can make data encryption/ decryption more efficient and secure. To demonstrate the correctness of our design, a prototype chip for the architecture has been implemented by using 0.35 μ CMOS technology. The chip can achieve an encryption rate of 200 Mb/s and consume 44 mW while operating at a 66 MHz clock rate. Therefore, the chip can be applied to on-line encryption in high-speed networking protocols like ATM networks.

1. INTRODUCTION

With the explosive growth in computer systems and their interconnections via networks has increased the dependence of both organizations and individuals on the information stored and communicated using these systems. However, in these networking environments there are no such guarantees that all kinds of information (databases, video programs, telecommunication etc...) can avoid unauthorized access, because the transmission medium is open, which implies that anyone with the appropriate protocol analyzer can eavesdrop as well. This, in turn, has led to a heightened awareness of the need to protect data and resources from disclosure, to guarantee the authenticity of data and messages, and to protect systems from network-based attacks.

Many of the cryptographic algorithms that have been developed are being used in software implementations on computers (e.g. to have protection of coded passwords for users). For low complexity type of applications, such as the protection of information in files and databases this is probably the most economic solution. However, a number of applications require such high throughputs for the encryption/decryption process that they cannot be executed on a normal general purpose microprocessor. These applications require dedicated ASIC implementations. In the past, many VLSI implementations in block cipher have been proposed such as DES, IDEA, SAFER, and 3WAY[2]-[4].

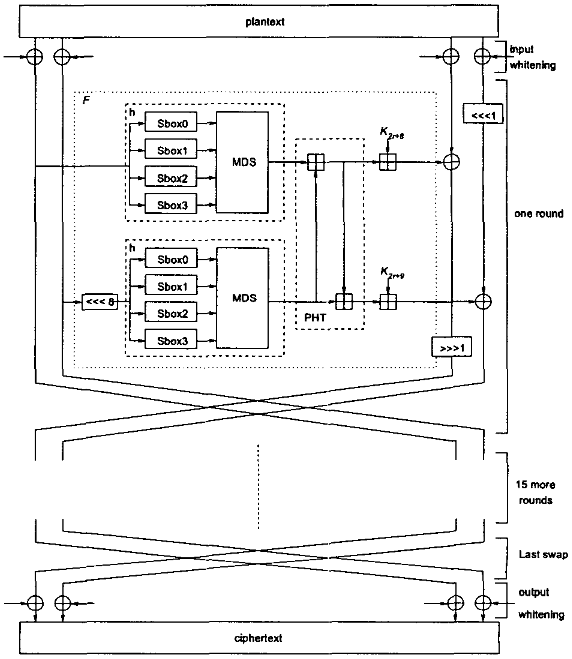

Figure 1: Data flow graph of twofish block cipher.

In this paper, we present a novel architecture and VLSI implementation of compact and low-power module which implements the Twofish data encryption algorithm. The proposed architecture can be efficiently applied to the high speed networking.

2. TWOFISH ENCRYPTION ALGORITHM

Twofish is a 128-bit block cipher. It can work with variable key lengths: 128, 192, or 256 bits. It consists of 16 rounds built similarly to Feistel network structure [5]. Figure 1 shows the data flow graph of the cipher structure. In addition, input and output data are XORed with eight subkeys, K_0 .. K_7. These XOR operations are called input and

0-7803-7448-7/02/$17.00 ©2002 IEEE

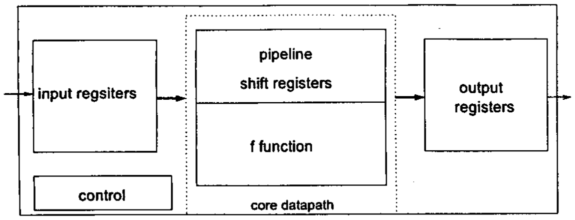

Figure 2: Overall architecture of Twofish

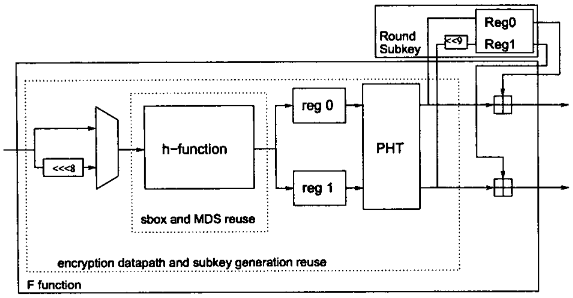

Figure 3: Architecture of F-function

output whitening. The only non-Feistel elements are the 1-bit rotates. The rotations can be moved into the F function to create a pure Feistel structure, but this requires an additional rotation of the words just before the output whitening step.

The plaintext is split into four 32-bit words. In the input whitening step, these are xored with four key words. This is followed by sixteen rounds. In each round, the two words on the left are used as input to the h functions. (One of them is rotated by 8 bits first.) The h function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an Maximum Distance Separable (MDS) matrix. The results of the two h functions are combined using a Pseudo-Hadamard Transform (PHT), and two keywords are added. These two results are then xored into the words on the right (one of which is rotated left by 1 bit first, the other is rotated right afterwards). The left and right halves are then swapped for the next round. After all the rounds, the swap of the last round is reversed, and the four words are xored with four more key words to produce the ciphertext.

3. VLSI ARCHITECTURE

The VLSI architecture for the realization of Twofish block cipher fundamentally consists of two main modules, key scheduling module and encryption datapath. As shown in Figure 2 and Figure 3, the key-scheduling module generates the subkeys on the fly from the user-defined session key. In the case of encryption/decryption process, the generated subkeys are provided to the encryption datapath. The core of the encryption datapath mainly performs the F function, as shown in Figure 4. It consists of S-boxe unit, MDS matrix unit, and PHT unit. In the following, we will discuss the detail of each component.

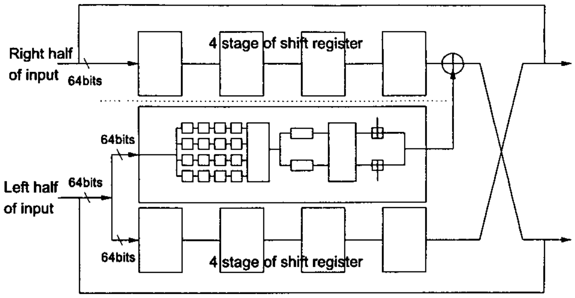

Figure 4: Detailed architecture of F function unit

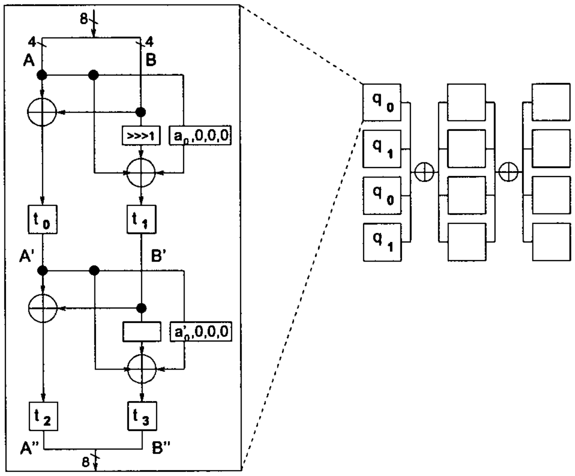

Figure 5: Architecture of Sbox.

3.1. F Function and Loop-Folding Technique

Typically, like many other block encryption algorithms, the Twofish block cipher is a 16-round Feistel-like network. It is not cost effective to map directly the 16-round encryption operation into hardware. Thus we fold the 16-round loop operations into one-round operation, as shown in Figure 4. The one-round operation is performed by a F-function Unit. For realization of the total algorithm the data are applied in a repeated manner to the F-function Unit by means of a feedback register and a multiplexer. Since there are some the same operations in F-function Unit, the parallel processing method can be applied to reduce the hardware cost.

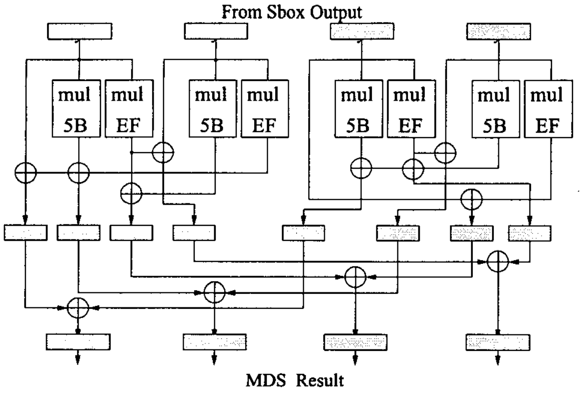

Figure 6: Architecture of MDS

3.2. S-box

The operation of the S-box in Twofish encryption algorithm is quite complicated. It needs three lookup tables. Each lookup table labeled q_0 or q_1, the q-box architecture is shown in the left of Figure 5. In this figure, the boxes labeled t_0, t_1, t_2 and t_3 are the real 4x4 tables. The q_0 and q_1 can be regarded as 8x8 lookup tables. Since RAM is not cost-effective, we use combinational logic circuits to implement the S-boxes instead.

3.3. MDS Matrix

The architecture of MDS matrix operations is shown in Figure 6. The four outputs from sbox are multiplied by a fixed matrix. There are only three different values, 01, 5B and EF, in the matrix. However, the operation here is not the general arithmetic multiplication, it uses the polynomial multiplication here, as follows.

$$\begin{pmatrix} z_0 \\ z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5b \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{pmatrix}$$

For example, the result z_0 should be $y_0 * 01 \oplus y_1 * EF \oplus y_2 * 5B \oplus y_3 * EF$. In the Figure 6, the most left register in first stage is the result of $y_0 * 01 \oplus y_1 * EF$, and the fifth register is $y_2 * 5B \oplus y_3 * 5B$. These two registers perform XOR operation in the next stage. Then, the result is put in the z_0 register. Similarly, we use the same method to get the z_1, z_2, and z_3.

3.4. PHT

The module of PHT is quite simple. Its architecture is shown in Figure 7. We only use two 32-bit adders to implement it.

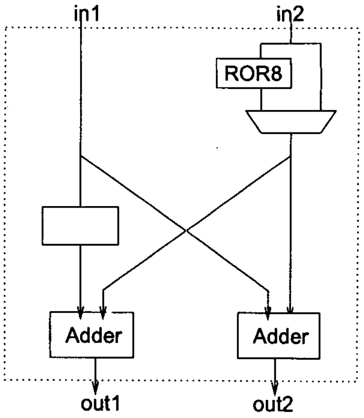

Figure 7: Architecture of PHT

The adders perform the addition of modulo 2^{32}. We implement the fast adders, carry-lookahead adders, to perform the operations.

Because of the use of subkey generation, the 8-bit hard-wired right rotation is implemented in the input. There are two paths for the input 2. While performing encryption, PHT will select the non-rotation input. Otherwise, while performing key scheduling operation, the rotated input will be selected.

4. VLSI IMPLEMENTATION AND PERFORMANCE ANALYSIS

To verify our VLSI assumption used to derive the performance of the architecture, a prototype VLSI chip was designed using 0.35 μm CMOS technology from TSMC. The chip area is 2.75 × 2.75 mm^2. The throughput rate of encryption is 200 Mbit/s operating at 66 MHz clock. The technical data and layout of the chip are shown in Table 1 and Figure 8, respectively.

We have completed the design by using CAD tools of SYNOPSYS and CADENCE. The comparison of our proposed architecture with the other architectures for the Twofish encryption algorithm is presented in Table 2. The result shows our proposed architecture achieves the highest throughput per gate. In addition, it also is cost-effective in hardware area.

5. CONCLUSION

A high-speed VLSI block encryption chip based on the Twofish block cipher has been presented. It can run at 66 Mhz with 200 Mbps throughput. While operating in 3.3V power, its power dissipation is 44 mW. The equivalent gate count is 35000 using TSMC 0.35 1p4m technology. The area is $2.75 * 2.75mm^2$. Since it integrates loop-folding technique

Table 2: Comparison of the twofish architectures

Method	Designer	Device (Technology)	Gate Count	Throughput	Throughput per Gate
Hardware Evaluation	NSA	0.5um	945993	2.27Gbps	2403.32
Hardware Evaluation	Mitsubishi	.35um	431857	394.08Mbps	912.52
FPGA	Kris Gaj	Xilinix XC4028XL	24800	90.9Mbps	3665
FPGA		Xilinix XVC1000	857560	1.59Gbps	1854.1
FPGA	Viktor Fischer	Altera FLEX10K	41093.75	80.3Mbps	1954
ASIC	Our Design	.35um	35000	200Mbps	5714.28

Table 1: Technical Data

Technology	tsmc .35um 1p4m
Gate count	35000
Chip area	$2.75 * 2.75\, mm^2$
Clock rate	66 Mhz
Throughput	200 Mbits/sec
Power dissipation	44 mW

and efficient hardware design in the ordinary and high-speed adapted versions. Thus it makes data encryption/decryption more efficient and secure. It is suitable for high-speed networking protocols like ATM or FDDI.

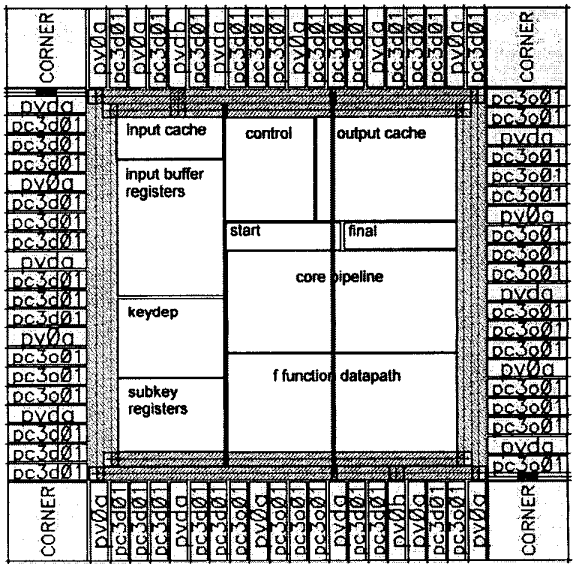

Figure 8: Chip layout

6. REFERENCES

[1] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson *Twofish: A 128-Bit Block Cipher*. Counterpane Internet Security, Inc, 1998

[2] Elbirt, A.J.; Yip, W.; Chetwynd, B.; Paar, C, " An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists ", *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 9, pp.545-557, Aug. 2001.

[3] S. Wolter, H. Matz, A. Schubert, and R. Laur, " On the VLSI Implementation of the International Data Encryption Algorithm IDEA", *Circuit and Systems, ISCAS'95 1995., IEEE International Symposium*, vol. 1, pp.397-400, 1995.

[4] Pawel Chodowiec, Kris Gaj (July 1999) *Implementation of the Twofish Cipher Using FPGA Devices*. Technical Report, Electrical and Computer Engineering, George Mason University

[5] H. Feistel, W.A. Notz and J.L. Smith, *Some Cryptography Techniques for Machine-to-Machine Data Commnuications*. Proceedings on the IEEE, v.63, n. 11, 1975, pp.1545-1554.

[6] Viktor Fischer, *Realization of the Round 2 AES Candidates Using Altera FPGA*. Techinical Report, MICRONIC s. r. o.