Intel Xeon Gold 6438M processor

Artikel	417755
Herstellernummer	PK8071305122301
EAN	8592978436575

Intel

Intel® Trusted Execution Technology
Intel® Trusted Execution Technology for safer computing is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. It enables an environment where applications can run within their own space, protected from all other software on the system.

Intel® Virtualization Technology for Directed I/O (VT-d)
Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

Intel® Virtualization Technology (VT-x)
Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple “virtual” platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

Intel® 64
Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.[1] Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Cache
CPU Cache is an area of fast memory located on the processor. Intel® Smart Cache refers to the architecture that allows all cores to dynamically share access to the last level cache.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) are a set of instructions that enable fast and secure data encryption and decryption. AES-NI are valuable for a wide range of cryptographic applications, for example: applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption.

Intel® Turbo Boost Technology
Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don’t.

Max Turbo Frequency
Max Turbo Frequency is the maximum single-core frequency at which the processor is capable of operating using Intel® Turbo Boost Technology and, if present, Intel® Turbo Boost Max Technology 3.0 and Intel® Thermal Velocity Boost. Frequency is typically measured in gigahertz (GHz), or billion cycles per second.

Execute Disable Bit
Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious-code attacks and

prevent harmful software from executing and propagating on the server or network.

Intel® Hyper-Threading Technology
Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® VT-x with Extended Page Tables (EPT)
Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® Speed Shift Technology
Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduces the performance impact of pervasive encryption and increases the performance of encryption-intensive workloads including SSL web serving, 5G infrastructure, and VPN/firewalls.

Intel® Software Guard Extensions (Intel® SGX)
Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications' sensitive routines and data. Intel® SGX provides developers a way to partition their code and data into CPU hardened trusted execution environments (TEE's).

Intel® Speed Select Technology – Core Power
Enables flexibility for workloads that benefit from higher base frequency on a subset of the processor's cores. While the max turbo frequency across the cores remain constant across the cores, a subset of the cores can be assigned as to run at a higher base frequency than specified, while the other cores run at lower base frequency.

Intel® Speed Select Technology – Turbo Frequency
Enables flexibility for workloads that benefit from higher turbo frequency on a subset of the processor's cores. While the base frequency remains constant across the cores, a subset of the cores can be assigned to run at a higher turbo frequency than specified, while the other cores run at lower turbo frequency.

Intel® Deep Learning Boost (Intel® DL Boost)
A new set of embedded processor technologies designed to accelerate AI deep learning use cases. It extends Intel AVX-512 with a new Vector Neural Network Instruction (VNNI) that significantly increases deep learning inference performance over previous generations.

Instruction Set Extensions
Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

Intel® Run Sure Technology
Intel® Run Sure Technology, includes advanced RAS (reliability, availability and serviceability) features that deliver high reliability and platform resiliency, to maximize uptime of servers running mission-critical workloads.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) helps protect data against exposure via physical attack on memory, such as cold-boot attacks.

Max # of UPI Links
Intel® Ultra Path Interconnect (UPI) links are a high speed, point-to-point interconnect bus between the processors, delivering increased bandwidth and performance over Intel® QPI.

# of AVX-512 FMA Units
Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Intel® Resource Director Technology (Intel® RDT)
Intel® RDT brings new levels of visibility and control over how shared resources such as last-level cache (LLC) and memory bandwidth are used by applications, virtual machines (VMs) and containers.

Intel® Speed Select Technology - Performance Profile

A capability to configure the processor to run at three distinct operating points.

Intel® Speed Select Technology - Base Frequency
Enables users to increase guaranteed base frequency on certain cores (high priority cores) in exchange for lower base frequency on remaining cores (low priority cores). Improves overall performance by boosting frequency on critical cores.

Mode-based Execute Control (MBEC)
Mode-based Execute Control can more reliably verify and enforce the integrity of kernel level code.

Intel® Boot Guard
Intel® Device Protection Technology with Boot Guard helps protect the system's pre-OS environment from viruses and malicious software attacks.

Intel® Control-Flow Enforcement Technology
CET - Intel Control-flow Enforcement Technology (CET) helps protect against the misuse of legitimate code snippets through return-oriented programming (ROP) control-flow hijacking attacks.

Intel® Transactional Synchronization Extensions
Intel® Transactional Synchronization Extensions (Intel® TSX) are a set of instructions that add hardware transactional memory support to improve performance of multi-threaded software.

Zusammenfassung

Intel® Trusted Execution Technology
Intel® Trusted Execution Technology for safer computing is a versatile set of hardware extensions to Intel® processors and chipsets that enhance the digital office platform with security capabilities such as measured launch and protected execution. It enables an environment where applications can run within their own space, protected from all other software on the system.

Intel® Virtualization Technology for Directed I/O (VT-d)
Intel® Virtualization Technology for Directed I/O (VT-d) continues from the existing support for IA-32 (VT-x) and Itanium® processor (VT-i) virtualization adding new support for I/O-device virtualization. Intel VT-d can help end users improve security and reliability of the systems and also improve performance of I/O devices in virtualized environments.

Intel® Virtualization Technology (VT-x)
Intel® Virtualization Technology (VT-x) allows one hardware platform to function as multiple "virtual" platforms. It offers improved manageability by limiting downtime and maintaining productivity by isolating computing activities into separate partitions.

Intel® 64
Intel® 64 architecture delivers 64-bit computing on server, workstation, desktop and mobile platforms when combined with supporting software.[1] Intel 64 architecture improves performance by allowing systems to address more than 4 GB of both virtual and physical memory.

Cache
CPU Cache is an area of fast memory located on the processor. Intel® Smart Cache refers to the architecture that allows all cores to dynamically share access to the last level cache.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) are a set of instructions that enable fast and secure data encryption and decryption. AES-NI are valuable for a wide range of cryptographic applications, for example: applications that perform bulk encryption/decryption, authentication, random number generation, and authenticated encryption.

Intel® Turbo Boost Technology
Intel® Turbo Boost Technology dynamically increases the processor's frequency as needed by taking advantage of thermal and power headroom to give you a burst of speed when you need it, and increased energy efficiency when you don't.

Max Turbo Frequency
Max Turbo Frequency is the maximum single-core frequency at which the processor is capable of operating using Intel® Turbo Boost Technology and, if present, Intel® Turbo Boost Max Technology 3.0 and Intel® Thermal Velocity Boost. Frequency is typically measured in gigahertz (GHz), or billion cycles per second.

Execute Disable Bit
Execute Disable Bit is a hardware-based security feature that can reduce exposure to viruses and malicious-code attacks and prevent harmful software from executing and propagating on the server or network.

Intel® Hyper-Threading Technology
Intel® Hyper-Threading Technology (Intel® HT Technology) delivers two processing threads per physical core. Highly threaded applications can get more work done in parallel, completing tasks sooner.

Intel® VT-x with Extended Page Tables (EPT)
Intel® VT-x with Extended Page Tables (EPT), also known as Second Level Address Translation (SLAT), provides acceleration for memory intensive virtualized applications. Extended Page Tables in Intel® Virtualization Technology platforms reduces the memory and power overhead costs and increases battery life through hardware optimization of page table management.

Intel® Speed Shift Technology
Intel® Speed Shift Technology uses hardware-controlled P-states to deliver dramatically quicker responsiveness with single-threaded, transient (short duration) workloads, such as web browsing, by allowing the processor to more quickly select its best operating frequency and voltage for optimal performance and power efficiency.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduces the performance impact of pervasive encryption and increases the performance of encryption-intensive workloads including SSL web serving, 5G infrastructure, and VPN/firewalls.

Intel® Software Guard Extensions (Intel® SGX)
Intel® Software Guard Extensions (Intel® SGX) provide applications the ability to create hardware enforced trusted execution protection for their applications' sensitive routines and data. Intel® SGX provides developers a way to partition their code and data into CPU hardened trusted execution environments (TEE's).

Intel® Speed Select Technology – Core Power
Enables flexibility for workloads that benefit from higher base frequency on a subset of the processor's cores. While the max turbo frequency across the cores remain constant across the cores, a subset of the cores can be assigned as to run at a higher base frequency than specified, while the other cores run at lower base frequency.

Intel® Speed Select Technology – Turbo Frequency
Enables flexibility for workloads that benefit from higher turbo frequency on a subset of the processor's cores. While the base frequency remains constant across the cores, a subset of the cores can be assigned to run at a higher turbo frequency than specified, while the other cores run at lower turbo frequency.

Intel® Deep Learning Boost (Intel® DL Boost)
A new set of embedded processor technologies designed to accelerate AI deep learning use cases. It extends Intel AVX-512 with a new Vector Neural Network Instruction (VNNI) that significantly increases deep learning inference performance over previous generations.

Instruction Set Extensions
Instruction Set Extensions are additional instructions which can increase performance when the same operations are performed on multiple data objects. These can include SSE (Streaming SIMD Extensions) and AVX (Advanced Vector Extensions).

Intel® Run Sure Technology
Intel® Run Sure Technology, includes advanced RAS (reliability, availability and serviceability) features that deliver high reliability and platform resiliency, to maximize uptime of servers running mission-critical workloads.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) helps protect data against exposure via physical attack on memory, such as cold-boot attacks.

Max # of UPI Links
Intel® Ultra Path Interconnect (UPI) links are a high speed, point-to-point interconnect bus between the processors, delivering increased bandwidth and performance over Intel® QPI.

# of AVX-512 FMA Units
Intel® Advanced Vector Extensions 512 (AVX-512), new instruction set extensions, delivering ultra-wide (512-bit) vector operations capabilities, with up to 2 FMAs (Fused Multiply Add instructions), to accelerate performance for your most demanding computational tasks.

Intel® Resource Director Technology (Intel® RDT)
Intel® RDT brings new levels of visibility and control over how shared resources such as last-level cache (LLC) and memory bandwidth are used by applications, virtual machines (VMs) and containers.

Intel® Speed Select Technology - Performance Profile
A capability to configure the processor to run at three distinct operating points.

Intel® Speed Select Technology - Base Frequency
Enables users to increase guaranteed base frequency on certain cores (high priority cores) in exchange for lower base frequency on remaining cores (low priority cores). Improves overall performance by boosting frequency on critical cores.

Mode-based Execute Control (MBEC)
Mode-based Execute Control can more reliably verify and enforce the integrity of kernel level code.

Intel® Boot Guard
Intel® Device Protection Technology with Boot Guard helps protect the system’s pre-OS environment from viruses and malicious software attacks.

Intel® Control-Flow Enforcement Technology
CET - Intel Control-flow Enforcement Technology (CET) helps protect against the misuse of legitimate code snippets through return-oriented programming (ROP) control-flow hijacking attacks.

Intel® Transactional Synchronization Extensions
Intel® Transactional Synchronization Extensions (Intel® TSX) are a set of instructions that add hardware transactional memory support to improve performance of multi-threaded software.

Intel Xeon Gold 6438M, Intel® Xeon® Gold, LGA 4677 (Socket E), Intel, 6438M, 2.2 GHz, 64-bit

Intel Xeon Gold 6438M. Processor family: Intel® Xeon® Gold, Processor socket: LGA 4677 (Socket E), Processor manufacturer: Intel. Memory channels: Octa-channel, Maximum internal memory supported by processor: 6 TB, Memory types supported by processor: DDR4-SDRAM. Market segment: Server, Use conditions: Server/Enterprise, Supported instruction sets: AMX, SSE4.2, AVX, AVX 2.0, AVX-512. Maximum Enclave Size Support for Intel® SGX: 128 GB, Intel® Data Streaming Accelerator (DSA): 1 default devices, Intel® In-memory Analytics Accelerator (IAA): 1 default devices. Processor package size: 77.5 x 56.5 mm

Merkmale

Logistics data

Harmonized System (HS) code	8542310001

Other features

Maximum internal memory	4 TB

Weight & dimensions

Processor package size	77.5 x 56.5 mm

Operational conditions

Tcase	85 °C
DTS Max	97 °C

Graphics

On-board graphics card	N
Discrete graphics card	N
On-board graphics card model	Not available
Discrete graphics card model	Not available

Memory

Maximum internal memory supported by processor	6 TB
Memory types supported by processor	DDR4-SDRAM
Memory channels	Octa-channel
ECC	Y

Technical details

Launch date	Q1'23
Status	Launched
Memory speed (max)	4800 MHz
Number of UPI links	3
Package carrier	E1B

Features

Execute Disable Bit	Y
Market segment	Server
Use conditions	Server/Enterprise
Maximum number of PCI Express lanes	80
PCI Express slots version	5.0
Supported instruction sets	AMX, SSE4.2, AVX, AVX 2.0, AVX-512
Scalability	2S
Embedded options available	N
Export Control Classification Number (ECCN)	5A992C
Commodity Classification	G180729

Automated Tracking System (CCATS)

Processor

Processor manufacturer	Intel
Processor generation	Intel Xeon Scalable 4th Gen
Processor model	6438M
Processor base frequency	2.2 GHz
Processor family	Intel® Xeon® Gold
Processor cores	32
Processor socket	LGA 4677 (Socket E)
Processor threads	64
System bus rate	16 GT/s
Processor operating modes	64-bit
Processor boost frequency	3.9 GHz
High priority cores	12
High priority core frequency	2.3 GHz
Low priority cores	20
Low priority core frequency	1.8 GHz
Processor cache	60 MB
Thermal Design Power (TDP)	205 W
Box	N
Stepping	S3
Processor codename	Sapphire Rapids
Processor ARK ID	232398

Processor special features

Intel® Hyper Threading Technology (Intel® HT Technology)	Y
Intel® Turbo Boost Technology	2.0
Intel® AES New Instructions (Intel® AES-NI)	Y
Intel Trusted Execution Technology	Y
Intel® Speed Shift Technology	Y
Intel® Transactional Synchronization Extensions	Y
Intel® Total Memory Encryption	Y
Intel® Control-flow Enforcement Technology (CET)	Y
Intel® Crypto Acceleration	Y
Intel® Platform Firmware Resilience Support	Y
Maximum Enclave Size Support for Intel® SGX	128 GB
Intel VT-x with Extended Page Tables (EPT)	Y
Intel® OS Guard	Y
Intel Software Guard Extensions (Intel SGX)	Y
Intel 64	Y
Intel Virtualization Technology (VT-x)	Y
Intel Virtualization Technology for Directed I/O (VT-d)	Y
AVX-512 Fused Multiply-Add (FMA) units	2
Intel® Boot Guard	Y
Intel® Deep Learning Boost (Intel® DL Boost)	Y

Intel® Speed Select technology - Performance Profile (Intel® SST-PP)	Y
Intel® Resource Director Technology (Intel® RDT)	Y
Intel® Run Sure Technology	Y
Mode-based Execute Control (MBE)	Y
Intel® Optane™ DC Persistent Memory Supported	Y
Intel® Speed Select Technology - Base Frequency (Intel® SST-BF)	Y
Intel® QuickAssist Software Acceleration	Y
Intel® On Demand Feature Activation	Y
Intel® Data Streaming Accelerator (DSA)	1 default devices
Intel® In-memory Analytics Accelerator (IAA)	1 default devices
Intel® Advanced Matrix Extensions (AMX)	Y