# 11th Generation Intel® Core™ Processor

## Specification Update

***Supporting 11th Generation Intel® Core™ Processor Families for S Platform, formerly known as Rocket Lake***

***Revision 002***

***April 2021***

Document Number: 634808-002

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

All product plans and roadmaps are subject to change without notice.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

© Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

*Other names and brands may be claimed as the property of others.

Copyright © 2021, Intel Corporation. All rights reserved.

# Contents



## Tables



## Figure

# Revision History

| Revision Number | Description | Revision Date |
|---|---|---|
| 001 | • Initial Release | March 2021 |
| 002 | • Added Erratum: RKL019 | April 2021 |

§§

# Preface

This document is an update to the specifications contained in the documents listed in the following Affected Documents/Related Documents table. It is a compilation of device and document errata and specification clarifications and changes, and is intended for hardware system manufacturers and for software developers of applications, operating system, and tools.

Information types defined in the Nomenclature section of this document are consolidated into this updated document and are no longer published in other documents. This document may also contain information that has not been previously published.

## Affected Documents

| Document Title | Document Number |
|---|---|
| 11th Generation Intel® Core™ Processors Datasheet, Volume 1 of 2 | 634648 |
| 11th Generation Intel® Core™ Processors Datasheet, Volume 2 of 2 | 636761 |

## Related Documents

| Document Title | Document Number/Location |
|---|---|
| AP-485, Intel® Processor Identification and the CPUID Instruction | http://www.intel.com/design/processor/applnots/241618.htm |
| Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 1: Basic Architecture<br>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2A: Instruction Set Reference Manual A-M<br>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 2B: Instruction Set Reference Manual N-Z<br>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3A: System Programming Guide<br>Intel® 64 and IA-32 Architectures Software Developer's Manual, Volume 3B: System Programming Guide<br>Intel® 64 and IA-32 Intel® Architecture Optimization Reference Manual | http://www.intel.com/products/processor/manuals/index.htm |
| Intel® 64 and IA-32 Architectures Software Developer's Manual Documentation Changes | http://www.intel.com/content/www/us/en/processors/architectures-software-developer-manuals.html |
| Intel® Virtualization Technology Specification for Directed I/O Architecture Specification | D51397-001 |
| ACPI Specifications | www.acpi.info |

## Nomenclature

**Errata –** These are design defects or errors. Errata may cause the processor's behavior to deviate from published specifications. Hardware and software designed to be used with any given stepping must assume that all errata documented for that stepping are present on all devices.

**Specification Changes –** These are modifications to the current published specifications. These changes is incorporated in the next release of the specifications.

**Specification Clarifications –** This describe a specification in greater detail or further highlight a specifications impact to a complex design situation. These clarifications is incorporated in the next release of the specifications.

**Documentation Changes –** This include typos, errors, or omissions from the current published specifications. These changes are incorporated in the next release of the specifications.

***Note:*** Errata remain in the specification update throughout the product's lifecycle, or until a particular stepping is no longer commercially available. Under these circumstances, errata removed from the specification update are archived and available upon request. Specification changes, specification clarifications, and documentation changes are removed from the specification update, when the appropriate changes are made to the appropriate product specification or user documentation (datasheets, manuals, etc.).

§ §

# Identification Information

## Component Identification via Programming Interface

The processor stepping is identified by the following register contents:

**Table 1. Processor Lines Component Identification**

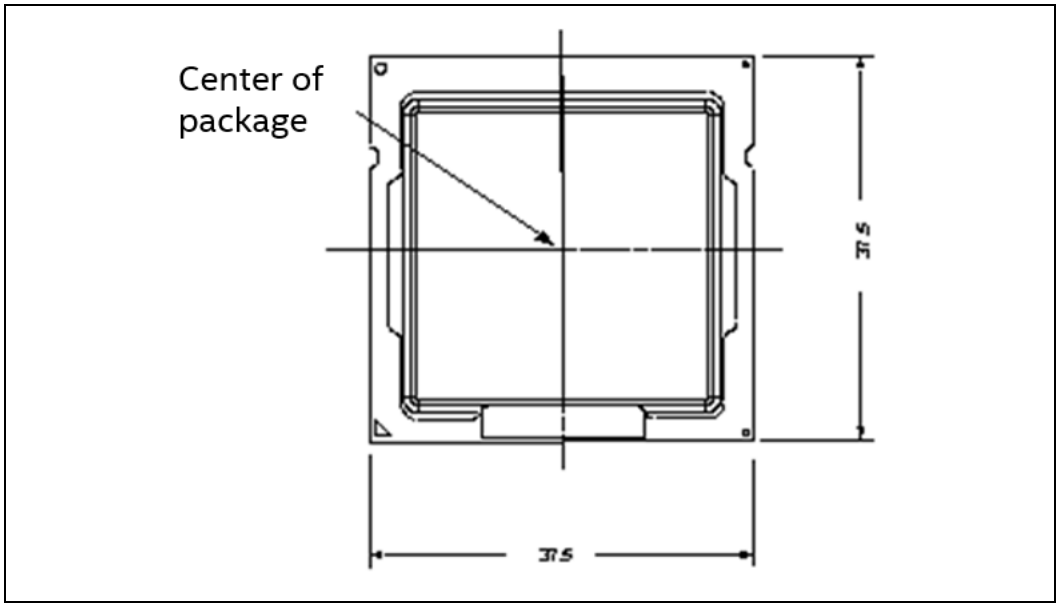
| Processor | CPUID | Reserved [31:28] | Extended Family [27:20] | Extended Model [19:16] | Reserved [15:14] | Processor Type [13:12] | Family Code [11:8] | Model Number [7:4] | Stepping ID [3:0] |
|---|---|---|---|---|---|---|---|---|---|
| **S** | A0671h | Reserved | 0000b | 1010b | Reserved | 00b | 0110b | 0111b | 0001b |

1. The Extended Family, Bits [27:20] are used in conjunction with the Family Code, specified in Bits[11:8], to indicate whether the processor belongs to the Celeron®, Pentium®, or Intel® Core™ processor family.
2. The Extended Model, Bits [19:16] in conjunction with the Model Number, specified in Bits [7:4], are used to identify the model of the processor within the processor's family.
3. The Family Code corresponds to Bits [11:8] of the EDX register after RESET, Bits [11:8] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the generation field of the Device ID register accessible through Boundary Scan.
4. The Model Number corresponds to Bits [7:4] of the EDX register after RESET, Bits [7:4] of the EAX register after the CPUID instruction is executed with a 1 in the EAX register, and the model field of the Device ID register accessible through Boundary Scan.
5. The Stepping ID in Bits [3:0] indicates the revision number of that model. Refer table above for the processor stepping ID number in the CPUID information.
6. When EAX is initialized to a value of '1', the CPUID instruction returns the Extended Family, Extended Model, Processor Type, Family Code, Model Number and Stepping ID value in the EAX register. The EDX processor signature value after reset is equivalent to the processor signature output value in the EAX register.

Cache and TLB descriptor parameters are provided in the EAX, EBX, ECX and EDX registers after the CPUID instruction is executed with a 2 in the EAX register.

# Component Marking Information

**Figure 1. S-Processor Line Multi-Chip Package LGA Top-Side Markings**




Pin Count: 1200 Package Size: 37.5 mm x 37.5 mm

**Production (SSPEC):**

- FPO: FPOxxxxx
- {eX}
- SWIR1: Intel® logo

***Note:*** "1" is used to extract the unit visual ID (2D ID).

***Note:*** Processor list can be found at:
https://ark.intel.com/content/www/us/en/ark/products/codename/192985/rocket-lake.html

§ §

# *Summary Tables of Changes*

The following table indicates the Specification Changes, Errata, Specification Clarifications or Documentation Changes, which apply to the listed processor stepping. Intel intends to fix some of the errata in a future stepping of the component, and to account for the other outstanding issues through documentation or Specification Changes as noted. This table uses the following notations:

## Codes Used in Summary Table

| Stepping | Description |
|---|---|
| (No mark) or (Blank Box) | This erratum is fixed in listed stepping or specification change does not apply to listed stepping. |

| Status | Description |
|---|---|
| Doc | Document change or update that is implemented. |
| Planned Fix | This erratum may be fixed in a future stepping of the product. |
| Fixed | This erratum has been previously fixed in Intel hardware, firmware, or software. |
| No Fix | There are no plans to fix this erratum. |

§ §

# Errata Summary Table

| ID | Processor Line/Stepping | Title |
|---|---|---|
| | S | |
| RKL001 | No Fix | Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses |
| RKL002 | Fixed | REP MOVSB Instruction To or From a Non-flat Segment May Cause Unpredictable System Behavior |
| RKL003 | Fixed | Usage of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt |
| RKL004 | No Fix | Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set |
| RKL005 | No Fix | Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception |
| RKL006 | No Fix | VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values |
| RKL007 | No Fix | Processor May Hang if Warm Reset Triggers During BIOS Initialization |
| RKL008 | No Fix | IA32_RTIT_STATUS.FilterEn Bit Might Reflect a Previous Value |
| RKL009 | Fixed | Time Stamp Counters May Contain a Shifted Time Value |
| RKL010 | No Fix | Incorrect ECC Reporting Following Entry to PKG-C7 |
| RKL011 | No Fix | PMU MSR_UNC_PERF_FIXED_CTR is Cleared after Pkg C7 or Deeper |
| RKL012 | No Fix | Unable to Transmit Modified Compliance Test Pattern at 2.5 GT/S or 5.0 GT/s Link Speeds |
| RKL013 | No Fix | PCIe Root Ports May Fail Tx Differential Return Loss Compliance Test |
| RKL014 | No Fix | PEG10 PCIe Root Port May Report Incorrect Maximum Link Width |
| RKL015 | Fixed | DMI Link Failure During L1 Exit |
| RKL016 | Fixed | Processor Peg Ports 10,11, or 12 PCIe Link May Hang During S0ix/S3/S4/S5 Cycles |
| RKL017 | No Fix | PCIe Root Ports May Fail Tx Differential Return Loss |
| RKL018 | Fixed | System May Hang if Booted with TXT Disabled |
| RKL019 | No Fix | Single Core configurations May Hang on S3/S4 Resume |

§ §

## Specification Changes

| No. | Specification Changes |
|---|---|
| | None for this revision of this specification update. |

## Specification Clarifications

| No. | Specification Clarifications |
|---|---|
| | None for this revision of this specification update. |

## Documentation Changes

| No. | Documentation Changes |
|---|---|
| | None for this revision of this specification update. |

§ §

# Errata Details

| RKL001 | Placing Page Table Information in the APIC-Access Page May Lead to Unexpected Page Faults While Performing Enclave Accesses |
|---|---|
| **Problem** | Guest-physical access using a guest-physical address that translates to an address on the APIC-access page (as identified by the APIC-access address field in the VMCS) should cause an APIC-access VM exit. This includes page table information accesses done as part of page translation (page walks). Due to this erratum placing page table information in the APIC-access page may result in a page fault instead of VM exit when the page translation is done as part of an enclave access. |
| **Implication** | Software that places page table information in the APIC access page may get page faults on executing enclave accesses, instead of exiting to the VMM (Virtual-Machine Monitor). Intel has not observed this erratum with any commercially available software. |
| **Workaround** | Software should not place page table information in the APIC access page. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL002 | REP MOVSB Instruction To or From a Non-flat Segment May Cause Unpredictable System Behavior. |
|---|---|
| **Problem** | Under complex microarchitectural conditions, using a REP MOVSB instruction in which at least one of the operands (destination or source) of the instruction is in a non-flat segment mode, might cause unpredictable system behavior. |
| **Implication** | Due to this erratum, unpredictable system behavior may occur. Intel has not observed this erratum with any commercially available software. |
| **Workaround** | It is possible for BIOS to contain a workaround for this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL003 | Usage of Bit 55 of IA32_TSC_DEADLINE MSR May Cause Spurious Timer Interrupt |
|---|---|
| **Problem** | When using the APIC timer in Time Stamp Counter Deadline (TSC-deadline) mode, if the most significant set bit in the written value to the TSC-Deadline MSR is bit 55, the processor may generate a spurious timer interrupt. |
| **Implication** | When this erratum occurs, a spurious timer interrupt may occur causing unpredictable system behavior. Intel has not observed this erratum with any commercially available software. |
| **Workaround** | It is possible for BIOS to contain a workaround for this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL004 | Overflow Flag in IA32_MC0_STATUS MSR May be Incorrectly Set |
|---|---|
| **Problem** | Under complex microarchitectural conditions, a single internal parity error seen in IA32_MC0_STATUS MSR (401h) with MCACOD (bits 15:0) value of 5h and MSCOD (bits 31:16) value of 7h, may set the overflow flag (bit 62) in the same MSR. |
| **Implication** | Due to this erratum,the IA32_MC0_STATUS overflow flag may be set after a single parity error. Intel has not observed this erratum with any commercially available software. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL005 | Wrong Page Access Semantics May be Reported When Intel® SGX ENCLU[EMODPE] Instruction Generates Page Fault (#PF) Exception |
|---|---|
| **Problem** | When Intel® SGX extends an Enclave Page Cache (EPC) via the page permissions instruction (ENCLU[EMODPE]) and generates a Page Fault (#PF), even though the page permissions instruction access is a read access to the target page, the Page Fault Error Code (#PF's PFEC) will indicate that the fault occurred on a write (PFEC.W bit will be set) instead. |
| **Implication** | This erratum may impact debugging Intel® SGX enclaves software. Intel has not observed this erratum with any commercially available software. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL006 | VERR Instruction Inside VM-entry May Cause DR6 to Contain Incorrect Values |
|---|---|
| **Problem** | Under complex microarchitectural conditions, a VERR instruction that follows a VM-entry with a guest-state area indicating MOV SS blocking (bit 1 in the Interruptibility state) and at least one of B3-B0 bits set (bits 3:0 in the pending debug exception) may lead to incorrect values in DR6. |
| **Implication** | Due to this erratum, DR6 may contain incorrect values. Intel has not observed this erratum with any commercially available software. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL007 | Processor May Hang if Warm Reset Triggers During BIOS Initialization |
|---|---|
| **Problem** | Under complex micro-architectural conditions, when the processor receives a warm reset during BIOS initialization, the processor may hang with a machine check error reported in IA32_MCi_STATUS, with MCACOD (bits [15:0]) value of 0400H, and MSCOD (bits [31:16]) value of 0080H. |
| **Implication** | Due to this erratum, the processor may hang. Intel has only observed this erratum in a synthetic test environment. |
| **Workaround** | None identified. |

| | |
|---|---|
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| **RKL008** | **IA32_RTIT_STATUS.FilterEn Bit Might Reflect a Previous Value** |
|---|---|
| **Problem** | Under complex microarchitectural conditions, reading the IA32_RTIT_STATUS.FilterEn bit (bit 0 in MSR 571h) after entering or exiting an RTIT region might reflect a previous value instead of the current one. |
| **Implication** | Due to this erratum, IA32_RTIT_STATUS.FilterEn bit might reflect a previous value. This erratum has not been seen in any commercially available software. |
| **Workaround** | Software should perform an LFENCE instruction prior to reading the IA32_RTIT_STATUS MSR to avoid this issue. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| **RKL009** | **Time Stamp Counters May Contain a Shifted Time Value** |
|---|---|
| **Problem** | Under complex microarchitectural conditions, the processor's RDTSC and RDTSCP instructions may report a shifted value. In these cases, the shift value will be larger than a minute. |
| **Implication** | Software may experience a non-monotonic time stamp counter, misalignment across threads, or a spurious timer interrupt. |
| **Workaround** | It is possible for BIOS to contain a workaround for this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| **RKL010** | **Incorrect ECC Reporting Following Entry to PKG-C7** |
|---|---|
| **Problem** | The Correctable and Uncorrectable ECC error address reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may be overwritten after a PKG-C7 event. |
| **Implication** | DDR Correctable and Uncorrectable ECC errors reported in ECCERRLOG0/1 (MCHBAR Offset 4048h/404Ch) may report an incorrect error address after resuming from PKG-C7. |
| **Workaround** | None Identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| **RKL011** | **PMU MSR_UNC_PERF_FIXED_CTR is Cleared after Pkg C7 or Deeper** |
|---|---|
| **Problem** | The Performance Monitoring Unit Uncore Performance Fixed Counter (MSR_UNC_PERF_FIXED_CTR (MSR 395h)) is cleared after pkg C7 or deeper. |
| **Implication** | Due to this erratum, once the system enters pkg C7 or deeper the uncore fixed counter does not reflect the actual count. |
| **Workaround** | None Identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL012 | Unable to Transmit Modified Compliance Test Pattern at 2.5 GT/S or 5.0 GT/s Link Speeds. |
|---|---|
| **Problem** | The processor's PCIe port (Bus 0, Device 1, Function 0/1/2 or Bus 0, Device 6, Function 0) does not transmit the Modified Compliance Test Pattern when in either 2.5 GT/S or 5.0 GT/s link speeds. |
| **Implication** | Due to this erratum, PCIe compliance testing may fail at 2.5 GT/S or 5.0 GT/s link speeds when enabling the Modified Compliance Test Pattern. |
| **Workaround** | None Identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL013 | PCIe Root Ports May Fail Tx Differential Return Loss Compliance Test |
|---|---|
| **Problem** | The processor's PCIe root ports may fail to meet the Tx Differential Return Loss Compliance Test's requirements as defined in PCIe Base Specification, version 4.0, section 9.3.6. |
| **Implication** | The processor may fail the Differential Return Loss compliance test. Intel has not observed this erratum to cause any functional failures. |
| **Workaround** | None identified |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL014 | PEG10 PCIe Root Port May Report Incorrect Maximum Link Width |
|---|---|
| **Problem** | When the PEG10 root port (Bus 0, Device 1, Function 0) is bifurcated, the port will incorrectly report Maximum Link Width (MLW) in the Link Capabilities register (Bus 0, Device 1, Function 0, Offset 0Ch). The processor will always indicate the MLW of x16, rather than x8. |
| **Implication** | Due to this erratum, software may expect the link to support x16 link widths, which the port cannot do while bifurcated. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL015 | DMI Link Failure During L1 Exit |
|---|---|
| **Problem** | During S3/S4/S5 and/or S0ix cycles, DMI may fail to exit L1 in the time required. |
| **Implication** | The system may hang with a machine check exception (MCACOD=2AH). |
| **Workaround** | It is possible for a BIOS code change to workaround this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL016 | Processor Peg Ports 10,11, or 12 PCIe Link May Hang During S0ix/S3/S4/S5 Cycles |
|---|---|
| **Problem** | During S0ix and/or S3/S4/S5 when processor exits a Package C-state, the PCIe link may hang for Peg ports 10, 11, or 12. |
| **Implication** | Due to this erratum, the PCIe link may hang with a machine check error (MCACOD=34H). |
| **Workaround** | It is possible for a BIOS code change to contain a workaround for this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL017 | PCIe Root Ports May Fail Tx Differential Return Loss |
|---|---|
| **Problem** | The processor's PCIe root ports may not meet the Tx Differential Return Loss specification as defined in PCIe Base Specification, version 4.0, section 8.3.7 Tx and Rx Return Loss. |
| **Implication** | The processor may fail the Tx Differential Return Loss specification. Intel has not observed any functional failures due to this erratum. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL018 | System May Hang if Booted with TXT Disabled |
|---|---|
| **Problem** | A system with TXT disabled may experience a hang during the boot process. |
| **Implication** | Due to this erratum, the system may hang during boot. |
| **Workaround** | It is possible for a BIOS code change to workaround this erratum. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

| RKL019 | Single Core configurations May Hang on S3/S4 Resume |
|---|---|
| **Problem** | When booting in a single core configuration, the system may hang when resuming from a S3/S4 or a warm reset. |
| **Implication** | Due to this erratum, the system may hang. |
| **Workaround** | None identified. |
| **Status** | For the steppings affected, refer to the Summary Table of Changes. |

§ §

# *Specification Changes*

| ID | Affected Products/ Steps | Specification Change Title | Issue | Previous Text Reference | New Text | Affected Document |
|---|---|---|---|---|---|---|
| N/A | N/A | N/A | N/A | N/A | N/A | N/A |

*§ §*

# Specification Clarification

None.

§ §

# Document-Only Change

None.

§ §