

Taehwan Park

Hwajeong Seo
Jongseok Choi
Ha Van Nguyen
Kyunghoon Kim
Sunhee Seok

Internet of Things

Big Data

FinTech

File System

Compression

Disk Encryption



Iron Park: I found that NSR developed the new hash function namely LSH. What is LSH?

JARVIS: LSH is abbreviation of (Lightweight Secure Hash).

Iron Park: Is there any unique features in it?

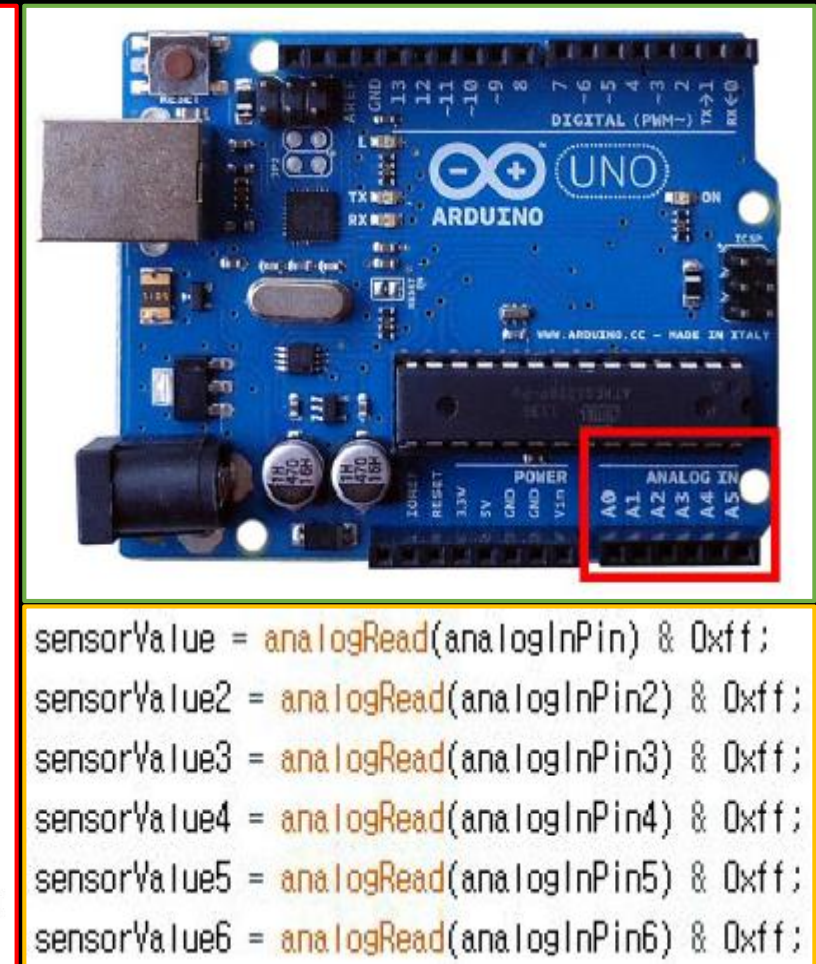
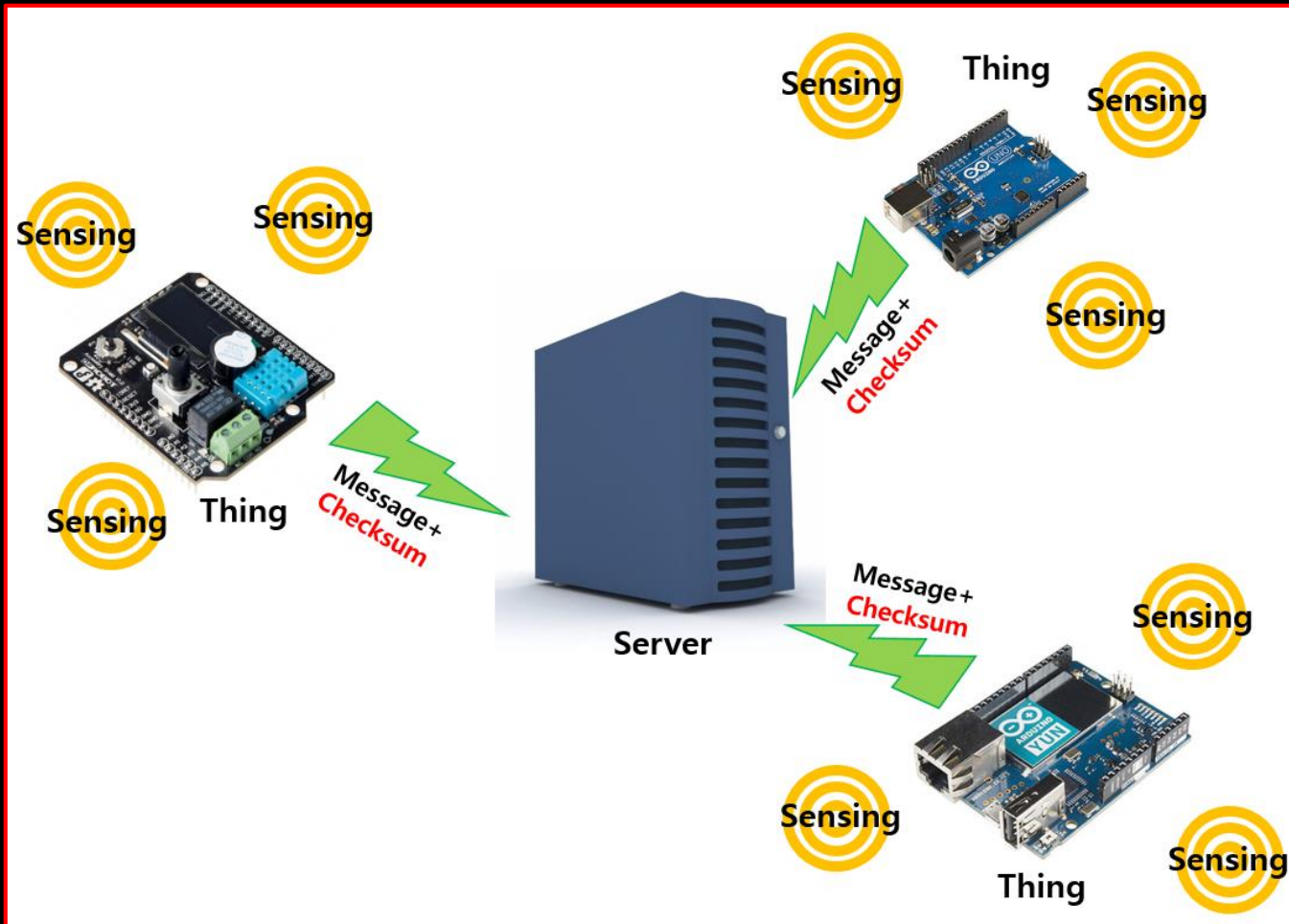
JARVIS: Absolutely yes. This has software and hardware friendly architecture. Furthermore, it is secure against all critical hash function attacks.

Iron Park: What an incredible results! I want to apply LSH into our avengers secure infrastructures.

JARVIS: I got your order.

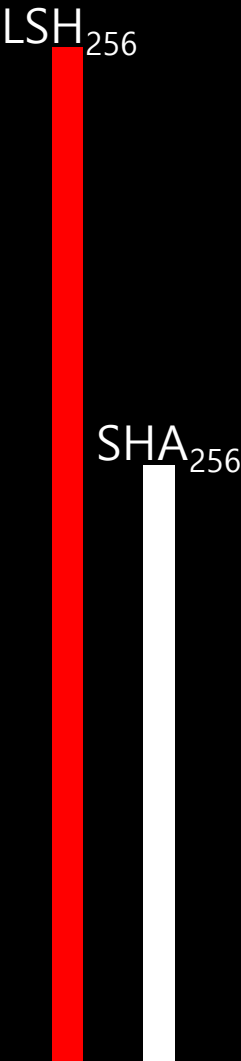
Internet of Things

:: Things sense the environment data and send to central server (checksum on message)



```
sensorValue = analogRead(analogInPin) & 0xff;
sensorValue2 = analogRead(analogInPin2) & 0xff;
sensorValue3 = analogRead(analogInPin3) & 0xff;
sensorValue4 = analogRead(analogInPin4) & 0xff;
sensorValue5 = analogRead(analogInPin5) & 0xff;
sensorValue6 = analogRead(analogInPin6) & 0xff;
```


Internet of Things (results)



CPU: Atmega328@20MHz, Bluno v1.8

OS: N/A

Language/Compiler: C(avr asm), Arduino 1.6.5

	LSH-256 our code	SHA-256 Tzikis Lib
Algorithm	145.2 Kbps	14.8 Kbps
S/W	13.7 Kbps X1.67	8.17 Kbps

Big Data

:: Large collections of data is continuously produced and stored into database (checksum on message)



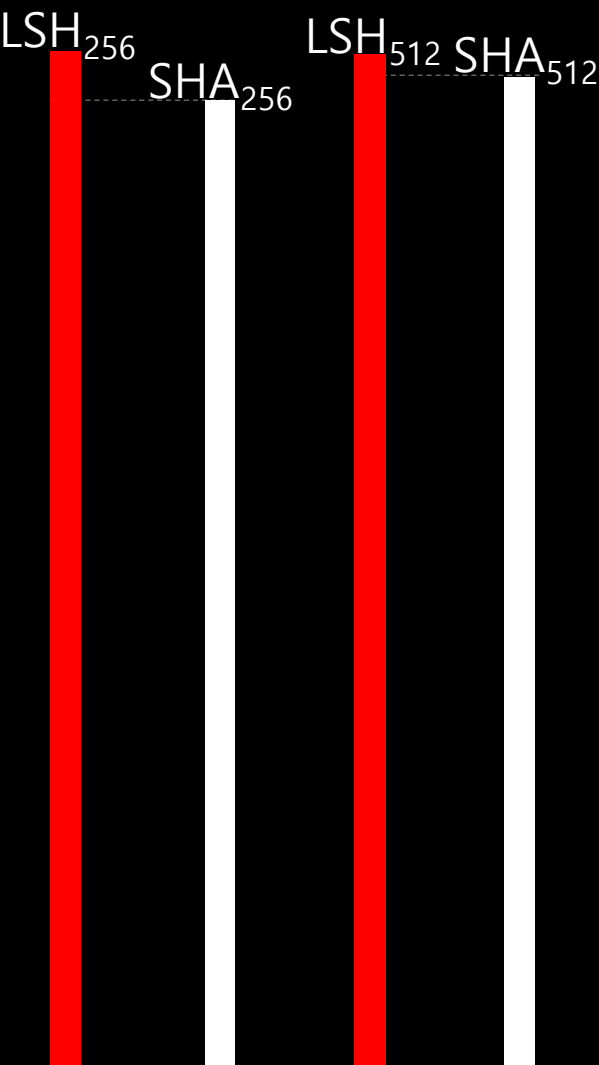
Field	Type	Null	Key	Default	Extra
id	int(11)	NO	PRI	NULL	auto_increment
text	varchar(4200)	NO		NULL	
hash	varchar(1000)	NO		NULL	

```
insert into hashtest values(NULL,DATA,SHA1(DATA))
insert into hashtest values(NULL,DATA,SHA2(DATA,256))
insert into hashtest values(NULL,DATA,SHA2(DATA,512))
```

```
Hash256(256, DATA, databilen, HASH)
insert into hashtest values(NULL,DATA,HASH)
```

```
Hash512(512, DATA, databilen, HASH)
insert into hashtest values(NULL,DATA,HASH)
```

Big Data (results)



CPU: Intel Core i5-4200U@1.60GHz 64-bit

OS: ubuntu 14.04 LTS 64-bit

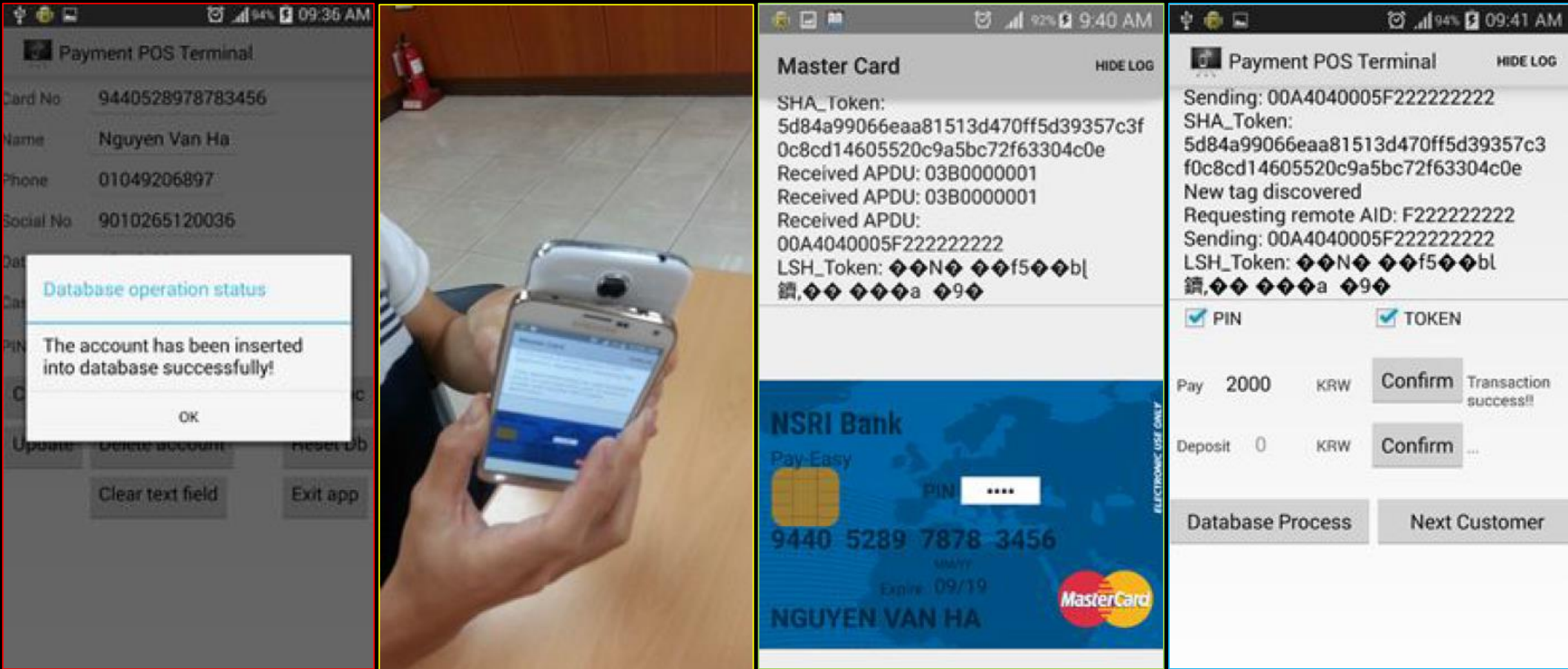
Language/Compiler: C(avx2 intrinsic) / gcc 4.8.2

Database: MySQL 14.14

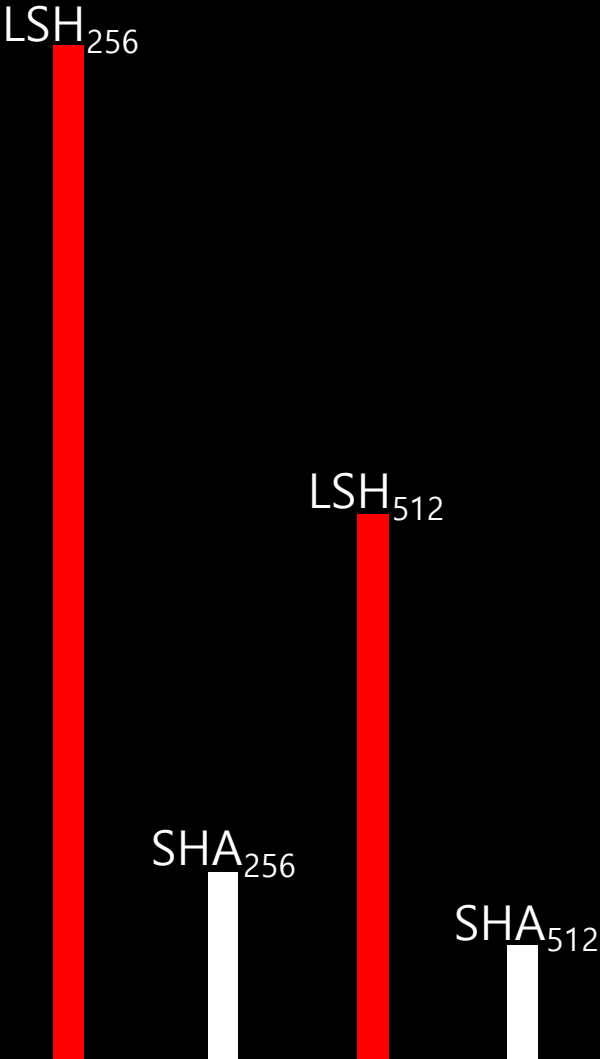
	LSH-256 NSR op.	SHA-256 mysql	LSH-512	SHA-512
Algorithm	355 Mbps	N/A	551 Mbps	N/A
S/W	26.3 Kbps X1.04	25.1 Kbps	26.1 Kbps X1.04	25.2 Kbps

FinTech

:: Technology provides financial services using software (one-time token)



FinTech (results)



CPU: Qualcomm Snapdragon801@2.5GHz 32-bit

OS: android 4.4.4 32-bit

Language/Compiler: C / gcc 4.9

	LSH-256 NSR ref.	SHA-256 Java Lib	LSH-512	SHA-512	
Algorithm	8B 42B 126B	4375 C/B 714 C/B 238 C/B	64375 C/B 13273 C/B 5019 C/B	10312 C/B 2023 C/B 674 C/B	86562 C/B 17023 C/B 5654 C/B
S/W	N/A	N/A	N/A	N/A	

File System

:: System is used to control how data is stored and retrieved (checksum on Inode)






```
C:\Temp> dir
Volume in drive C is C
Volume Serial Number is 74F5-B93C

Directory of C:\Temp

2009-08-25 11:59 <DIR>          .
2009-08-25 11:59 <DIR>          ..
2007-03-01 11:37          2,321,600 AdobeUpdater12345.exe
2009-04-03 10:01          27,988 dd_depcheckdotnetfx30.txt
2009-04-03 10:01           764 dd_dotnetfx3error.txt
2009-04-03 10:01         32,572 dd_dotnetfx3install.txt
2009-06-09 13:46         35,145 GenProfile.log
2009-08-05 12:11          155 KB969856.log
2009-04-20 08:37          402 MSI29e0b.LOG
2009-04-09 16:34        38,895 offcIn11.log
2009-04-03 16:02 <DIR>      OfficePatches
2009-07-14 14:30 <DIR>      OHotfix
2009-08-25 10:52         16,384 Perflib_Perfdata_c30.dat
2009-04-03 10:01          1,744 uxeventlog.txt
2009-08-25 11:42    50,245,632 Wfv2F.tmp
2009-04-20 10:07          1,397 {AC76BA86-7AD7-1033-7B44-A81200000003}.ini
2009-04-20 10:13          617 {AC76BA86-7AD7-1033-7B44-A81300000003}.ini
               13 File(s)      52,723,295 bytes
               4 Dir(s)  83,570,208,768 bytes free
```

```
encfs --reverse ~/enc ~/.enc
```

```
dd if=/dev/zero of=~/enc/10m bs=10M count=1
dd if=/dev/zero of=~/enc/20m bs=20M count=1
dd if=/dev/zero of=~/enc/50m bs=50M count=1
```

Name	Size	Type:	File Folder
 99998.txt	1 KB	Location:	C:\
 99999.txt	1 KB	Size:	488 KB (500,059 bytes)
 100000.txt	1 KB	Size on disk:	390 MB (409,608,192 bytes)
 mkfile.bat	1 KB	Contains:	100,002 Files, 0 Folders
 source.txt	1 KB		

File System (results)

LSH₂₅₆ SHA₁



CPU: Intel Core i7-4790@3.6GHz 64-bit

OS: Mac OS X 10.10.4 64-bit

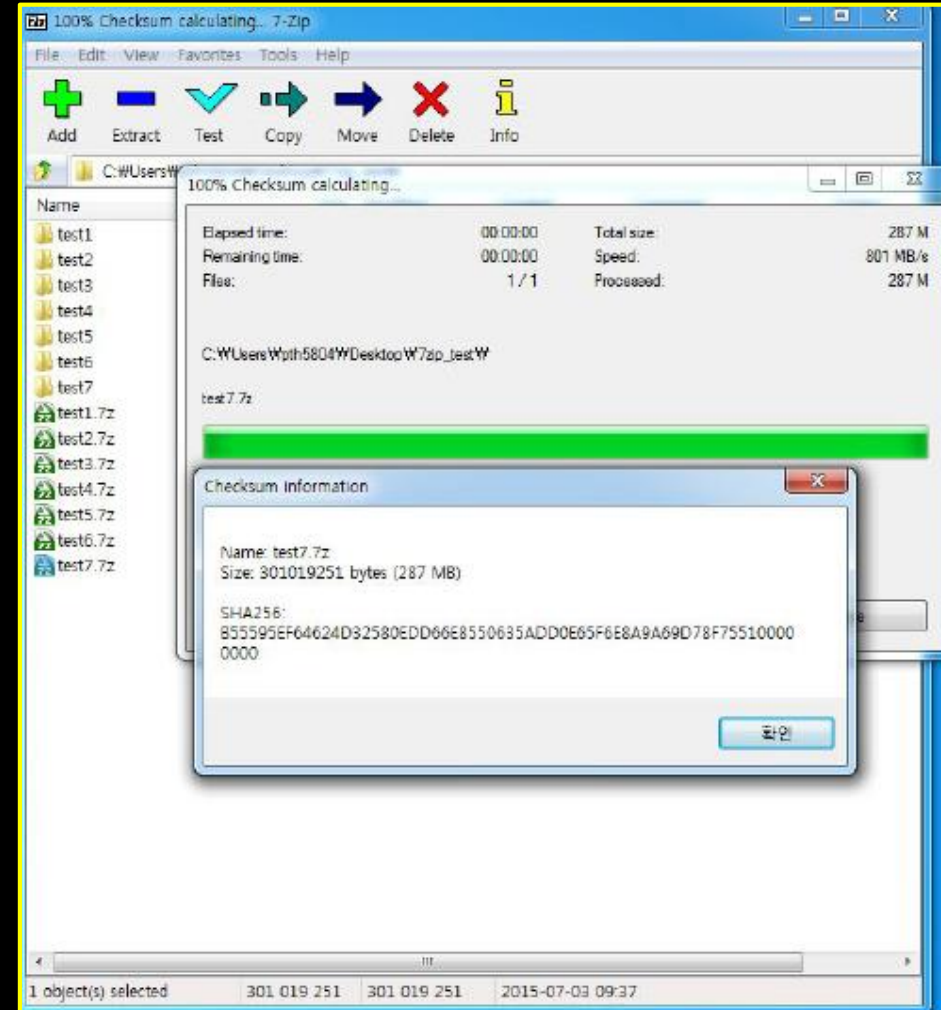
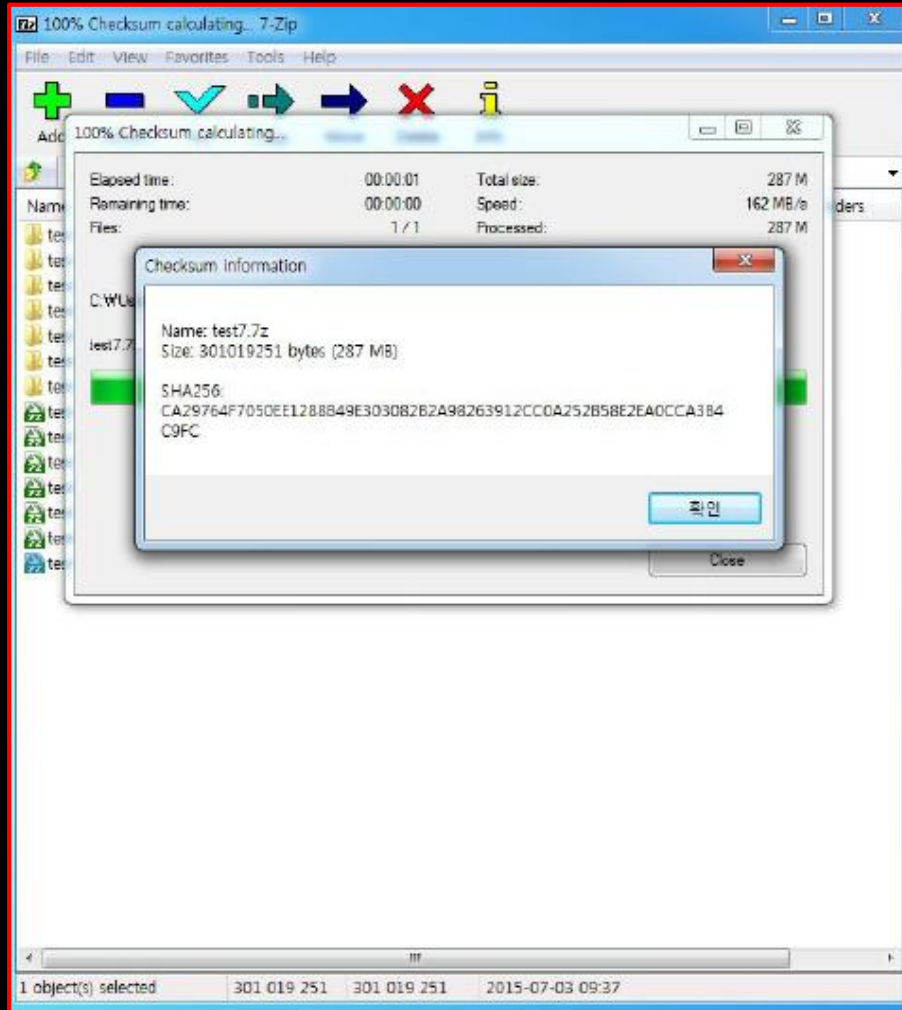
Language/Compiler: C(avx2 intrinsic) / gcc 5.1.1

File system: EncFS

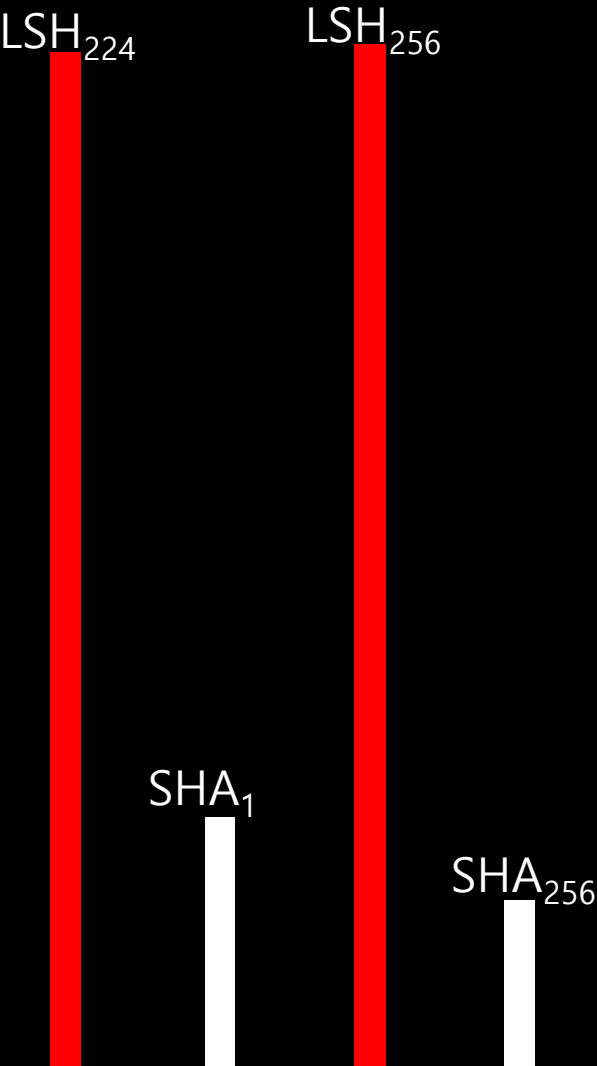
	LSH-256 NSR op.	SHA-1 openssl
Algorithm	130.3 Mbps	96.9 Mbps
S/W	50 Mbps	50 Mbps

Compression

:: Data compression involves encoding information using fewer bits (checksum on message)



Compression (results)



CPU: Intel Core i7-3770@3.40GHz 64-bit

OS: Windows 7 32-bit

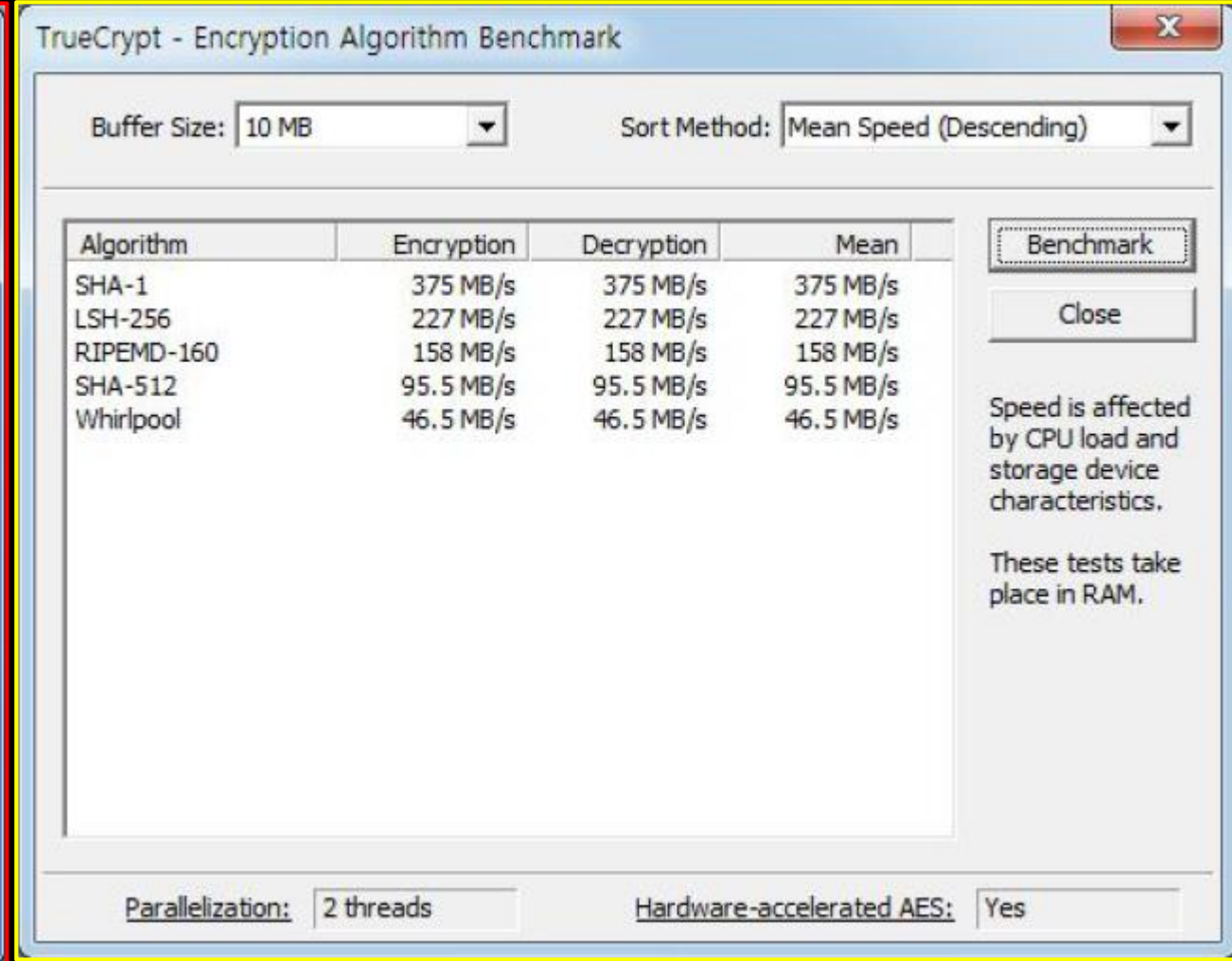
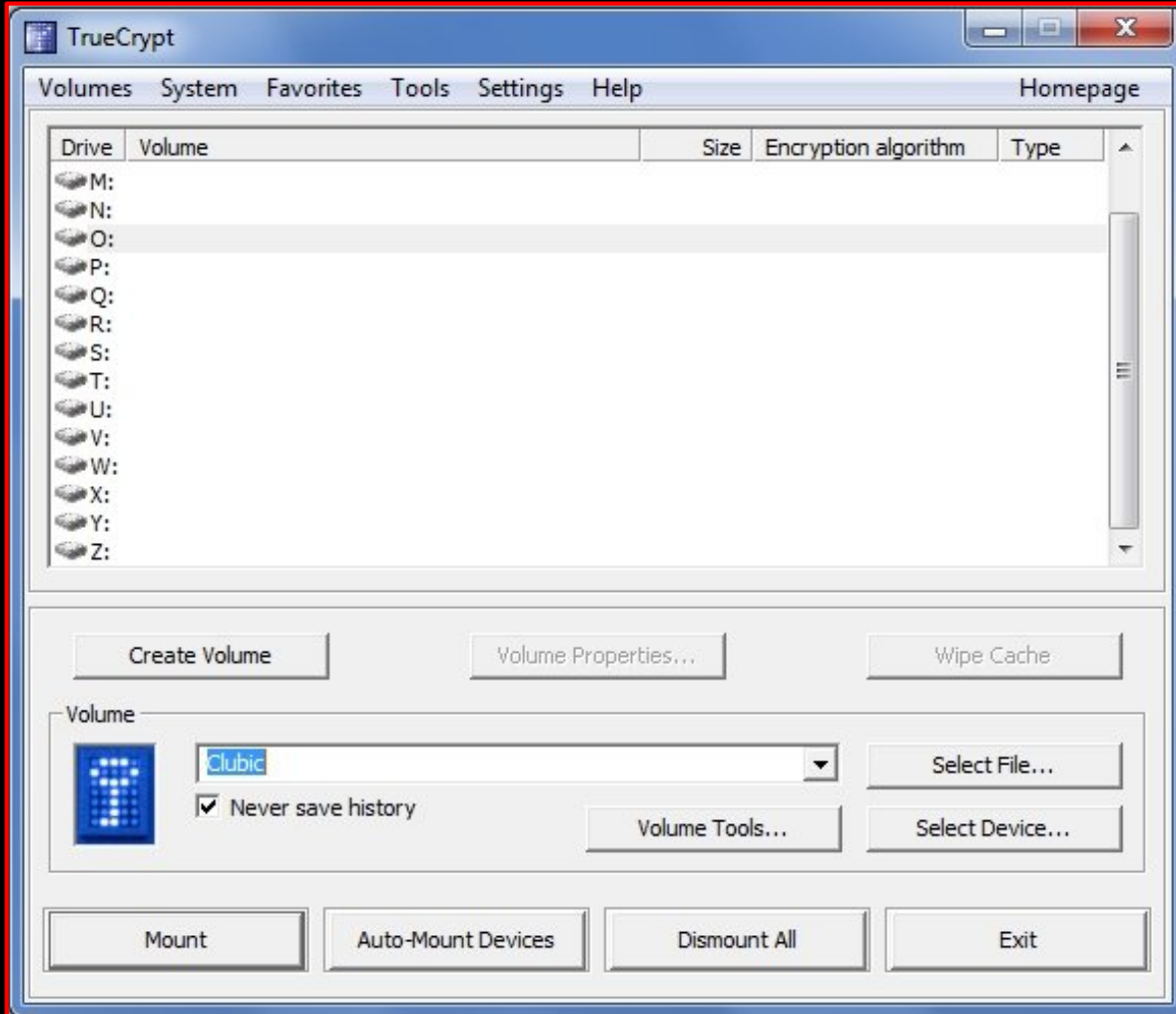
Language/Compiler: C / gcc 4.9

Compression S/W: 7zip 15.05 beta

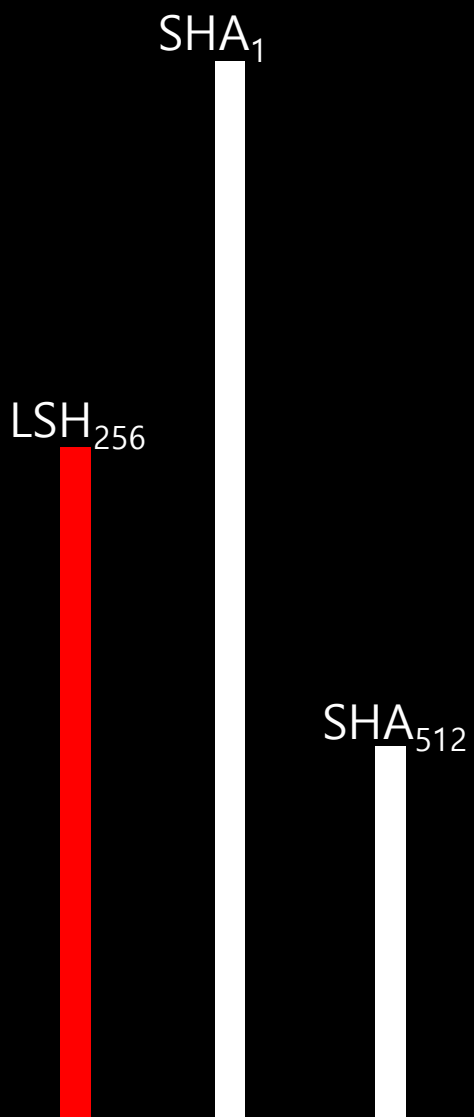
		LSH-224 NSR op.	SHA-1 7zip	LSH-256 NSR op.	SHA-256 7zip
Algorithm		N/A	N/A	N/A	N/A
S/W	4.6MB	237Mbps X4.85	145Mbps	206Mbps X4.87	94Mbps
	36.7MB		213Mbps		140Mbps
	294MB		272Mbps		155Mbps

Disk Encryption

:: This creates a virtual encrypted disk within a file or encrypt a partition (checksum on message)



Disk Encryption (results)



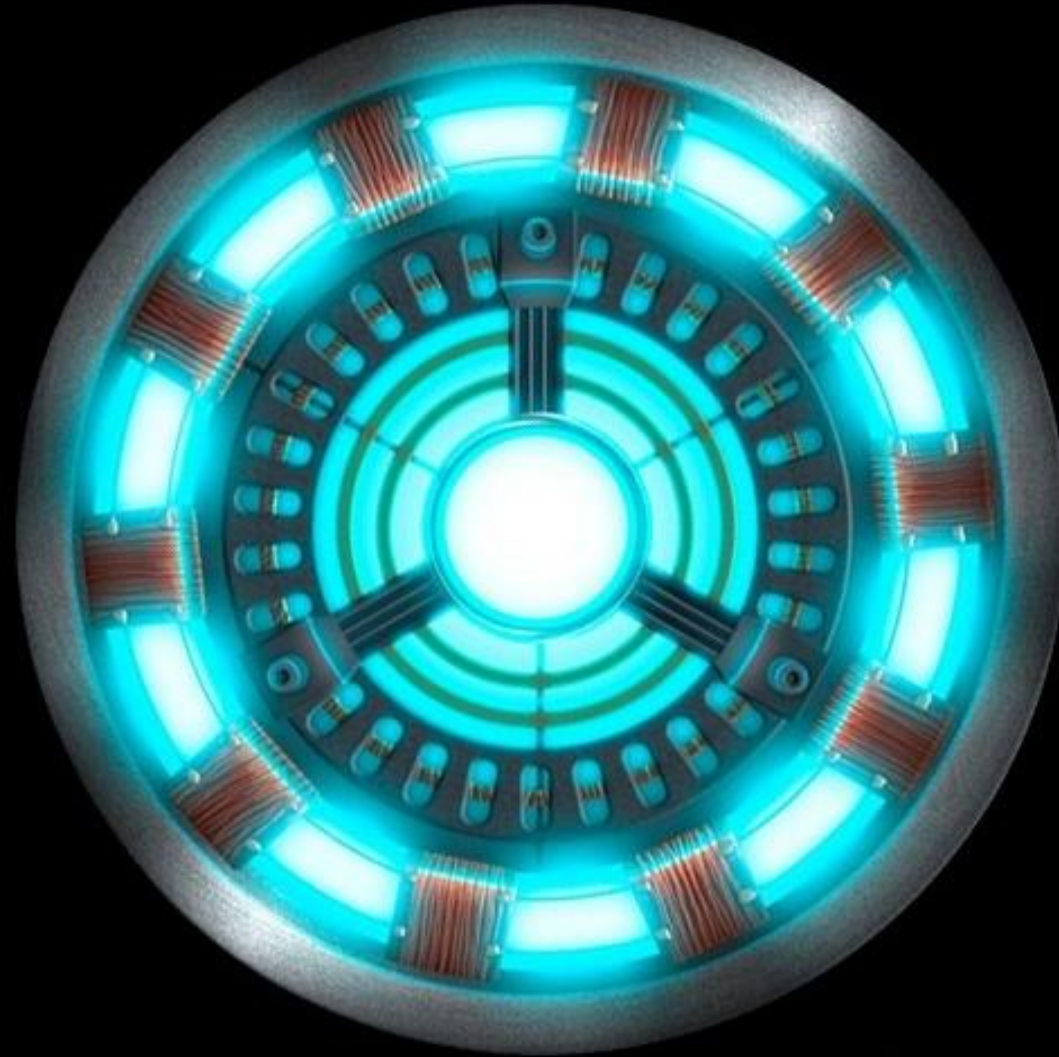
CPU: Intel Core i5-4670@3.40GHz 64-bit

OS: Windows 7 64-bit

Language/Compiler: C / Visual Studio 2008 SP1

Disk Encryption S/W: TrueCrypt 7.1a

		LSH-256 NSR ref.	SHA-1 TrueCrypt	SHA-512
Algorithm		N/A	N/A	N/A
S/W	100KB	210Mbps	350Mbps	75Mbps
	10MB	230Mbps	379Mbps	110Mbps
	100MB	226Mbps	371Mbps	96Mbps



Mission Completed