Apacer

Instant Keychange

White Paper

December 20, 2018

Version 1.1

Apacer Technology Inc.
1F, No.32, Zhongcheng Rd., Tucheng Dist., New Taipei City, Taiwan, R.O.C
Tel: +886-2-2267-8000 Fax: +886-2-2267-2261
www.apacer.com

Table of Contents

1. Introduction

As SSDs have become more popular for storing sensitive data, there is a growing need for strong data encryption to mitigate the risk of data loss. One of the most recommended methods is to implement hardware-based encryption, offering a strong defense against various attack techniques.

This white paper describes the general concept of AES and ATA Secure Command (Erase Function). It also explains how Apacer's Instant Keychange is implemented to eliminate any unauthorized access to confidential data.

1.1 What is AES Encryption?

As data is taken in from a host and sent through the controller, it is processed with an AES encryption key. This key is known only to the controller, not to the data provider or user, and is known as an AES Key. (A user can then further encrypt an AES key with a password-based Access Key, if required.)

The controller sends the encrypted data, along with the AES key, to the flash memory to be stored. Later, when it is accessed, the AES key is called upon once again to decrypt the data into its original readable form. Since this process happens in hardware, there is no additional strain on the host's CPU.

As data passing from the host is encrypted with an AES key before written to flash memory, it also needs to be decrypted by the same key before it can be accessed by the host, as illustrated in Figure 1-1.

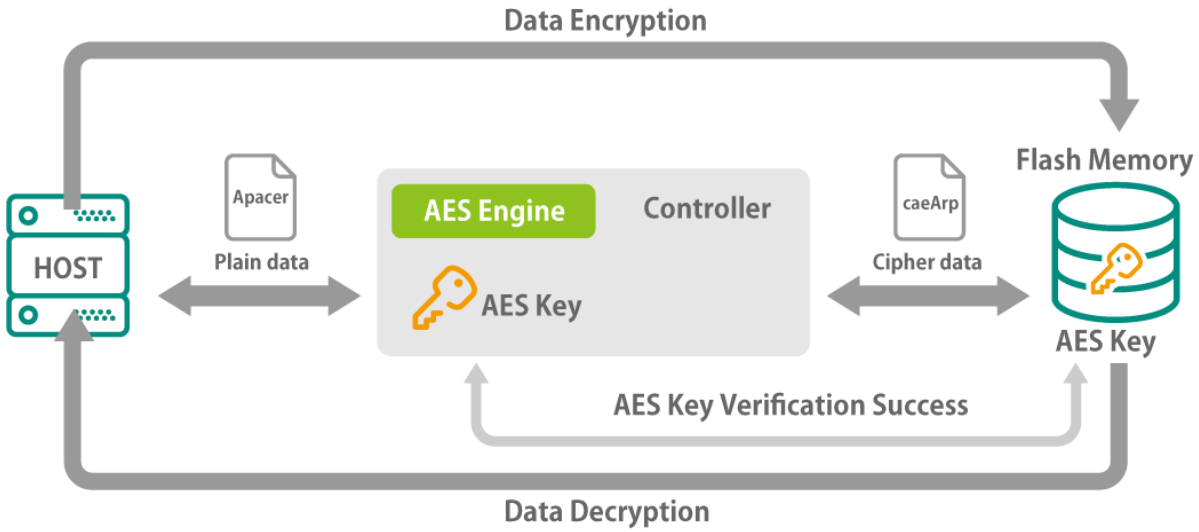

Figure 1-1 Typical implementation of AES encryption/decryption

1.2 What is ATA Secure Command (Erase Function)?

One common way to erase a NAND Flash drive is by using the ATA Secure Command erase function. If this function is executed, then all user data and the management table will be destroyed and cannot be permanently retrieved. The amount of time that it takes to carry out this function is dependent on the size of the drive. For example, to carry out this function on a 512GB drive will take approximately 20 seconds.

2. Instant Keychange

2.1 How It Works

As previously mentioned, all the data stored on a drive protected by AES encryption needs to be decrypted by a matching AES key before it can be read. The real advantage of AES encryption is that the key is automatically generated during production and provides an instant protection mechanism. And since it is a 256-bit key, the chance of it being brute-forced is practically impossible.

This is the Instant Keychange function, as shown in figure 1-2 below. When an Instant Keychange command is issued, a new key will be generated to replace the original key stored in the flash memory less than a second. Since the new key does not match the old one, when the host is attempting to access the data present in the flash memory, the data will be irretrievable due to AES key authentication failure. The data has not been erased in the conventional sense of all the bits being rewritten as ones or zeros, but it is functionally unreadable and therefore completely protected.

Another important feature of the Instant Keychange function is that it can be activated in two ways. Either a software command can be sent, or a hardware trigger can be activated.

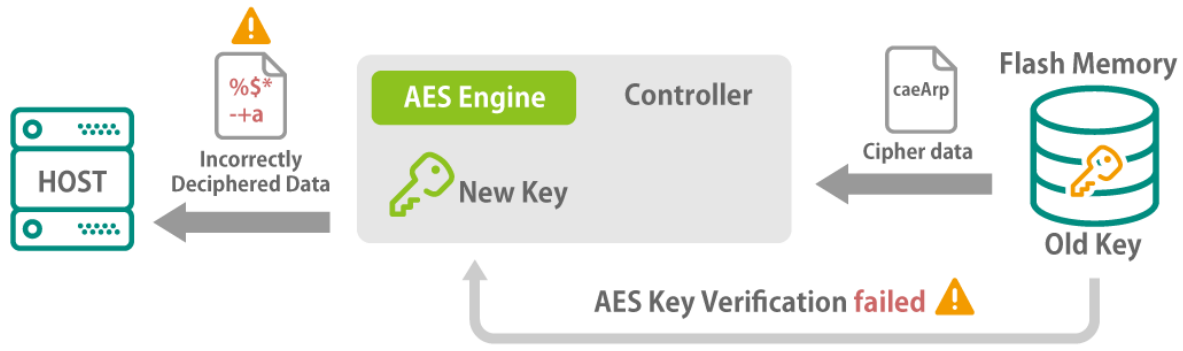

Figure 1-2 Data unreadable after execution of Instant Keychange command

2.2 ATA Secure Command (Erase Function) vs. Instant Keychange

When comparing ATA Secure Command's erase function to Instant Keychange, the latter has one clear advantage. That is the advantage of time. While a 512GB hard drive would take about 20 seconds to erase with ATA Secure Command, it would take less than one second for a drive of the same size that incorporates Apacer's Instant Keychange technology to generate a new encryption key and make the data unreadable. For situations where time is extremely limited, Instant Keychange provides a superior solution.

3. Conclusion

To keep data secure from potential malicious users, Apacer NAND flash storage devices have adopted AES technology via the Instant Keychange tool, by storing the data in an encrypted format with an encryption key. The encrypted data can never be accessed once the original key is destroyed. And destroying the original key and creating a new one takes less than a second – much faster than traditional forms of drive erasure. It can be accomplished via a hardware trigger or a software command. In addition, the type of AES 256-bit encryption adopted to block unauthorized access attempts is hardware-based rather than software-based because of the advantages of the former in cost, security and consumption of CPU resources.

Revision History

Revision	Description	Date
1.0	Official release	10/3/2018
1.1	Textual and naming revisions	12/20/2018

Global Presence

Taiwan (Headquarters)
Apacer Technology Inc.
1F., No.32, Zhongcheng Rd., Tucheng Dist.,
New Taipei City 236, Taiwan R.O.C.
Tel: 886-2-2267-8000
Fax: 886-2-2267-2261
amtsales@apacer.com

U.S.A.
Apacer Memory America, Inc.
46732 Lakeview Blvd., Fremont, CA 94538
Tel: 1-408-518-8699
Fax: 1-510-249-9551
sa@apacerus.com

Japan
Apacer Technology Corp.
6F, Daiyontamachi Bldg., 2-17-12, Shibaura, Minato-Ku,
Tokyo, 108-0023, Japan
Tel: 81-3-5419-2668
Fax: 81-3-5419-0018
jpservices@apacer.com

Europe
Apacer Technology B.V.
Science Park Eindhoven 5051 5692 EB Son,
The Netherlands
Tel: 31-40-267-0000
Fax: 31-40-290-0686
sales@apacer.nl

China
Apacer Electronic (Shanghai) Co., Ltd
Room D, 22/FL, No.2, Lane 600, JieyunPlaza,
Tianshan RD, Shanghai, 200051, China
Tel: 86-21-6228-9939
Fax: 86-21-6228-9936
sales@apacer.com.cn

India
Apacer Technologies Pvt Ltd,
1874, South End C Cross, 9th Block Jayanagar,
Bangalore-560069, India
Tel: 91-80-4152-9061/62
Fax: 91-80-4170-0215
sales_india@apacer.com