Implementations for Dynamic SHA2

Zijie Xu
E-mail: xuzijiewz@gmail.com

Abstract. This paper specifies the implementations of Dynamic SHA2 algorithms.

Key words: SHA, Dynamic SHA2

1 Introduction

This paper specifies the implementations of Dynamic SHA2 algorithms. The implementations include ANSI C implementation and hardware implementation.

2. Implementation

2.1 Platforms

Dynamic SHA2 has been implemented at follow platform :

1. Intel 80/87c58.
2. Wintel personal computer, with an Intel Core 2 Duo Processor, 2.4GHz clock speed, 2GB RAM, running Windows Vista Ultimate 32-bit (x86) Edition.
3. Wintel personal computer, with an Intel Core 2 Duo Processor, 2.4GHz clock speed, 2GB RAM, running Windows Vista Ultimate 64-bit (x64) Edition.

This ANSI C code file and implementation result is in CD.

2.2 Estimation

2.2.1 8-bit processor

Dynamic SHA2 has been implemented at the simulation “Keil uVision” , the processor is Intel 80/87c58. The parameter of Intel 80/87c58 is:

MCS-51 CHMOS single-chip 8-bit microcontroller with 32 I/O lines, 3 Timers/Counters, 6 Interrupts/4 priority levels, 32K Bytes On-Chip

ROM/EPROM, 256 Bytes on-chip RAM, Programmable Serial Channel with Frame Error Detection, 24 MHz crystal oscillation.

2.2.2 Reference Implementation

The result of reference implementation as table 2.1show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	1.38×10^{-2}	6.89×10^{-1}	7.15×10^{-1}	1.59	1.29×10	1.27×10^{2}
Dynamic SHA2-256	1.38×10^{-2}	6.90×10^{-1}	7.16×10^{-1}	1.59	1.29×10	1.27×10^{2}
Dynamic SHA2-384	2.66×10^{-2}	1.13	1.19	1.88	1.62×10	1.59×10^{2}
Dynamic SHA2-512	2.66×10^{-2}	1.14	1.20	1.88	1.62×10	1.59×10^{2}

Table 2.1 The seconds of reference implementation of Dynamic SHA2 on Intel 80/87c58

The Program Size is as table 2.2 show:

	Data (bytes)	Xdata (bytes)	Code (bytes)	Total (bytes)
Dynamic SHA2-224	34	10595	9352	10445
Dynamic SHA2-256	34	10595	6478	10445
Dynamic SHA2-384	61	11063	12201	23325
Dynamic SHA2-512	61	11063	12201	23325

Table 2.2 The Program Size of reference implementation of Dynamic SHA2 on Intel 80/87c58

2.2.3 Optimized Implementation

The result of optimized implementation as table 2.3show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	1.38×10^{-2}	6.17×10^{-1}	6.42×10^{-1}	1.45	1.18×10	1.15×10^{2}
Dynamic SHA2-256	1.38×10^{-2}	6.18×10^{-1}	6.43×10^{-1}	1.48	1.18×10	1.15×10^{2}
Dynamic SHA2-384	2.66×10^{-2}	1.11	1.17	1.86	1.60×10	1.58×10^{2}
Dynamic SHA2-512	2.66×10^{-2}	1.11	1.17	1.86	1.60×10	1.58×10^{2}

Table 2.3 The seconds of optimized implementation of Dynamic SHA2 on Intel 80/87c58

The Program Size is as table 2.4 show:

	Data (bytes)	Xdata (bytes)	Code (bytes)	Total (bytes)
Dynamic SHA2-224	34	10593	38667	49294
Dynamic SHA2-256	34	10609	38667	49294
Dynamic SHA2-384	67	11051	51038	62156
Dynamic SHA2-512	67	11051	51038	62156

Table 2.4 The Program Size of optimized implementation of Dynamic SHA2 on Intel 80/87c58

From table 2.1, 2.2, 2.3 and 2.4. it is known that the program size of optimized implementation is about 4.72(resp. 2.66) times of the program size of reference implementation. And optimized implementation has a higher speed. The contrast as table 2.5 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	1	89.6%	89.8%	91.2%	91.5%	90.6%
Dynamic SHA2-256	1	89.6%	89.8%	93.1%	91.5%	90.6%
Dynamic SHA2-384	1	98.2%	98.3%	98.9%	98.8%	99.4%
Dynamic SHA2-512	1	97.4%	97.5%	98.9%	98.8%	99.4%

Table 2.5 The contrast of speed optimized implementation and reference implementation

In table 2.5, it is known that Dynamic SHA2-224/256 optimized implementation is speedyer about 10% than reference implementation. Dynamic SHA2-384/512 optimized implementation is speedyer about 1% than reference implementation.

2.3 Windows Vista Ultimate 32-bit (x86) Edition.

The platform of this implementation is :Wintel personal computer, with an Intel Core 2 Duo Processor, 2.4GHz clock speed, 2GB RAM, running Windows Vista Ultimate 32-bit (x86) Edition.

Compiler: The ANSI C compiler in the Microsoft Visual Studio 2005 Professional Edition.

2.3.1 Reference Implementation

The result of reference implementation as table 2.6 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	107	1695	1787	4143	31255	303293
Dynamic SHA2-256	100	1747	1826	4184	31283	303484
Dynamic SHA2-384	134	5254	5503	7793	70370	687734
Dynamic SHA2-512	131	5288	5523	7723	70856	687205

Table 2.6 The numbers of processor clock cycles on Windows Vista Ultimate 32-bit (x86) Edition

The memory requirement is as table 2.7 show:

	File size (bytes)	Message words (bytes)	work variables (bytes)	temporary words (bytes)
Dynamic SHA2-224	69632	64	32	4
Dynamic SHA2-256	69632	64	32	4
Dynamic SHA2-384	77824	128	64	8
Dynamic SHA2-512	77824	128	64	8

Table 2.7 The memory requirement of reference implementation of Dynamic SHA2 on Windows Vista Ultimate 32-bit (x86) Edition

2.3.2 Optimized Implementation

The result of optimized implementation as table 2.8 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	107	1103	1168	2764	22965	219526
Dynamic SHA2-256	100	1117	1232	2808	22991	219218
Dynamic SHA2-384	135	4897	5144	6973	70304	680287
Dynamic SHA2-512	130	4903	5113	6967	69583	673139

Table 2.8 The numbers of processor clock cycles on Windows Vista Ultimate 32-bit (x86)

The memory requirement is as table 2.9 show:

	File size (bytes)	Message words (bytes)	Work variables (bytes)	temporary words (bytes)
Dynamic SHA2-224	73728	64	32	4
Dynamic SHA2-256	73728	64	32	4
Dynamic SHA2-384	98304	128	64	8
Dynamic SHA2-512	98304	128	64	8

Table 2.9 The memory requirement of optimized implementation of Dynamic SHA2 on Windows Vista Ultimate 32-bit (x86) Edition

From table 2.6, 2.7, 2.8 and 2.9. it is known that the file size of optimized implementation is about 1.06(resp. 1.26) times of reference implementation. And optimized implementation has a higher speed. The contrast as table 2.10 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	1	65.1%	65.4%	66.7%	73.5%	72.4%
Dynamic SHA2-256	1	63.9%	67.5%	67.1%	73.5%	72.2%
Dynamic SHA2-384	1	93.2%	93.5%	89.5%	100%	98.9%
Dynamic SHA2-512	1	92.7%	92.6%	90.2%	98.2%	98.0%

Table 2.10 The contrast of speed optimized implementation and reference implementation

In table 2.10, it is known that Dynamic SHA2-224/256 optimized implementation is speedyer about 30% than reference implementation. Dynamic SHA2-384/512 optimized implementation is speedyer about 10%~0% than reference implementation.

2.4 Windows Vista Ultimate 64-bit (x64) Edition.

The platform of this implementation is :Wintel personal computer, with an Intel Core 2 Duo Processor, 2.4GHz clock speed, 2GB RAM, running Windows Vista Ultimate 64-bit (x64) Edition.

Compiler: The ANSI C compiler in the Microsoft Visual Studio 2005

Professional Edition.

2.4.1 Reference Implementation

The result of reference implementation as table 2.11 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	101	1705	1767	4192	31435	304294
Dynamic SHA2-256	100	1744	1827	4189	31394	303790
Dynamic SHA2-384	129	5277	5530	7849	71838	692942
Dynamic SHA2-512	130	5297	5515	7869	72234	687865

Table 2.11 The numbers of processor clock cycles on Windows Vista Ultimate 64-bit (x64) Edition

The memory requirement is as table 2.12 show:

	File size (bytes)	Message words (bytes)	work variables (bytes)	temporary words (bytes)
Dynamic SHA2-224	69632	64	32	4
Dynamic SHA2-256	69632	64	32	4
Dynamic SHA2-384	77824	128	64	8
Dynamic SHA2-512	77824	128	64	8

Table 2.12 The memory requirement of reference implementation of Dynamic SHA2 on Windows Vista Ultimate 64-bit (x64) Edition

2.4.2 Optimized Implementation

The result of optimized implementation as table 2.13 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	103	1105	1168	2757	23012	219415
Dynamic SHA2-256	100	1113	1225	2815	23019	219279
Dynamic SHA2-384	130	4850	5083	6822	69411	675494
Dynamic SHA2-512	130	4826	5022	6825	69458	671808

Table 2.13 The numbers of processor clock cycles on Windows Vista Ultimate 64-bit (x64) Edition

The memory requirement is as table 2.14 show:

	File size (bytes)	Message words (bytes)	work variables (bytes)	temporary words (bytes)
Dynamic SHA2-224	73728	64	32	4
Dynamic SHA2-256	73728	64	32	4
Dynamic SHA2-384	98304	128	64	8
Dynamic SHA2-512	98304	128	64	8

Table 2.14 The memory requirement of optimized implementation of Dynamic SHA2 on Windows Vista Ultimate 64-bit (x64) Edition

From table 2.6, 2.7, 2.8 and 2.9. it is known that the file size of optimized implementation is about 1.06(resp. 1.26) times of reference implementation. And optimized implementation has a higher speed. The contrast as table 2.15 show:

	Run time for set up	Bytes processed				
		1	10	100	1000	10000
Dynamic SHA2-224	1	64.8%	66.1%	65.8%	73.2%	72.1%
Dynamic SHA2-256	1	63.8%	67.0%	67.2%	73.3%	72.2%
Dynamic SHA2-384	1	91.9%	91.9%	86.9%	96.6%	97.5%
Dynamic SHA2-512	1	91.1%	91.1%	86.7%	96.2%	97.7%

Table 2.15 The contrast of speed optimized implementation and reference implementation

In table 2.15, it is known that Dynamic SHA2-224/256 optimized implementation is speedyer about 30% than reference implementation. Dynamic SHA2-384/512 optimized implementation is speedyer about 10%~3% than reference implementation.

3 Hardware Implementation

The top-level architecture for Dynamic SHA2 implementation is as Figure 1:

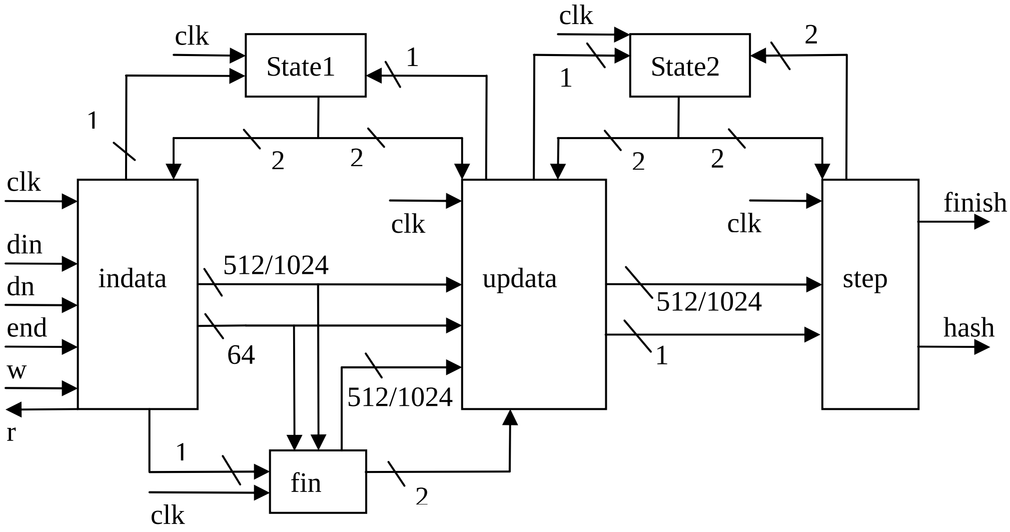

Figure 1: Atop-level block diagram of Dynamic-SHA2

Implementation results of Dynamic-SHA2 are presented in Table 2.1.

	SHA2-224/256	SHA2-384/512
Equivalent gate count	60,591	179,281
Slices	4,514	9,036

Table 2.1: Implementation results of Dynamic-SHA2

4. Conclusions

Form the implementation results of Dynamic-SHA2, it is known that the optimized implementation need more memory and are speedlyer than reference implementation at different platform.

And form the implementation results of Dynamic-SHA2, it is known that Dynamic-SHA2 can be used in low power, constrained memory environments, such as: 8-bit processors (e.g., smartcards), voice applications, satellite applications.