JEDEC STANDARD

Replay Protected Monotonic Counter (RPMC) for Serial Flash Devices

JESD260

APRIL 2021

JEDEC SOLID STATE TECHNOLOGY ASSOCIATION

NOTICE

JEDEC standards and publications contain material that has been prepared, reviewed, and approved through the JEDEC Board of Directors level and subsequently reviewed and approved by the JEDEC legal counsel.

JEDEC standards and publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for use by those other than JEDEC members, whether the standard is to be used either domestically or internationally.

JEDEC standards and publications are adopted without regard to whether or not their adoption may involve patents or articles, materials, or processes. By such action JEDEC does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the JEDEC standards or publications.

The information included in JEDEC standards and publications represents a sound approach to product specification and application, principally from the solid state device manufacturer viewpoint. Within the JEDEC organization there are procedures whereby a JEDEC standard or publication may be further processed and ultimately become an ANSI standard.

No claims to be in conformance with this standard may be made unless all requirements stated in the standard are met.

Inquiries, comments, and suggestions relative to the content of this JEDEC standard or publication should be addressed to JEDEC at the address below, or refer to www.jedec.org under Standards and Documents for alternative contact information.

Published by
©JEDEC Solid State Technology Association 2021
3103 North 10th Street
Suite 240 South
Arlington, VA 22201-2108

PRICE: Contact JEDEC

REPLAY PROTECTED MONOTONIC COUNTER (RPMC) FOR SERIAL FLASH DEVICES

Contents

Foreword

This document was prepared by the JC42.4_3 Serial Flash task group authorized by the JC42.4 Non-Volatile Memory subcommittee.

Introduction

The Serial Flash is the persistent storage available on the motherboard of a PC platform. In PC platforms the Serial Flash contains CPU BIOS code. In addition it provides persistent storage support for a number of microcontrollers on the platform used for critical functions such as security and power management.

Serial Flash access control is enforced at a sector or a subsector granularity. A specific sector may be read only (write protected), or read/write (can be written to during runtime for normal functionality). The Flash read/write protection is performed by the Serial Flash Controller HW on the motherboard.

REPLAY PROTECTED MONOTONIC COUNTER (RPMC) FOR SERIAL FLASH DEVICES

(From JEDEC Board Ballot JCB-21-12, formulated under the cognizance of the JC-42.4 Subcommittee on Nonvolatile Memory Devices

1 Scope

The security protections described in the Introduction are necessary but not sufficient to meet advanced use cases of a PC. This document provides the requirements for an additional block called as Replay Protection Monotonic Counter. (RPMC) Replay Protection provides a building block towards providing additional security. This block requires modifications in both a Serial Flash device and Serial Flash Controller. The standard defines new commands for Replay Protected Monotonic Counter operations. A device that supports RPMC can support these new commands as defined in this standard.

2 Normative References

The following normative documents contain provisions that through reference in this text, constitutes provisions of this standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated. For undated references, the latest edition of the normative document referred to applies.

JM7.01, *Style Manual for Standards and Other Publications of JEDEC*

JESD88E, *Dictionary of Terms for Solid-State Technology*

JESD216, *Serial Flash Discoverable Parameters (SFDP)*

NIST 180-4, *Secure Hash Standard (SHS)*

NIST 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*