16-bit RISC Cryptographic Processor Architecture for Security Operations on Virtex5 FPGA

Mahaba saad aziz, Shoubra Faculty of Engineering, Benha University
Khalid Youssef, Institute of Aviation Engineering & Technology, Aviation Academy
Hala Abdel-Kader, Shoubra Faculty of Engineering, Benha University
Mohamed Tarek, Shoubra Faculty of Engineering, Benha University
Abstract— Security is one of the most important features in data communication due to the rapid evolution of communication systems offers and to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Cryptographic algorithms are mainly used for this purpose to obtain confidentiality and integrity of data in communication. This paper provides a dynamic crypto processor used for some symmetric key cryptographic ciphers (DES, 3DES, AES, Blowfish, RC5, and RC6). Also, provides an implementation of 16bit cryptographic processor that performs logical operations and arithmetic operations like rotate shift left, modular addition $2^\text{16}$, $S$ _box operation, and key expansion operation on virtex5, xc5vlx50 FPGA. Simulation results show that developed processor working with high Speed, low power, and low delay time.

Index Terms— Cryptographic Processor, DES, 3DES, AES, Blowfish, RC5, RC6, Data Encryption, FPGA.

I. INTRODUCTION

Cryptography is one of the most critical and necessary element of every network infrastructure and communication. It is an important research topic due to the explosive growth in data communications and Internet services. It can be divided into two families: Asymmetric key cryptography: the data is encrypted with the public key and decrypted with private key. Symmetric key cryptography: encrypt and decrypt data by using a single key. These are based on a mathematical function to encrypt a plain-text message and to produce cipher message. XOR ($\oplus$) operator and rotate shift left are the most importantly used for all cryptographic algorithms, which there are basic operation. Addition modulo $2^{32}$ (mod $2^{32}$) and multiplication Modulo $2^{32}$ operations are also used for some cryptographic algorithms. Data Encryption Standard (DES), 3DES, Advanced Encryption Standard (AES), Blowfish, RC5, and RC6 are the selected algorithm used for this study

II. CRYPTOGRAPHIC ALGORITHMS FOR SYMMETRIC BLOCK CIPHERS

DES [1, 2] is the oldest data encryption standard. It operates on blocks of 64-bits in size for plaintext and key. The key actually looks like a 64 bit quantity, but one bit in each of the 8 octets is used for odd parity on each octet. There are 256 possible keys that must be tried to encrypt or decrypt the data block. 56-bit key is used in DES and 16 round of each 48-bit sub keys are formed by permuting 56-bit key. Plain text block size of 64-bit is made from L and R blocks of 32-bit. The advantages of DES: any a change of one input or key bit results in changing more than half output bits. Also, each bit of cipher text depends upon multiple bits of plaintext and key. DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; DES keys have been broken in less than 24 hours by Brute force attack in which it consists of systematically checking all possible keys until the correct key is found. There are also some analytical results which demonstrate theoretical weaknesses in the cipher.

3DES [2] is designed to increase the encryption level. 3DES runs three times slower than DES. It also has low performance, 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data. It is quite slow for hardware and software implementations. But it is easy to implement, secure and very efficient in hardware. It takes three 64-bit keys, for an overall key length of 192 bits (3*64 bit) that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES. The procedure and operations are exactly the same as regular DES, but it is repeated three times.

AES [2, 3] was designed after DES and 3DES, so AES is more secure than them due to the larger-size key. AES operates on a $4\times4$ matrix of bytes termed as a state. So the strength of AES showed by the combination of security, performance, efficiency, implementation ability, and flexibility. It allows the data length of 128, 192 and 256 bits,
http://www.ieejournal.com/
and supporting three different key lengths, 128, 192, and 256
bits. AES works with byte quantities so it must be converted
into bytes. AES is an iterated block cipher. This means that
the same operations are performed many times on a fixed
number of bytes. These operations are: ADD ROUND KEY,
BYTE SUB, SHIFT ROW, and MIX COLUMN.
Blowfish [5, 7] is a symmetric block cipher that encrypts
data in 64-bit blocks. The algorithm has two parts, key
expansion and data encryption. Eighteen 32-bit sub-keys, and
four arrays (the S-boxes), each of size 256 by 32 bits, from a
key of at most 448 bits (56 bytes). The data encryption uses a
16-round Feistel Network. The main operations used in
Blowfish are XOR and Addition modulo 2^32.
RC5 [8, 9] is a parameterized algorithm, designated as
RC5-w/r/b, where w: word size (in bits), r: number of rounds,
b: length of key (in bytes). The allowable value of w is 16, 32
and 64; the allowable values of r and b range from 0 to 255.
RC5 is a highly efficient and flexible cryptographic
algorithm, for which many parameters (key size, block size,
number of rounds) can be adjusted to tradeoff security
strength with power consumption and computational
overhead. The parameter of RC5-32/12/16 is commonly
chosen. There are three operations: words addition, XOR, and
data-dependent left rotation of x by y denoted by x <<< y.
RC6 [10] appears to be a useful cryptographic solution that
has taken the advantage of RC5 and the AES evaluations.
RC6 remains an ideal choice for many high-security and
high-performance applications. RC6 encryption, like RC5
parameterized algorithm RC6-w/r/b, (w= 32; (lg(w) = 5), r= 20,
and b= 16, 24, or 32 ). RC6 is based on seven operations
like addition modulo 2w, subtraction modulo 2w, XOR of
w-bit words, multiplication modulo 2w. Rotate the w-bit word
to the left or to the right, and Parallel assignment of values on
the right to registers on the left. The addition, subtraction, and
multiplication operations use two’s complement
representations.
III. LITERATURE REVIEW
We have surveyed a number of studies that make a design
of cryptographic processor. In [12] the authors implement 32
bit pipelined processor on FPGA using Verilog, to perform
logical and arithmetic operations like rotate word, modular
addition modular multiplication, matrix multiplication, fixed
coefficient multiplier ,mix column transform using binary
extension field operations (2^m) for arbitrary irreducible
Polynomial. Simulation results showed that increase overall
performance of the speed with low area and low propagation
delay. It was concluded in [13] that 32-bit RICS processor
introduces modular addition, Polynomial matrix
multiplication, Reduction Modulo Multiplication, and Rotate
word to increase overall performance of the speed with low
area and low power consumption. In [14] describes the design
of high performance MIPS Cryptography processor based on
3DES. There are 3 new 32-bit instructions LK LW, LK UW
and CRYPT in order to increase the processor functionality
and performance. In [15] the authors design to perform
addition, multiplication, shift operations, matrix
multiplications, fixed coefficient multiplier, mix column
transformation, multiplier X (2X+1), and circular shift
operations for arbitrary irreducible polynomial. The main
objective of these works is to reduce the power consumption,
increase the speed of operation and reduce the programming
length.
IV. SECURITY ARCHITECTURE OF
CRYPTO-PROCESSOR
The architecture of processor is shown in Fig.1. 16-bit
processor has a complete instruction set, general purpose
registers, control unit, decoder, S box controller, and
Arithmetical Logic Unit (ALU). ALU design performs the
cryptographic operations like rotate shift left, modular
addition 2^16, S box operation for simplicity, and key
expansion operation. For cryptographic processor, it was
necessary to create dedicate instruction set. Table I describes
complete Instruction set. The instructions are classified in to
Data manipulation, arithmetic logical operations and
composite operation. Instruction Set Architecture (ISA) of a
CPU defines the set of operations that can be performed, and
on what data types. Each instruction will be 16 bits long,
divided as shown in table II for arithmetic operation and data
manipulation. This allows instruction decoder to be much simpler. The main blocks of our developed processor are

<table>
<thead>
<tr>
<th>Table I Instruction Set of the Developed Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>opcode</td>
</tr>
<tr>
<td>0</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>100</td>
</tr>
<tr>
<td>101</td>
</tr>
<tr>
<td>110</td>
</tr>
<tr>
<td>111</td>
</tr>
<tr>
<td>1000</td>
</tr>
<tr>
<td>1001</td>
</tr>
<tr>
<td>1010</td>
</tr>
<tr>
<td>1011</td>
</tr>
<tr>
<td>1100</td>
</tr>
<tr>
<td>1110</td>
</tr>
<tr>
<td>1111</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table II Instruction Set Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>opcode</td>
</tr>
<tr>
<td>-------</td>
</tr>
<tr>
<td>RIL</td>
</tr>
<tr>
<td>RRD</td>
</tr>
<tr>
<td>RWD</td>
</tr>
<tr>
<td>RWL</td>
</tr>
</tbody>
</table>

Mahabb et. al., 16-bit RISC Cryptographic Processor Architecture for Security Operations on Virtex5 FPGA
eight 16-bit general purpose registers, Decoder, Control unit, memory controller, pc unit, ALU with composite operations, Program Counter Unit.

A. General Purpose Registers (GPR’s)

GPR store and save operands and result during program execution so a set of eight 16-bit registers are used. Two registers are the operands to ALU which performs the operation. So, ALU and memories must be able to write/read those registers. Fig.2 represents RTL schematic of GPR.

B. Control Unit

This unit is responsible for telling other units what to do, and when. The control unit is technically a state machine, the main operations performed by it are reset, synchronize everything up and drive the enable bits, instruction fetch.

C. Decoder Unit

This unit used to statically pull bits out from the instruction stream and forward them on to the other units we connect to: The Register file, ALU, and Control unit.

D. Arithmetic Logic Unit (ALU)

ALU should take the opcode given by the decoder, along with input data read from the register file, and output a result that can then be written to the register file. It has 16 operations; each one of them was created and converted into a symbol. New operations are developed to perform composite operations like s_box operation, module addition, rotate left shift and key expansion. Fig.4 showed RTL schematic and fig.5 showed simulation result.

E. Program Counter Unit (PC)

PC is just a register (16 bit) containing the location of the currently executing instruction. PC unit will create to manage this. PC unit will obviously hold the current PC, and on command increment it. It will have an input for setting the
next PC value, the ability to stop – stay at the same location – which needed due to pipeline being several cycles long and also set PC to reset vector, which is 0x0000. So, a 2-bit select input can be used to select one of these operations. RTL schematic is showed in Fig.6.

III. SIMULATION RESULT OF NEW INSTRUCTIONS SET OF NOVEL ARCHITECTURE SIMULATION

16 bit processor was described using ISE 14.1 tool. This tool including the simulator, synthesizer and programming; after synthesized the hardware resource consumption for the complete processor implemented in a Xilinx virtex5, xc5vlx50-3ff324 FPGA is shown in table III. Simulation result of four new security composite operations is listed below.

<table>
<thead>
<tr>
<th>Table III Implementation Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Slice Logic Utilization</strong></td>
</tr>
<tr>
<td>Number of Slice Registers</td>
</tr>
<tr>
<td>Number used as Flip Flops</td>
</tr>
<tr>
<td>Number of Slice LUTs</td>
</tr>
<tr>
<td>Number used as logic</td>
</tr>
<tr>
<td>Number used as Memory</td>
</tr>
<tr>
<td>Number of occupied Slices</td>
</tr>
<tr>
<td>Number with an unused Flip Flop</td>
</tr>
<tr>
<td>Number with an unused LUT</td>
</tr>
<tr>
<td>Number of fully used LUT-FF pairs</td>
</tr>
<tr>
<td>Number of slice register sites lost to control set restrictions</td>
</tr>
<tr>
<td>Number of bonded IOBs</td>
</tr>
<tr>
<td>Number of BUFG/BUFGCTRLs</td>
</tr>
<tr>
<td>Number of DSP48Es</td>
</tr>
<tr>
<td>Average Fanout of Non-Clock Nets</td>
</tr>
</tbody>
</table>

A. Module Addition 2^16 Operation

Module addition 2^32 is used in blowfish, RC5, and RC5 algorithms. The novelty is in breaking the original 32-bit input plain text into 16-bit data set and performs module addition 2^16. Fig.7 represents simulation result. A simple description of mod 2^16 addition in terms of integer addition:

$$x + y \mod 2^{16} = \begin{cases} x + y & \text{if there was no a carry out} \\ x + y - 2^{16} & \text{if there was a carry out} \end{cases}$$

B. S_box Composite Operation

S-box operation provides an extra layer of security. It is usually the most important task while designing DES algorithm. S-box is a lookup table, using six bits as input and four bits as output. The 6 input bits are split into two groups.
D. Key Expansion Composite Operation

Input key is expanded to generate sub keys before data encryption in all selected algorithms. This part is used as a separated unit in the algorithm steps, so the novelty is used this as an opcode executed by ALU. Fig.10 represents simulation result.

VI. POWER ANALYSIS

Power estimate of the FPGA implementation is given by the sum of static power and dynamic power. The static power represents the additional power consumption when the device is configured but there is no switching activity. Static power depends on the specific FPGA family. The dynamic power is the sum of logic power, input & output power, signal power and clock power, i.e. power consumption from the user logic utilization and switching activity. XPower analyzer is used to calculate total power consumption. Table VI represents these values for crypto processor design.

| Static power | 0.529 W |
| Dynamic power | 0.006 W |
| Total power | 0.535 W |

VII. CONCLUSION

This paper proposes architecture for 16bit RISC network processor based on new instruction set architecture for next generation network processors as a dynamic processor than can be perform the following algorithms: DES, 3DES, AES, Blowfish, RC5 and RC6. Thus 16bit cryptographic processor performs these security operations used in selected symmetric key algorithms, has been designed using VHDL. This 16-bit processor introduces the cryptographic instructions like Modular addition, S_box operation, Key expansion operation, and Rotate left shift. These operations are used as separated unit in the algorithm steps to increase overall performance and speed with low area and low power consumption by reducing the number of instruction cycles of executing the algorithm.

REFERENCES

Mahaba et. al., 16-bit RISC Cryptographic Processor Architecture for Security Operations on Virtex5 FPGA


