Project 2 Specification

Optimization of Arithmetic Operations in SHA-1

April 11, 2002

Roar Lien

1. Abstract

The purpose of this project is to design an optimized hardware implementation of the arithmetic operations in SHA-1 hash function with respect to throughput and latency. Two implementations of SHA-1 will be implemented for this purpose. A basic architecture with number of rounds *#rounds* as specified in the SHA-1 algorithm. In the second architecture, partial loop unrolling will be used. If the number of unrolled loops is given by *K*, assuming that K is a divisor of *#rounds*, the only difference of the modified architecture to the basic architecture is that the combinational part of this architecture implements K rounds, instead of a single round.

The number of clock cycles to compute the message digest, will in the modified architecture decrease by a factor of *K*. At the same time minimum clock frequency increases by a factor slightly smaller than *K*. Leading to a small overall increase in the maximum throughput of the circuit

The implementation target for the design is SLAAC1-V FPGA accelerator board, based on Xilinx Virtex 1000 devices. The arithmetic operations of SHA-1, as well as the physical properties of the target device will be taken into account when designing an optimal architecture.

2. Functional Requirements of Hardware Operations

The SHA-1 algorithm takes as input a message with maximum length of less than 2^{64} bits and produces as output a 160-bit message digest. The function of interest in this project is the compression function in and is of the form:

$$A, B, C, D, E \leftarrow (E + f(_t, B, C, D) + S^5(A) + W_t + W_t), A, S^{30}(B), C, D \qquad (1)$$

The basic iterative architecture is given in figure 2.1. The second architecture with 5 unrolled loops is given in figure 2.2.

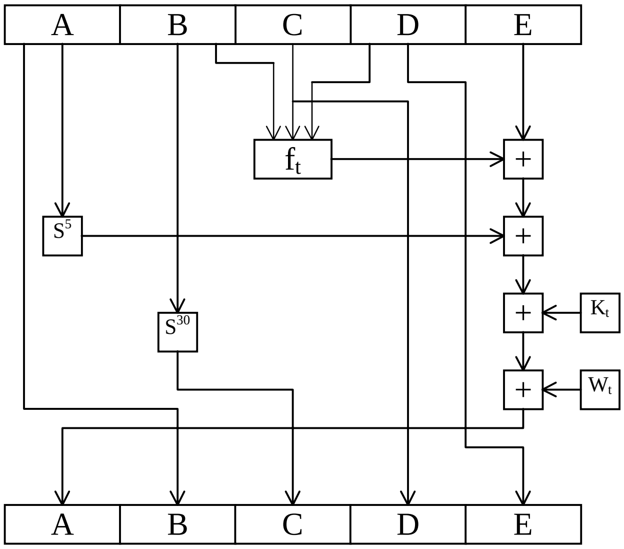

Figure 2.1

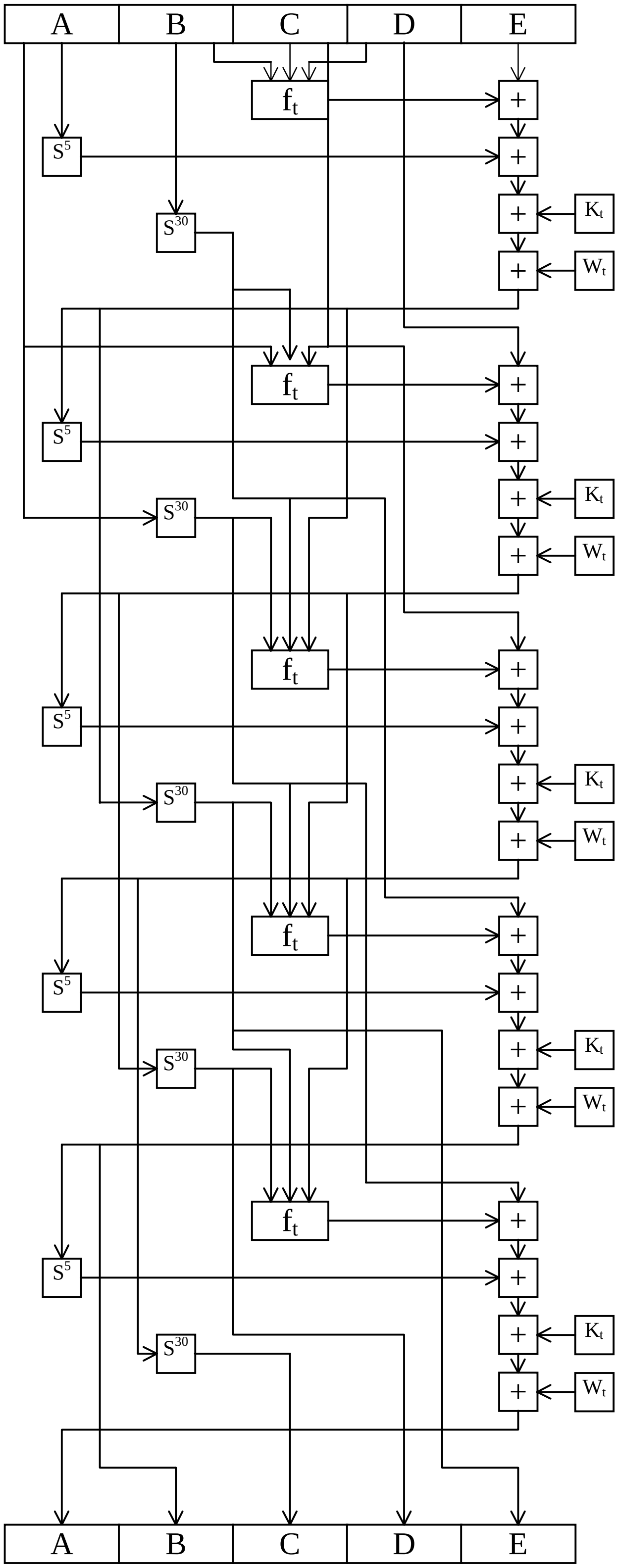

Figure 2.1

Where

A, B, C, D, E = five words of the buffer that is initialized with in IV

t = step number

f($_t$, B, C, D) = primitive logic function for step t

S^k = circular left shift of the 32-bit argumen by k bits

W_t = a 32-bit word derived from the current 512-bit input block

K_t = an additive constant

+ = addition modulo 2^{32}

For the basic architecture the compression function of figure 2.1 is processed 80 times. Unrolling the loops *K* times will thus produce the same function processed 80/*K* times. Thus with 5 unrolled loops, the compression function of figure 2.2 is processed 16 times.

The constant K_t and function f_t selected according to step number t for the basic architecture, and the partially unrolled architecture is shown in table 2.1, and table 2.2 respectively

0<=t<=19	K_t=5A827999	f_1=f (t,B,C,D) = (B AND C) OR (NOT B AND D)
20<=t<=39	K_t=6ED9EBA1	f_2=f (t,B,C,D) = B XOR C XOR D
40<=t<=59	K_t=8F1BBCDC	f_3=f (t,B,C,D) = (B AND C) OR (B AND D) OR
60<=t<=79	K_t=CA62C1D6	f_4=f (t,B,C,D) = B XOR C XOR D

Table 2.1

0<=t<=3	K_t=5A827999	f_1=f (t,B,C,D) = (B AND C) OR (NOT B AND D)
4<=t<=7	K_t=6ED9EBA1	f_2=f (t,B,C,D) = B XOR C XOR D
8<=t<=11	K_t=8F1BBCDC	f_3=f (t,B,C,D) = (B AND C) OR (B AND D) OR
12<=t<=15	K_t=CA62C1D6	f_4=f (t,B,C,D) = B XOR C XOR D

Table 2.2

3. Application

Authentication is required part of any secure packet switched computer network.
The goal of this design is to implement SHA-1 compliant with 1 Gigabit IPSEC.

4. Optimization Criteria

The main goal for this project is to design a hardware implementation of the SHA-1 compression function with minimum latency, and maximum throughput for a basic iterative architecture, and as well for an extended architecture with partially unrolled loops.

5. CAD Tools

The design entry method is VHDL. Active HDL 5.1. For synthesis Xilinx ISE 4 with FPGA Express will be used for design specification and implementation. For experimentally testing the design we will be using SLAAC1-V FPGA accelerator boards, based on Xilinx Virtex 1000 devices.

6. Test plan

The implementation will be experimentally tested using SLAAC-1V FPGA accelerator boards based on Xilinx Virtex 1000 devices. The testing procedure will consist of three phases. The first phase is aimed at verifying the circuit functionality as a single clock frequency. The goal of the second phase is to determine the maximum clock frequency at which the circuit operates correctly. In the third phase the goals is to determine the limit of the maximum throughput of the circuit, taking into account the limitations of the PCI interface SLAAC-1V FPGA accelerator board.

Various size files will be used to find maximum clock frequency that can be applied to the circuit, as well as the throughput its maximum throughput.

7. References

i. W.Stallings, Cryptography and Network Security, 1999 Prentice-Hall, Inc. Upper Saddle River, New Jersey 07458. 2nd Edition. ISBN 0-13-869017-0.

ii. http://www.itl.nist.gov/fipspubs/fip180-1.htm.

iii. Mihir Bellare, Ran Canetti, Hugo Krawczyk, “Keying Hash Functions for Message Authentication”, Crypto 96 proceedings.

iv. C. P. Pfleeger, Security in Computing, 1997 Prentice-Hall, Inc. Upper Saddle River, New Jersey 07458. 2nd Edition. ISBN 0-13-337486-6

Note that the above list is not exhaustive and more will be added as required.