International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-6S, August 2019

Development of Algorithm to Enhance the Security Feature of SATA on Solid State Drives

Pooja Patil, Balaso Jagdale

ABSTRACT--- Now a day's quantity of data growing day by day accordingly the size of storage media is also increasing rapidly. In most of the storage devices flash memories are used one of them is Solid State drive. Solid state drives i.e. SSDs are non-volatile data storage devices which store determined data in NAND or NOR i.e. in flash memories, which provides similar functionality like traditional hard disk (HDD). This paper provides comparative study of Solid-state drives over Hard-disk drives. Also, implementation of algorithm to enhance the security of Solid-state drives in terms of user authentication, access control and media recovery from ATA security feature set. This algorithm fulfils security principles like Authentication and Data Integrity.

Keywords - Big Data, MapReduce, MRBIG, Top-k. Dominance

1. INTRODUCTION

Solid state storage devices are trading over the hard disk drives in many Enterprise and Client requests due to their improved performance, smaller formula factor, low power utilization and diversity of device interfaces. Solid state drive also called as electronic drive or usually known as SSD i.e. storage device which usage solid state memory to store persevering data in the same manner of providing access in the traditional hard disk drive. In hard disk drive data is stored on spinning metal platters and whenever we need some data a needle like component call head move over the data platters but in SSD there are no such mechanical arms. Basic structure of SSD is as shown in the figure 1.

As shown in Fig.1, NAND flash, DRAM and SSD controller together composes Solid-state drive. For easy replacement HDDs with SSDs in most applications, SSD and HDD have same host interfaces i.e. SATA, SAS etc. As the NAND flash memory must erases pervious data before writing operation unlike hard disk drives. Flash Translation Layer (FTL) is used to exchange data with the host in storage devices based on NAND flash memory to expose an array of logical sectors to the upper level host system while competing with hard disk drives. Its major functions include address translation from logical to physical, Wear Levelling as well as Garbage Collection [1].

From decade, because of flash memory chips on solid state drives shock resistance, high energy efficiency and high I/O performance aspects made SSD popular auxiliary to the Hard Disk drives. Each SSD should be able to keep track of the address translation information which is usually preserved or stored in the RAM space of the SSD. In hard disks which are made up of magnetic materials holds data in the form of zeros and ones so having the ability to write same data at every position. Afterwards when that data is been deleted stain would be erased but it will be still accessible on some sectors which are unused where these deleted files will be recoverable at any time.

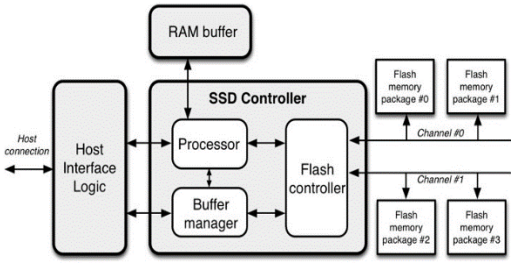


Fig 1. SSD Block Diagram

The TRIM i.e. removing space in storage performs a deletion of unacceptable data from the memory of SSD's to guarantee that performance of rewrite function is well often. For removing deleted data permanently in the background from sectors self- corrosion and garbage collection are the features of solid-state drive introduce All these done immediately or within few minutes of deletion of data. Depending on data generated it declares that superior use of TRIM commands and destroying of the proof issue in non-volatile memory origins tough in forensics investigation. The exclusive distinction of TRIM mechanism could permit the file system whereas trashed or erased data can be collected sometimes even after deletion stored somewhere on the chip.

2. ANALYSIS OF SATA PROTOCOL

Serial-ATA primarily host interfacing with HDDs for doubling the transmission speed between host system and connected storage device that's the reason for further implementation by the SSDs and hybrid drives improved over time.For transmission of data information and control using host bus adaptor SATA protocol uses one to one direct connection.

Manuscript published on 30 August 2019.
***** Correspondence Author (s)
Pooja Patil, School of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune, India. (E-mail: Patilpk298@gmail.com)
Balaso Jagdale, School of Computer Engineering and Technology, Dr. Vishwanath Karad MIT World Peace University, Pune. India.(E-mail: balaso.jagdale@mitwpu.edu.in)

The host bus adapters and storage devices interconnect to each other over a high-speed serial cable with two pairs of conductors. One pair for variance transmission and the other one for variance reception. The Serial ATA Commands Logger captures the ATA commands between the attached storage devices and the host bus adopter also sends the captured commands to a serial console. The set of captured commands are reflexive with the ATA/ATAPI Command Set specification. In 2014 two chipsets were planned which supporting Intel Haswell and Haswell Refresh processors. Both the processors have support of Platform Controller Hubs i.e. H97 and Z97 announced by Intel for 9 series chipsets of SATA Express[13]. SATA device hot plugging requires to check capabilities of drive i.e. insertion or removal of drive that has power on which is connecting from or into backplane connector. As the powered device are not automatically in inactive state. Device initializes and operates normally after device insertion depending on the host operating system. It may also intializes hot swap initialization of devices.There are several revisions of SATA according to the generations of SATA according to the speed and other modified versions in SATA.

1. ***SATA Revision 1.0*:** SATA Revision 1.0 was released on 7th January 2003. First generation of SATA interfaces having communication rate is 1.5Gbit/s. It does not supports Native Command Queuing i.e. NCQ for communication and data transmission over host adaptor and storage device.
2. ***SATA Revision 2.0*:** SATA Revision 2.0 was released in April 2004 introducing with the Native Command Queuing. This second-generation SATA interface run with 3 Gbit/s. Further SATA Revision 2.5 was announced in August 2005 by handling contemporary mechanical drives without losing data transfer routine. SATA Revision 2.6 announced in February 2007 by adding features like Micro connector, NCQ priority, Slimline connector etc.
3. ***SATA Revision 3.0*:** Serial ATA International Organisation i.e. SATA-IO presented draft specifications of SATA Revision 3.0 in July 2008 and full specification was released on May 2009. This third generation of SATA having native transfer rate is 6 Gbit/s. In July 2011 SATA Revision 3.1 released with host identification capabilities of device as well as enabling hardware control features. Further in August 2013, SATA revision 3.2 defined as SATA Express released which is combined interface of SATA and PCI Express. This SATA revision delivers greater performance for Solid State Drives. Now SATA revision 3.3 released on February 2016 by adding features like Power disable feature which allows the power cycle drives remotely also gives greater increase in hard drives capacity.

3. PROPOSED MODEL FOR SATA SECURITY STATE MODEL

SATA security feature set is the password system which restricts access to user data on the drive as well as specific configuration capabilities. Security feature set is necessary to acquire information about current security status, supported security capabilities and security settings. There are different security states by changing in security characteristics like Power ON-OFF, Security lock ENABLE- DISABLE, FROZEN etc. This security feature set is used to allow storage device to authenticate the user using the commands provided from ATA specification which are used by the BIOS. In short SATA Security Feature Set is part of ATA sepcification in the form of commands or set of commands.

These security feature set commands are divided into three groups:

- *Password Manipulation Commands*

SECURITY SET PASSWORD: This command sets the password to drive and put drive in locked state which simultaneously restricts the access to the drive. Only the commands like identify device are accepted in locked state. As initially we can use drive without authentication, or we can say it is easily usable till execution of SECURITY SET PASSWORD command on the drive [3].

SECURITY DISBLE PASSWORD: This command deactivates the lock by removing password on the device permanently. Any command will be accepted in unlocked state only. As if the drive is in locked state then we cannot use SECURITY DISBLE PASSWORD command on the drive [3].

- *Access Control Commands*

SECURITY UNLOCK: This command unlocks drive provisionally for general use of the drive. As after power cycle or any other cold operation drive goes into lock mode again. SECURITY UNLOCK makes drive unlock but keeps safety functions as it is activated [2].

SECURITY FREEZE LOCK: This command protects unauthorised changes in security of the drive. This is especially used to protect device from attacks on the operating system level which can change the security settings of the system. If we put drive in FREEZE state, then it's impossible to make change in security settings and security states of SSD. SECURITY FREEZE LOCK command [2] is initiated from the BIOS of the host system that's the reason it freezes the security features including passwords. Also, we cannot even perform secure erase command on the drive if the drive is in a frozen state [2].

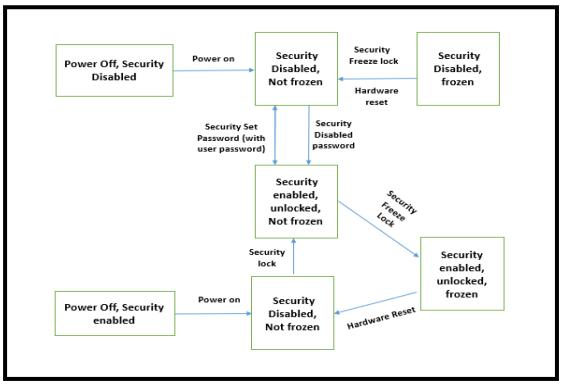


Fig 2. Proposed System

- *Media Recovery Commands*

SECURITY ERASE UNIT: This command is for the drive controller to erase all the data on the drive permanently. SECURITY ERASE UNIT command executed by the drive controller to erase the data once for all while taking the load off from the peripheral computer interfaces and CPUs. Drive must be in unfrozen state and security enabled state to execute SECURITY ERASE UNIT command [2].

***ENHANCED SECURITY ERASE UNIT*:** This command ignores device configuration overlays and overwrites all sectors. Only drive controller can have access for this command instead of the operating system[2].

This algorithm designed for testing the security features of the Solid-state drive in every achievable transitional mode by traversing one state to another in a different way. This security test suit is divided into four test cases as follows:

1. ***Security Walkthrough All States test*:** This test ensures that all the ATA commands executed as expected including the expected failure which causes expected transitions and drive stick to ATA security rules.
2. ***Security Random Transition test***: This test ensures that all ATA commands executed randomly as expected failures including execution result or state transition as well as No transition irrespective of any sequence of commands and device stick to ATA security rules.
3. ***Security No Transition test***: This test ensures that there is No change in state if transitions are not supported from one state to another state that is, we can say success or failure causing No change in state of drive while sticking to the ATA security rules.
4. ***Enhanced Security test***: This test verifies time taken for secure erase command in different modes of security like Normal security mode, Extended Normal security mode, Enhanced security mode, Extended enhanced security mode etc.

There are three phases to run a test case on the DUT i.e. Device Under Test which is solid test drive in this project.

1. ***Set-up Phase***: In Set-up phase, we check the device is ready to accept the ATA commands and is accessible through the system. We check for drive identification using IDENTIFY command.
2. ***Run Phase*:** In Run phase, the DUT goes under rigorous tests of security feature set different cases. In this phase, DUT checked after every power cycle operation for healthy state. It is checked for any unexpected state of solid-state drive.
3. ***Tear-down Phase*:** In Tear-down phase, the device clears all its occupied resources and is brought to normal state if it gets to any unexpected state.

4. ALGORITHM

Step 1: Connect SATA port and Power port of Solid-State Drive to Host System properly.

Step 2: Check whether drive is identified by Host system or not.

a. If Drive executes IDENTIFY command, then go to Step 3
b. Else go to step 1.

Step 3: Enter Set-up phase. If pass go to next step else go to

Step 4: Enter Run Phase.

Set expected output values each state as:

SEC1: ENABLED bit = 0, LOCKED bit =0, FROZEN bit = 0;
SEC2: ENABLED bit = 0, LOCKED bit =0, FROZEN bit = 1;
SEC3: POWER DOWN, ENABLED bit=1;
SEC4: ENABLED bit = 1, LOCKED bit =1, FROZEN bit = 0;
SEC5: ENABLED bit = 1, LOCKED bit =0, FROZEN bit = 0;
SEC6: ENABLED bit = 1, LOCKED bit =0, FROZEN bit = 1;
SEC0: POWER DOWN, ENABLED bit=0;

Step 5: Call Security Walkthrough All Transition Test

i. Initialize with SEC1
ii. Perform Transition from one SEC to Another
iii. Execute IDENTIFY and Compare with ENABLED bit, LOCKED bit, FROZEN bit values.
iv. If obtaining values and expecting values are same, then mark it PASS else mark it FAIL and go to Step 6.

Step 6: Call Security Random Transition Test

i. Initialize with SEC1.
ii. Run Random() to select transition
iii. Execute IDENTIFY and Compare with ENABLED bit, LOCKED bit, FROZEN bit values.
iv. If obtaining values and expecting values are same, then mark it PASS else mark it FAIL and go to Step 7.

Step 7: Call No Transition Test

i. Initialize with SEC1.
ii. Send command check there is No Transaction perform.
iii. Execute IDENTIFY and Compare with ENABLED bit, LOCKED bit, FROZEN bit values.
iv. If obtaining values and expecting values are same, then mark it PASS else mark it FAIL and go to Step 8.

Step 8: Call Enhance Security Test

i. Execute IDENTIFY check Sector Size.
ii. Perform SECURE ERASE UNIT.
iii. Check Security Mode Support value whether it is 0 or 1.
iv. If value is 0 then mark test PASS else mark it FAIL and go to step 9.

Step 9: Generate Result Table for all test cases with Runtime.

Step 10: Enter Teardown Phase.

Step 11: End.

5. RESULTS AND ANALYSIS

After execution of the Algorithm, each ATA security feature set command is executed on the solid-state drive using different test cases like security walkthrough all state transitions, security random transition, security no transition and enhanced security test. It gives output in the form of logfile. Logfile includes solid state drive details like serial number, model, device capacity, device protocol, Firmware revision, etc. Also, system details like device number, host name, host IP, operating system version, system memory details, etc. Along with the system and drive details log file contains output of security feature set i.e. change in state after each transition perform in the solid-state drive. In each test case initially checked that whether it supports security feature set or not, if yes then it starts the test case.

In every test case it frequently checks the state or change in current state with IDENTIFY command which gives value of isSecEnabled, isSecFrozen, isSecLocked. If this command return value 1 it means True and vice versa if value is 0 means False i.e. 1 means drive is in that current state and 0 means drive is not in that state as shown in fig 3. The command CHECK POWER MODE returns the current state of power module if it is 0xff it means power is ON and if it is OFF it returns error code.

```
Sending Command: CHECK POWER MODE
Check power mode returned value.............................0xff
Current Power State: .....................................PM0: Active
Sending Command: IDENTIFY
isSecEnabled value: 1
isSecFrozen value: 0
isSecLocked value: 1
returned value devSecState: 4
Security state of the drive: 4
```

Fig. 3 IDENTIFY & CHECK POWER MODE commands execution

Initially this algorithm test starts with the test case Security Walkthrough All State Test. This test case ensures that each ATA command from Security Feature Set executed successfully and returns expected failure or success which causes expected transition and device follows ATA security transition rule. Here all possible transitions are covered by traversing one state to another by obeying commands in Security Feature Set. Fig 4 shows the inter-state transition count after execution of Security Walkthrough All State test as a result.

[Inter State transition count]:

From\To	SEC0	SEC1	SEC2	SEC3	SEC4_A	SEC4_B	SEC4_C	SEC4_D	SEC4_E	SEC4_F	SEC5	SEC6
SEC0	X	2	X	X	X	X	X	X	X	X	X	X
SEC1	1	4	3	X	X	X	X	X	X	X	17	X
SEC2	1	2	X	X	X	X	X	X	X	X	X	X
SEC3	X	X	X	X	8	X	X	X	X	X	X	X
SEC4_A	X	4	X	1	4	93	X	X	X	X	40	X
SEC4_B	X	2	X	1	2	2	62	X	X	X	26	X
SEC4_C	X	2	X	1	2	X	2	37	X	X	20	X
SEC4_D	X	2	X	1	2	X	X	2	18	X	14	X
SEC4_E	X	2	X	1	2	X	X	X	2	5	7	X
SEC4_F	X	X	X	1	4	X	X	X	X	6	X	X
SEC5	X	4	X	1	116	X	X	X	X	X	326	3
SEC6	X	X	X	1	2	X	X	X	X	X	X	X
Total	2	24	4	8	142	95	64	39	20	11	450	4

Fig. 4 Inter-state Transition Count after Security Walkthrough Testcase

After the Security Walkthrough All State test next test case is Security Random Transition test. This test ensures that random execution of each ATA command from the Security Feature Set executed successfully and returns success or failure caused by commands. Also, these return value causes expected transitions or No transitions in state of security model irrespective of any sequence of commands and device obeys to commands in Security Feature Set. Fig 5 shows the inter-state transition count after execution of Security Random Transition test as a result.

[Inter State transition count]:

From\To	SEC0	SEC1	SEC2	SEC3	SEC4_A	SEC4_B	SEC4_C	SEC4_D	SEC4_E	SEC4_F	SEC5	SEC6
SEC0	X	5	X	X	X	X	X	X	X	X	X	X
SEC1	4	174	2	X	X	X	X	X	X	X	6	X
SEC2	1	1	X	X	X	X	X	X	X	X	X	X
SEC3	X	X	X	X	3	X	X	X	X	X	X	X
SEC4_A	X	1	X	1	94	2	X	X	X	X	7	X
SEC4_B	X	1	X	0	1	1	0	X	X	X	0	X
SEC4_C	X	0	X	0	0	X	0	0	X	X	0	X
SEC4_D	X	0	X	0	0	X	X	0	0	X	0	X
SEC4_E	X	0	X	0	0	X	X	X	0	0	0	X
SEC4_F	X	X	X	0	0	X	X	X	X	0	X	X
SEC5	X	4	X	2	6	X	X	X	X	X	25	1
SEC6	X	X	X	0	1	X	X	X	X	X	X	X
Total	5	186	95	3	105	3	0	0	0	0	38	45

Fig. 5 Inter-state Transition Count after Security Random Testcase

In case of any wrong or irrelevant command send then security state should not be change or perform no transition on the solid-state drive. For this purpose, Security No Transition test is designed. In Security No Transition test unlike Security Walkthrough All Transition test and Security Random Transition test checking for expected change in state of the security state model after the command execution. In this test Security Feature set commands complete and do not transit to other security state if transition is not supported that is success or failure in the Security Feature Set command causes no transition obeys on solid-state drive. Fig 6 shows the inter-state transition count after execution of Security No Transition State test as a result.

[Inter State transition count]:

From\To	SEC0	SEC1	SEC2	SEC3	SEC4_A	SEC4_B	SEC4_C	SEC4_D	SEC4_E	SEC4_F	SEC5	SEC6
SEC0	X	0	X	X	X	X	X	X	X	X	X	X
SEC1	0	72	1	X	X	X	X	X	X	X	2	X
SEC2	0	1	X	X	X	X	X	X	X	X	X	X
SEC3	X	X	X	X	0	X	X	X	X	X	X	X
SEC4_A	X	0	X	0	74	21	X	X	X	X	7	X
SEC4_B	X	0	X	0	0	11	16	X	X	X	5	X
SEC4_C	X	0	X	0	0	X	11	11	X	X	5	X
SEC4_D	X	0	X	0	0	X	X	11	6	X	5	X
SEC4_E	X	0	X	0	0	X	X	X	11	1	4	X
SEC4_F	X	X	X	0	1	X	X	X	X	17	X	X
SEC5	X	1	X	0	26	X	X	X	X	X	148	1
SEC6	X	X	X	0	1	X	X	X	X	X	X	X
Total	0	74	79	0	102	32	27	22	17	18	176	79

Fig. 6 Inter-state Transition Count after Security No. Transition Testcase

For testing media recovery commands in Security Feature Set we perform SECURITY ERASE UNIT command. This command executed by the drive controller to erase the data once for all while taking a load off from the peripheral computer interfaces and CPUs. This command ignores device configuration overlays and overwrites all sectors. Test case Enhanced Security Test verifies time taken for secure erase command in every security mode.

There are four different security modes in secure erase i.e. Normal Security Mode, Extended Normal Security Mode, Enhanced Security Mode, Extended Enhanced Security Mode. Each mode has its estimated time for completion of SECURE ERASE UNIT command which is placed in IDENTIFY command. Fig 7 & 8 shows verification of Normal and Enhanced Security Mode time respectively.

```
Sending Command: IDENTIFY
Drive Logical Sector Size .....512
Drive Maximum LBA Range.....468862128
Security Feature Set.....Supported

######################## Verification of Normal Security Mode Time ########################
Sending Command: IDENTIFY
[ 1.1 ] (1)         Identify Device Command (Expected Value: Command completed without error).....passed
[ 1.2 ] (1)         Check Normal Security Mode Support (Expected Value: 0 (0x0) ).....passed
```

Fig. 7 Verification of Normal Security Mode Time

As this algorithm is designed for testing the security features of solid-state drive in every possible transition method i.e.in each test case.

```
[ 1.5 ]      total test steps 2 : passed steps 2 : failed steps 0.....passed

[ 1 ]        total test steps 10 : passed steps 10 : failed steps 0.....passed

######################## Verification of Enhanced Security Mode Time ########################
Sending Command: IDENTIFY
[ 2.1 ] (1)         Identify Device Command (Expected Value: Command completed without error).....passed
[ 2.2 ] (1)         Check Enhanced Security Mode Support (Expected Value: 0 (0x0) ).....passed
```

Fig. 8 Verification of Enhanced Security Mode Time

After execution of all the testcases the final result prints the result i.e. test either pass or fail with the run time of the test as shown in fig 9.

```
|========================================== Test Suite Result ==========================================|
| Test Name                                                                  | Result  |  Runtime  |
|----------------------------------------------------------------------------|---------|-----------|
| Walkthrough                                                                | passed  | 00:41:44  |
| RandomTraversal                                                            | passed  | 00:31:05  |
| NoTransition                                                               | passed  | 00:24:33  |
| EnhancedSec                                                                | passed  | 01:23:27  |
|============================================================================================================|
| Total test cases  : 4                                                                                      |
| Passed tests      : 4                                                                                      |
| Failed tests      : 0                                                                                      |
|============================================================================================================|
```

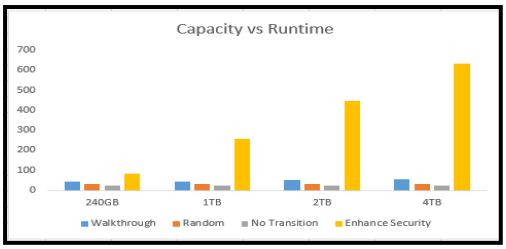
Fig. 9 Final result of all the testcases with run time

Failure in any testcase can be consider by failure in ATA command which can be either unexpected outcome of the command on the device as well as ATA command execution success or failure has caused unexpected security state transition. When we execute all the security testcases on different capacity Solid state drives we get the results as shown in following table 1.

Table 1. Runtime (in Min) for different capacity SSDs.

Capacity	Walk-through	Random	No Transition	Enhance Security
240GB	41.79	30.6	24.35	84.14
1TB	45.54	30.42	24.02	256.06
2TB	52.1	30.34	24.43	448
4TB	57.45	30.45	24.26	632.09

We can see variations in graph 1. Enhance Security test's runtime with different capacity drives as capacity increases runtime also increases i.e., we can say runtime and drive capacity are directly proportional to each other in Enhance Security testcase.



Graph 1. Capacity vs Runtime

The reason behind this time variation is read- write operation perform on the drive. Other testcases consumes approximately same time because other security state change transitions are performing on firmware level.

6. APPLICATION

- Verification of ATA- Security feature set with rigorous testing.
- Validate the security features on firmware testing.

7. CONCLUSION

Here, as we focused on the internal structure and components of Solid-state drives becoming hot plug over Hard-disk drives. By losing the mechanical arms moving on the rotating magnetic disk to support of flash memory chips to store data and in case of host controllers, SATA SSDs should preferable for the client-based host systems as well for enterprise system. SATA security feature set allows the Solid-state drives to make the device authenticate to the users also manage the access i.e. restricts the access of data as well as specific configuration capabilities. Also, we conclude that overall runtime for security feature model is increases as increase in solid state drive's capacity.

REFERENCE

1. Pooja Patil, Balasaheb Jagdale, Comparative study of Host Interfaces Typically use on Solid State Drives, Journal of Applied Science and Computation, Volume VI, March 2019.
2. Advanced Technology Attachment Command Set -3, INCITS, October 2016.
3. Ravi Kant Chaurasia, Dr. Priyanka Sharma, Solid State Drive (SSD) Forensics Analysis: A New Challenge, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, December 2017
4. Belkasoft,,"Recovering Evidence from SSD Drive in 2014: Understanding TRIM, Garbage Collection and Exclusions." Forensic Focus Articles. 23 Sept. 2014.
5. Wei, Michael, Laura Grupp, Steven Swanson. "Reliably Erasing Data from Flash-Based Solid-State Drives." University of California, San Diego.
6. Mao, Chau-yuan "SDD TRIM Operations: Evaluation and Analysis" Site. Natinal Chiao Tung University, July 2013.
7. Accardi, K.C. and Wilcox, M. Linux storage stack performance. In Linux Storage and Filesystem Workshop (San Jose 2008), USENIX.

8. "Seagate, APT and Vitesse Unveil the First Serial ATA Disc Drive at Intel Developer Forum", Seagate Technology, Aug. 22, 2000
9. Jeffrey Janukowicz, “Worldwide Solid-State Storage 2012-2016 – Forecast & Analysis” Solid State Drives and Hard Drive Components, June 2012.
10. CrystalDiskMark, http://crystalmark.info/software/CrystalDiskMark/index-e.html.
11. CE Stevens. AT Attachment 8-ATA/ATAPI Command Set – 4 (ACS-4) working Draft, American National Standard, Revision 14, 2016.
12. R. Micheloni, L. Crippa, and A. Marelli: Inside NAND Flash Memories. New York, NY, USA: Springer-Verlag, 2010.
13. Zophar Sante, ATA Security Feature Set Guide With introduction to TCG Opal and SEDs with AES 256 Encryption, BiTMICRO Networks, Inc May 28, 2018.
14. Rino Micheloni, Microsemi Corporation, ‘Solid-State Drive (SSD): A Non-volatile Storage System’ Vol. 105, No. 4, April 2017 Proceedings of the IEEE.
15. Martin, Nick, and Jeff Zimmerman. "Analysis of the forensic challenges posed by flash devices." University of Nebraska Niels Broekhuijsen, Niels Broekhuijsen,"Report: Intel 9-Series Will Feature 10-16 Gb/s SATA Express", January 10,2014.