Intel Xeon Silver 4410Y processor

Artikel	417728
Herstellernummer	PK8071305120002
EAN	8592978435424
Intel	

Intel® Trusted-Execution-Technik
Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt werden.

Intel® Directed-I/O-Virtualisierungstechnik (VT-d)
Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

Intel® Virtualisierungstechnik (VT-x)
Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

Intel® 64
In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

Cache
Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Intel® Turbo-Boost-Technik
Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

Max. Turbo-Taktfrequenz
Die maximale Turbo-Taktfrequenz ist die maximale Einzelkern-Taktfrequenz, zu der der Prozessor mit der Intel® Turbo-Boost-

Technik und, falls vorhanden, mit Intel® Thermal Velocity Boost betrieben werden kann. Die Frequenz wird in Gigahertz (GHz) gemessen bzw. in Milliarden Takten pro Sekunde.

Execute-Disable-Bit
Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireninfektionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

Intel® Hyper-Threading-Technik
Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

Intel® VT-x mit Extended Page Tables (EPT)
Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

Intel® Speed Shift Technology
Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduziert die Leistungsauswirkungen der allgegenwärtigen Verschlüsselung und steigert die Leistung von verschlüsselungsintensiven Workloads wie SSL-Web-Serving, 5G-Infrastruktur und VPN/Firewalls.

Intel® Software Guard Extensions (Intel®SGX)
Die Intel® Software Guard Extensions (Intel® SGX) geben Anwendungen die Möglichkeit, einen per Hardware durchgesetzten Trusted-Execution-Schutz für deren sensible Routinen und Daten einzurichten. Intel® SGX bietet Entwicklern eine Möglichkeit, Code und Daten in von der CPU gesicherten vertrauenswürdigen Umgebungen für die Programmausführung (Trusted Execution Environments, TEEs) zu partitionieren.

Intel® Deep Learning Boost (Intel® DL Boost)
Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

Befehlssatzerweiterungen
Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) schützt Daten vor dem Risiko physischer Angriffe auf den Speicher, wie Kaltstartattacken.

Anzahl der UPI-Links
Intel® Ultra Path Interconnect (UPI) Links bedeutet ein Punkt-zu-Punkt-Hochgeschwindigkeit-Interconnect-Bus zwischen den Prozessoren, der erhöhte Bandbreite und Leistung über Intel® QPI bietet.

Anzahl der AVX-512 FMA-Einheiten
Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

Intel® Resource Director Technology (Intel® RDT)
Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

Intel® Speed Select Technology – Leistungsprofil
Es besteht die Möglichkeit, den Prozessor an drei spezifischen Betriebspunkten zu konfigurieren.

MBE (Mode-based Execute Control, modusbasierte Ausführungssteuerung)
Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

Intel® Boot Guard

Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und bösartigen Softwareangriffen vor der Aktivierung des Betriebssystem bei.

Intel® Control-Flow Enforcement Technology
CET – Intel Control-Flow Enforcement Technology (CET) schützt vor dem Missbrauch legitimer Code-Ausschnitte durch ROP-Angriffe (return-oriented programming) zur Übernahme der Kontrollstruktur.

Intel® TSX-NI
Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die verbesserte Steuerung von Locks in Software.

Zusammenfassung

Intel® Trusted-Execution-Technik
Die Intel® Trusted-Execution-Technik erhöht die Sicherheit von PCs. Sie umfasst eine Reihe von Hardware-Erweiterungen für Intel® Prozessoren und Chipsätze, die zusätzliche Sicherheitsfunktionen für die digitale Büroplattform bereitstellen, wie das sichere Starten von Systemprogrammen und des Betriebssystems und das Ausführen von Anwendungen in einem geschützten Bereich. Dies ermöglicht eine Umgebung, in der Anwendungen auf einem eigenen, von aller anderen Software des Systems abgeschotteten Bereich ausgeführt werden.

Intel® Directed-I/O-Virtualisierungstechnik (VT-d)
Die Intel® Directed-I/O-Virtualisierungstechnik (VT-d) setzt die bestehende Unterstützung von Virtualisierungslösungen für die IA-32 (VT-x) und Systeme mit Itanium® Prozessoren (VT-i) fort und erweitert diese um neue Unterstützung für die I/O-Gerätevirtualisierung. Die Intel VT-d kann Benutzern helfen, die Sicherheit und Zuverlässigkeit von Systemen sowie die Leistung von I/O-Geräten in virtualisierten Umgebungen zu verbessern.

Intel® Virtualisierungstechnik (VT-x)
Mit der Intel® Virtualisierungstechnik (VT-x) kann eine Hardwareplattform als mehrere „virtuelle“ Plattformen eingesetzt werden. Sie bietet verbesserte Verwaltbarkeit durch weniger Ausfallzeiten und eine Beibehaltung der Produktivität, indem die Rechenvorgänge in separate Partitionen verschoben werden.

Intel® 64
In Verbindung mit der entsprechenden Software ermöglicht die Intel® 64 Architektur die 64-Bit-Verarbeitung bei Servern, Workstations, PCs und Mobilplattformen.[1] Intel 64 verbessert die Leistung, da das System durch diese Prozessorerweiterung mehr als 4 GB virtuellen und physischen Speicher adressieren kann.

Cache
Der CPU-Cache ist ein Bereich des schnellen Speichers, der sich im Prozessor befindet. Intel® Smart-Cache bezieht sich auf die Architektur, die ermöglicht, dass alle Kerne den Zugriff auf den Last-Level-Cache dynamisch teilen.

Intel® AES New Instructions
Intel® AES New Instructions (Intel® AES-NI) ist eine Zusammenstellung von Anweisungen zur schnellen und sicheren Verschlüsselung und Entschlüsselung von Daten. AES-NI sind wertvolle Komponenten für kryptografische Anwendungen, z. B. für: Anwendungen zur Massenverschlüsselung/-entschlüsselung, Authentifizierung, Generierung von zufälligen Nummern und Authentifizierungsverschlüsselung.

Intel® Turbo-Boost-Technik
Die Intel® Turbo-Boost-Technik erhöht dynamisch die Frequenz eines Prozessors nach Bedarf, indem die Temperatur- und Leistungsreserven ausgenutzt werden, um bei Bedarf mehr Geschwindigkeit und andernfalls mehr Energieeffizienz zu bieten.

Max. Turbo-Taktfrequenz
Die maximale Turbo-Taktfrequenz ist die maximale Einzelkern-Taktfrequenz, zu der der Prozessor mit der Intel® Turbo-Boost-Technik und, falls vorhanden, mit Intel® Thermal Velocity Boost betrieben werden kann. Die Frequenz wird in Gigahertz (GHz) gemessen bzw. in Milliarden Takten pro Sekunde.

Execute-Disable-Bit
Die Execute-Disable-Bit ist eine hardwarebasierte Sicherheitsfunktion, die das Risiko von Vireninfektionen verringert und verhindern kann, dass bösartige Software auf dem Server bzw. im Netzwerk ausgeführt wird.

Intel® Hyper-Threading-Technik
Die Intel® Hyper-Threading-Technik ermöglicht zwei Verarbeitungs-Threads pro physischem Kern. Anwendungen mit vielen Threads können mehr Aufgaben parallel erledigen und Tasks früher beenden.

Intel® VT-x mit Extended Page Tables (EPT)
Intel® VT-x mit Extended Page Tables (EPT), auch bekannt als Second Level Address Translation (SLAT), beschleunigt speicherintensive Virtualisierungsanwendungen. Der Einsatz von Extended Page Tables bei Plattformen mit Intel® Virtualisierungstechnik reduziert die Gesamtkosten für Speicher und Stromversorgung und erhöht die Akkulaufzeit durch Hardwareoptimierung der Seitentabellenverwaltung.

Intel® Speed Shift Technology
Die Intel® Speed Shift Technology nutzt hardware-gesteuerte P-Stati, um mit vorübergehenden Single-Thread-Workloads von kurzer Dauer (wie beim Browsen im Internet) eine bedeutend schnellere Reaktionszeit zu erzielen. Dazu wird es dem Prozessor ermöglicht, die jeweils beste Betriebsfrequenz und Spannung zu wählen, um optimale Leistung und Energieeffizienz zu erzielen.

Intel® Crypto Acceleration
Intel® Crypto Acceleration reduziert die Leistungsauswirkungen der allgegenwärtigen Verschlüsselung und steigert die Leistung von verschlüsselungsintensiven Workloads wie SSL-Web-Serving, 5G-Infrastruktur und VPN/Firewalls.

Intel® Software Guard Extensions (Intel®SGX)
Die Intel® Software Guard Extensions (Intel® SGX) geben Anwendungen die Möglichkeit, einen per Hardware durchgesetzten Trusted-Execution-Schutz für deren sensible Routinen und Daten einzurichten. Intel® SGX bietet Entwicklern eine Möglichkeit, Code und Daten in von der CPU gesicherten vertrauenswürdigen Umgebungen für die Programmausführung (Trusted Execution Environments, TEEs) zu partitionieren.

Intel® Deep Learning Boost (Intel® DL Boost)
Ein neuer Satz mit Embedded-Prozessor-Technologien zur Beschleunigung von KI-Deep-Learning-Anwendungsfällen. Damit wird Intel AVX-512 mit einer neuen VNNI (Vector Neural Network Instruction) erweitert, welche die Deep-Learning-Leistung im Vergleich zu früheren Generationen bedeutend verbessert.

Befehlssatzerweiterungen
Befehlssatzerweiterungen sind zusätzliche Anweisungen zur Erhöhung der Leistung, wenn die gleichen Vorgänge auf mehreren Datenobjekten ausgeführt werden. Diese können SSE (Streaming SIMD Extensions) und AVX (Advanced Vector Extensions) umfassen.

Intel® Total Memory Encryption
TME – Total Memory Encryption (TME) schützt Daten vor dem Risiko physischer Angriffe auf den Speicher, wie Kaltstartattacken.

Anzahl der UPI-Links
Intel® Ultra Path Interconnect (UPI) Links bedeutet ein Punkt-zu-Punkt-Hochgeschwindigkeit-Interconnect-Bus zwischen den Prozessoren, der erhöhte Bandbreite und Leistung über Intel® QPI bietet.

Anzahl der AVX-512 FMA-Einheiten
Intel® Advanced Vector Extensions 512 (AVX-512) sind neue Anleitungssatzerweiterungen, die Ultra-Breitband (512 Bit) Vektorbetriebsfunktionalitäten mit bis zu 2 FMAs („Fused Multiply Add“-Anweisungen) zur Beschleunigung Ihrer anspruchsvollsten rechnergestützten Aufgaben bieten.

Intel® Resource Director Technology (Intel® RDT)
Intel® Resource Director Technology (Intel® RDT) ermöglicht bessere Transparenz und Kontrolle der Verwendung gemeinsam genutzter Ressourcen durch Anwendungen, virtuelle Maschinen (VMs) und Container – zum Beispiel Last-Level-Cache (LLC) und Speicherbandbreite.

Intel® Speed Select Technology – Leistungsprofil
Es besteht die Möglichkeit, den Prozessor an drei spezifischen Betriebspunkten zu konfigurieren.

MBE (Mode-based Execute Control, modusbasierte Ausführungssteuerung)
Modusbasierte Ausführungssteuerung kann die Integrität des Codes auf Kernel-Ebene zuverlässiger verifizieren und durchsetzen.

Intel® Boot Guard
Die Intel® Device Protection Technology mit Boot Guard trägt zum Schutz der Umgebung vor Viren und bösartigen Softwareangriffen vor der Aktivierung des Betriebssystem bei.

Intel® Control-Flow Enforcement Technology
CET – Intel Control-Flow Enforcement Technology (CET) schützt vor dem Missbrauch legitimer Code-Ausschnitte durch ROP-Angriffe (return-oriented programming) zur Übernahme der Kontrollstruktur.

Intel® TSX-NI
Bei den Intel® Transactional Synchronization Extensions New Instructions (Intel® TSX-NI) handelt es sich um eine Reihe von Anweisungen für die Multithread-Leistungsskalierung. Diese Technik verbessert die Effizienz bei parallelen Vorgängen durch die

verbesserte Steuerung von Locks in Software.

Intel Xeon Silver 4410Y, Intel® Xeon Silver, LGA 4677 (Socket E), Intel, 4410Y, 2 GHz, Intel Xeon Scalable 4th Gen

Intel Xeon Silver 4410Y. Prozessorfamilie: Intel® Xeon Silver, Prozessorsockel: LGA 4677 (Socket E), Prozessorhersteller: Intel. Speicherkanäle: Okta-Kanal, Maximaler interner Speicher, vom Prozessor unterstützt: 6 TB, Speichertypen, vom Prozessor unterstützt: DDR4-SDRAM. Marktsegment: Server, Nutzungsbedingungen: Server/Enterprise, Unterstützte Befehlssätze: AMX, SSE4.2, AVX, AVX 2.0, AVX-512. Unterstützung der maximalen Enklavengröße für Intel® SGX: 64 GB, Intel® Data Streaming Accelerator (DSA): 1 default devices. Verpackungsart: Einzelhandels-Box

Merkmale

Gewicht und Abmessungen

Prozessor-Paketgröße	77.5 x 56.5 mm

Logistikdaten

Warentarifnummer (HS)	8542310001

Sonstige Funktionen

RAM-Speicher maximal	4 TB

Verpackungsdaten

Verpackungsart	Einzelhandels-Box

Betriebsbedingungen

Tcase	78 °C
DTS Max	93 °C

Grafik

Eingebaute Grafikadapter	Nein
Separater Grafikadapter	Nein
Eingebautes Grafikkartenmodell	Nicht verfügbar
Separates Grafikkartenmodell	Nicht verfügbar

Speicher

Maximaler interner Speicher, vom Prozessor unterstützt	6 TB
Speichertypen, vom Prozessor unterstützt	DDR4-SDRAM
Speicherkanäle	Okta-Kanal
ECC	Ja

Technische Details

Startdatum	Q1'23
Status	Launched
Unterstützte Arbeitsspeicher	DDR4-SDRAM
Speichergeschwindigkeit (max.)	4000 MHz
Anzahl der UPI-Links	2
Paketträger	E1B

Merkmale

Execute Disable Bit	Ja
Marktsegment	Server
Nutzungsbedingungen	Server/Enterprise
Maximale Anzahl der PCI-Express-Lanes	80
PCI-Express-Slots-Version	5.0
Unterstützte Befehlssätze	AMX, SSE4.2, AVX, AVX 2.0, AVX-512
Skalierbarkeit	2S
Eingebettete Optionen verfügbar	Ja
Exportkontroll-Klassifizierungsnummer (ECCN)	5A992C
Warenklassifizierungssystem zur automatisierten Nachverfolgung (CCATS)	G180729

Prozessor

Prozessorhersteller	Intel
Prozessorgeneration	Intel Xeon Scalable 4th Gen
Prozessor	4410Y
Grundfrequenz des Prozessors	2 GHz
Prozessorfamilie	Intel® Xeon Silver
Anzahl Prozessorkerne	12
Prozessorsockel	LGA 4677 (Socket E)
Prozessor-Threads	24
Systembus-Rate	16 GT/s
Prozessor Boost-Frequenz	3,9 GHz

Prozessor-Cache	30 MB
Thermal Design Power (TDP)	150 W
Box	Nein
Stepping	S3
Prozessor Codename	Sapphire Rapids
ARK Prozessorerkennung	232376

Prozessor Besonderheiten

Intel® Hyper-Threading-Technik (Intel® HT Technology)	Ja
Intel® Turbo-Boost-Technologie	2.0
Intel® AES New Instructions (Intel® AES-NI)	Ja
Intel® Trusted-Execution-Technik	Ja
Intel®-Speed-Shift-Technologie	Ja
Intel® Transactional Synchronization Extensions	Ja
Intel® Total Memory Encryption	Ja
Intel® Control-flow Enforcement Technology (CET)	Ja
Intel® Crypto-Beschleunigung	Ja
Unterstützung der Intel® Plattform-Firmware Resilience	Ja
Unterstützung der maximalen Enklavengröße für Intel® SGX	64 GB
Intel® VT-x mit Extended Page Tables (EPT)	Ja
Intel® OS Guard	Ja
Intel® Software Guard Extensions (Intel® SGX)	Ja
Intel® 64	Ja
Intel® Virtualization Technologie (VT-X)	Ja
Intel® Virtualisierungstechnik für direkte I/O (VT-d)	Ja
AVX-512 Abgesicherte Multiply-Add (FMA) Einheiten	2
Intel® Boot Guard	Ja
Intel® Deep Learning Boost (Intel® DL Boost) on CPU	Ja
Intel® Speed Select-Technologie - Leistungsprofil (Intel® SST-PP)	Ja
Intel® Resource Director Technology (Intel® RDT)	Ja
Modusbasierte Execute Control (MBE)	Ja
Intel® QuickAssist Software Acceleration	Ja
Aktivierung von Intel® On Demand-Funktionen	Ja
Intel® Data Streaming Accelerator (DSA)	1 default devices
Intel® Advanced Matrix Extensions (AMX)	Ja

Preisänderungen und Irrtümer vorbehalten. Alle Produkte solange der Vorrat reicht.