Содержание

PC

https://en.wikipedia.org/wiki/List_of_Intel_processors

https://en.wikipedia.org/wiki/List_of_Intel_CPU_microarchitectures

https://en.wikipedia.org/wiki/List_of_Intel_chipsets

https://en.wikipedia.org/wiki/List_of_Intel_codenames

https://linuxreviews.org/The_Massive_Intel_Leak:_The_Files_It_Contains_And_Their_Content

https://en.wikipedia.org/wiki/List_of_Intel_Xeon_chipsets

https://en.wikipedia.org/wiki/List_of_Intel_Xeon_processors

CoffeTime	https://forums.overclockers.ru/viewtopic.php?f=1&t=602278&start=12640
Модификация UEFI BIOS. Софт для работы.	https://forums.overclockers.ru/viewtopic.php?f=25&t=479847
CPU microcode archive	https://www.win-raid.com/t5709f47-OFFER-Intel-CPU-Microcode-Archives.html

Intel x86 microarchitectures

x86 microarchitectures

Year	Micro-<wbr />architecture	Pipeline stages	Max clock (MHz)	Process node
1978	8086 (8086, 8088)	2	5	3000 nm
1982	186 (80186, 80188)	2	25	
1982	286 (80286)	3	25	1500 nm
1985	386 (80386)	6	33	
1989	486 (80486)	5	100	1000 nm
1993	P5 (Pentium)	5	200	800, 600, 350 nm
1995	P6 (Pentium Pro, Pentium II)	14 (17 with load & store/retire)	450	500, 350, 250 nm
1997	P5 (Pentium MMX)	6	233	350 nm
1999	P6 (Pentium III)	12 (15 with load & store/retire)	1400	250, 180, 130 nm
2000	NetBurst (Pentium 4) (Willamette)	20 unified with branch prediction	2000	180 nm
2002	NetBurst (Pentium 4) (Northwood, Gallatin)		3466	130 nm
2003	Pentium M (Banias, Dothan) Enhanced Pentium M (Yonah)	10 (12 with fetch/retire)	2333	130, 90, 65 nm
2004	NetBurst (Pentium 4, Pentium D) (Prescott)	31 unified with branch prediction	3800	90, 65 nm
2006	Intel Core	12 (14 with fetch/retire)	3000	65 nm
2007	Penryn (die shrink)		3333	
2008	Nehalem	20 unified (14 without miss prediction)	3600	45 nm
	Bonnell	16 (20 with prediction miss)	2100	

2010	Westmere (die shrink)	20 unified (14 without miss prediction)	3866	32 nm
2011	*Saltwell (die shrink)*	16 (20 with prediction miss)	2130	
2012	Sandy Bridge	14 (16 with fetch/retire)	4000	
	Ivy Bridge (die shrink)		4100	
2013	*Silvermont*	14–17 (16–19 with fetch/retire)	2670	22 nm
2014	Haswell	14 (16 with fetch/retire)	4400	
	Broadwell (die shrink)		3700	
2015	*Airmont (die shrink)*	14–17 (16–19 with fetch/retire)	2640	
	Skylake	14 (16 with fetch/retire)	5200	14 nm
2016	*Goldmont*	20 unified with branch prediction	2600	
2017	*Goldmont Plus*	20 unified with branch prediction (?)	2800	
2018	Palm Cove	14 (16 with fetch/retire)	3200	
2019	Sunny Cove	14–20 (misprediction)	4100	10 nm
2020	*Tremont*	20 unified	3300	
	Willow Cove	14 unified	5300	
	Cypress Cove	14 unified	5300	14 nm
2021	Golden Cove	12 unified	5500	
	Gracemont	20 unified with misprediction penalty	4300	Intel 7
2022	Raptor Cove	12 unified	6000	
2023	Redwood Cove			Intel 4
	Crestmont			

Note: Atom/Power efficient microarchitectures are in *Italic*

Roadmap

Pentium 4 / Core roadmap

Fabrication process]]	Micro-architecture	Code names	Core generation	Xeon Scalable generation	Release date	Processors				
						Desktop	Mobile	Enthusiast /WS	2P Server/WS	4P/8P Server

180 nm	P6, NetBurst	Willamette	-	-	2000-11-20	Willamette	-		Foster	Foster MP
130 nm		Northwood/ Mobile Pentium 4 Banias			2002-01-07	Northwood	Northwood Mobile Banias	Northwood-XE	Prestonia Gallatin	Gallatin
90 nm		Prescott Dothan			2004-02-01	Prescott Smithfield	Dothan	Prescott 2M-XE Smithfield-XE	Nocona Irwindale Paxville	Potomac Cranford Paxville
65 nm		Cedar Mill Yonah Presler	Core (Yonah only)		2006-01-05	Cedar Mill Presler	Yonah	Presler-XE	Dempsey Sossaman	Tulsa
45 nm	Core	Merom	Core 2		2006-07-27	Conroe	Merom	Kentsfield	Woodcrest Clovertown	Tigerton
		Penryn			2007-11-11	Wolfdale	Penryn	Yorkfield	Harpertown	Dunnington
	Nehalem	Nehalem	Previous (Core i)		2008-11-17	Lynnfield	Clarksfield	Bloomfield	Gainestown	Beckton
		Westmere			2010-01-04	Clarkdale	Arrandale	Gulftown	Westmere-EP	Westmere-EX
32 nm	Sandy Bridge	Sandy Bridge	2 (Core i)		2011-01-09	Sandy Bridge	Sandy Bridge-M	Sandy Bridge-E	Sandy Bridge-EP	-
		Ivy Bridge	3		2012-04-29	Ivy Bridge	Ivy Bridge-M	Ivy Bridge-E	Ivy Bridge-EP	Ivy Bridge-EX
22 nm	Haswell	Haswell	4	-	2013-06-02	Haswell-DT	Haswell-MB Haswell-H Haswell-ULP/ULX	Haswell-E	Haswell-EP	Haswell-EX
		Devil's Canyon			2014-06	Haswell-DT		-		
	Skylake	Broadwell	5		2014-09-05	Broadwell-DT	Broadwell-H Broadwell-U Broadwell-Y	Broadwell-E	Broadwell-EP	Broadwell-EX
		Skylake	6	1	2015-08-05	Skylake-S	Skylake-H Skylake-U Skylake-Y	Skylake-X Skylake-W	Skylake-SP (formerly Skylake-EP/-EX)	
		Kaby Lake	7 / 8	-	2016-10	Kaby Lake-S	Kaby Lake-G Kaby Lake-H Kaby Lake-U Kaby Lake-Y	Kaby Lake-X <ref name=«auto» />	-	
		Coffee Lake	8 / 9		2017-10	Coffee Lake-S	Coffee Lake-B Coffee Lake-H Coffee Lake-U	Coffee Lake-W		
14 nm		Whiske Lake	8	-	2018-08-28	-	Whiskey Lake-U		-	
		Amber Lake	8 / 10				Amber Lake-Y			
		Cascade Lake	-	2	2019-04-02		-	Cascade Lake-X Cascade Lake-W Cascade Lake-SP	Cascade Lake-SP	
		Comet Lake	10	-	2019-09	Comet Lake-S	Comet Lake-H Comet Lake-U	Comet Lake-W	-	
		Cooper Lake	-	3	2020-06		-			Cooper Lake-SP
	Cypress Cove	Rocket Lake	11	-	2021-03	Rocket Lake-S	-	Rocket Lake	-	
	Palm Cove	Cannon Lake	8	-	2018-05		Cannon Lake-U		-	
10 nm	Sunny Cove	Ice Lake	10	3	2019-09 (mobile) 2021-04 (server)	-	Ice Lake-U	Ice Lake-W	Ice Lake-SP	-
	Willow Cove	Tiger Lake	11	-	2020-09		Tiger Lake-H Tiger Lake-H35 Tiger Lake-UP3 Tiger Lake-UP4		-	
	Golden Cove	Alder Lake (hybrid)	12		2021-11-04	Alder Lake-S	Alder Lake-H Alder Lake-P Alder Lake-U			
		Sapphire Rapids	-	4	2023-01-10		-	Sapphire Rapids-WS	Sapphire Rapids-SP	
Intel 7	Raptor Cove	Raptor Lake	13 / 14	-	2022-10-20	Raptor Lake-S	Raptor Lake-HX Raptor Lake-H Raptor Lake-P Raptor Lake-U		-	
		Emerald Rapids	-	5	2023-12-14		-	TBA	Emerald Rapids-SP	
Intel 4	Redwood Cove	Meteor Lake	Core Ultra Series 1	-	2023-12-14	N/A	Meteor Lake-H Meteor Lake-U		-	

Intel 3		Granite Rapids	-	6	2024		-		TBA	Granite Rapids-SP
Intel 20A	TBA	Arrow Lake	Core Ultra	-	2024	N/A	TBA	TBA	-	
		Lunar Lake			2024					
Intel 18A		Panther Lake			2025		TBA			

Fabrication process	Micro-architecture	Code names	Core generation	Xeon Scalable generation	Release date	Desktop	Mobile	Enthusiast /WS	2P Server/WS	4P/8P Server
						Processors				

Atom lines

https://en.wikipedia.org/wiki/List_of_Intel_Atom_processors

Atom roadmap

Fabri-cation process	Micro-archi-tecture	Release date	Processors/SoCs							
			Mobile Internet device MID, smartphone	Tablet	Netbook	Nettop	Embedded	Server	Communication	Consumer Electronics, CE
45 nm	Bonnell	2008	Silverthorne	-	Diamondville		Tunnel Creek, Stellarton	-	-	Sodaville
		2010	Lincroft		Pineview					Groveland
32 nm	Saltwell	2011	Medfield (Penwell & Lexington), Clover Trail+ (Cloverview)	Clover Trail (Cloverview)	Cedar Trail (Cedarview)		-	Centerton & Briarwood	-	Berryville
22 nm	Silvermont	2013	Merrifield (Tangier)	Bay Trail-T (Valleyview)	Bay Trail-M (Valleyview)	Bay Trail-D (Valleyview)	Bay Trail-I (Valleyview)	Avoton	Rangeley	-
14 nm	Airmont	2014	Binghamton & Riverton	Cherry Trail-T (Cherryview)	Braswell			~~Denverton~~	-	-
	Goldmont	2016	~~Broxton~~	~~Willow Trail~~ Apollo Lake	Apollo Lake			Denverton	-	-
	Goldmont Plus	2017	-	-	Gemini Lake			-	-	-
10 nm	Tremont	2020	-	Lakefield (hybrid)	Lakefield (hybrid)			Jacobsville Parker Ridge	-	-
Intel 7	Gracemont	2021	-	-	Alder Lake (hybrid)			-	-	-
Intel 4	Crestmont	2023	-	-	Meteor Lake (hybrid)			Grand Ridge	-	-
Intel 3	Crestmont	2024	-	-	-	-	-	Sierra Forest-AP	-	-
Intel 20A	Skymont	2024	-	-	Arrow Lake (hybrid)			-	-	-
Intel 18A	Darkmont	2025	-	-	-	-	-	Clearwater Forest-AP	-	-

Tremont-Embedded-Elkhart Lake

List of embedded processors as follows: Products formerly Elkhart Lake

Part Name	RCP,$	Price	Cores (threads)	TDP	Processor branding & model	TA	PSE	IHS	IBECC	TCC	Target segment	GPU model		CPU clock rate base	CPU clock rate turbo	Graphics clock rate base	Graphics clock rate turbo	Memory	Ordering Code
J6413	64	66.4	4	10 W	Celeron	0...70	+	-	-	-	PC Client	UHD Graphics	16 EU	1.8 GHz	3.0 GHz	400 MHz	800 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	DC8070304190822
J6412	64	57.8	4	10 W	Celeron	0...70	-	-	-	-	PC Client	UHD Graphics	16 EU	2.0 GHz	2.6 GHz	400 MHz	800 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	DC8070304190881
J6426	96		4	10 W	Pentium	0...70	+	-	-	-	PC Client	UHD Graphics	32 EU	1.8 GHz	3.0 GHz	400 MHz	850 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	DC8070304190882

Part Name	RCP,$	Price	Cores (threads)	TDP	Processor branding & model	TA	PSE	IHS	IBECC	TCC	Target segment	GPU model		CPU clock rate base	CPU clock rate turbo	Graphics clock rate base	Graphics clock rate turbo	Memory	Ordering Code
N6211	64		2	6.5 W	Celeron	0…70	+	-	-	-	PC Client	UHD Graphics	16 EU	1.2 GHz	3.0 GHz	250 MHz	750 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	DC8070304190819
N6210	64	52	2	6.5 W	Celeron	0…70	-	-	-	-	PC/Client/Tablet	UHD Graphics	16 EU	1.2 GHz	2.6 GHz	250 NHz	750 MHz	4 × LPDDR4X-3200 2 × DDR4-3200	DC8070304190883
N6415	96	102.5	4	6.5 W	Pentium	0…70	+	-	-	-	PC Client	UHD Graphics	16 EU	1.2 GHz	3.0 GHz	350 MHz	800 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	DC8070304190820
x6211E	42	66.5	2	6 W	Atom	-40…85	+	+	+	-	Embedded	UHD Graphics	16 EU	1.2 GHz	3.0 GHz	350 MHz	750 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304243807
x6413E	51	75	4	9 W	Atom	-40…85	+	+	+	-	Embedded	UHD Graphics	16 EU	1.5 GHz	3.0 GHz	500 MHz	750 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304243865
x6425E	67	99.7	4	12 W	Atom	-40…85	+	+	+	-	Embedded	UHD Graphics	32 EU	1.8 GHz	3.0 GHz	500 MHz	750 MHz	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304243808
x6212RE	45		2	6 W	Atom	-40…85	+	+	+	+	Industrial	UHD Graphics	16 EU	1.2 GHz	-	350 MHz	-	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304243808
x6214RE	47		2	6 W	Atom	-40…85	+	+	+	+	Industrial	UHD Graphics	16 EU	1.4 GHz	-	400 MHz	-	4 × LPDDR4X-3200 2 × DDR4-3200	FH8070304289531
x6414RE	55		4	9 W	Atom	-40…85	+	+	+	+	Industrial	UHD Graphics	16 EU	1.5 GHz	-	400 MHz	-	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304289591
x6416RE	63		4	9 W	Atom	-40…85	+	+	+	+	Industrial	UHD Graphics	16 EU	1.7 GHz	-	450 MHz	-	4 × LPDDR4X-3200 2 × DDR4-3200	FH8070304289532
x6425RE	71		4	12 W	Atom	-40…85	+	+	+	+	Industrial	UHD Graphics	32 EU	1.9 GHz	-	400 MHz	-	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304289558
x6427FE	83		4	12 W	Atom	-40…85	+	+	+	+	FuSa Industrial	UHD Graphics	32 EU	1.9 GHz	-	400 MHz	-	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304289690
x6200FE	45		2	4.5 W	Atom	-40…85	+	+	+	+	FuSa Industrial	-	-	1.0 GHz	-	-	-	4 × LPDDR4X-4267 2 × DDR4-3200	FH8070304289582

Motherboards

supermicro	x13dai-t	page	datasheet

Desktop processors

Codename	Desktop Name	Socket Name	Gen
SKL	Sky Lake	LGA 1151 LGA 2066 LGA 3647	6
KBL	Kaby Lake	LGA 1151 LGA 2066	7
CFL	Coffe Lake	LGA 1151	8
CFL	Coffe Lake Refresh	LGA 1151	9
CML	Comet Lake	LGA 1200	10
RKL	Rocket Lake	LGA 1200	11
ADL	Alder Lake	LGA 1700	12
RPL	Raptor Lake	LGA 1700	13
MTL	Meteor Lake		

PCH

PCH Name	Chipset Series		
Ibex Peak	5	Lynnfield and Clarkdale	https://en.wikipedia.org/wiki/Intel_5_Series
Cougar Point	6	Sandy Bridge	https://en.wikipedia.org/wiki/LGA_1155#Sandy_Bridge_family_of_chipsets
Panther Point	7	Ivy Bridge	https://en.wikipedia.org/wiki/LGA_1155#Ivy_Bridge_family_of_chipsets
Lynx Point	8/9	Haswell / Broadwell	https://en.wikipedia.org/wiki/LGA_1150#Haswell_chipsets
Sunrise Point	100	Sky Lake	https://en.wikipedia.org/wiki/LGA_1151#Skylake_chipsets_(100_series)
Union Point	200	Kaby Lake	https://en.wikipedia.org/wiki/LGA_1151#Kaby_Lake_chipsets_(200_series)
Cannon Point	300	Coffee Lake	https://en.wikipedia.org/wiki/LGA_1151#Coffee_Lake_chipsets_(300_series_and_C240_series)
	400	Comet Lake	https://en.wikipedia.org/wiki/LGA_1200#Comet_Lake_chipsets_(400_series)
	500	Rocket Lake	https://en.wikipedia.org/wiki/LGA_1200#Rocket_Lake_chipsets_(500_series)
	600	Alder Lake	https://en.wikipedia.org/wiki/LGA_1700#Alder_Lake_chipsets_(600_series)
	700	Raptor Lake	https://en.wikipedia.org/wiki/LGA_1700#Raptor_Lake_chipsets_(700_series)

Embedded controller

https://github.com/intel/ecfw-zephyr

BIOS

https://www.sentinelone.com/labs/moving-from-common-sense-knowledge-about-uefi-to-actually-dumping-uefi-firmware/

https://malware.news/t/moving-from-manual-reverse-engineering-of-uefi-modules-to-dynamic-emulation-of-uefi-firmware/43799

https://edk2-docs.gitbook.io/edk-ii-uefi-driver-writer-s-guide/

https://github.com/LongSoft/UEFITool

https://github.com/LongSoft/UEFITool/blob/new_engine/common/guids.csv

https://github.com/theopolis/uefi-firmware-parser

https://github.com/erocarrera/pefile

https://formats.kaitai.io/uefi_te/python.html

https://github.com/intel/FSP

ME

https://github.com/platomav/MEAnalyzer/

https://comsystem-tlt.ru/obzori/me-txe-region

https://winraid.level1techs.com/t/intel-cs-management-engine-drivers-firmware-and-tools-2-15/30719

DEBUG

https://github.com/ptresearch/IntelTXE-PoC/blob/master/README.md

http://standa-note.blogspot.com/2021/03/debugging-system-with-dci-and-windbg.html

APIC

https://wiki.osdev.org/APIC

Intel® 64 and IA-32 Architectures Software Developer's Manual

Volume 1: Basic Architecture
Volume 2A: Instruction Set Reference, A-L
Volume 2B: Instruction Set Reference, M-U
Volume 2C: Instruction Set Reference, V
Volume 2D:Instruction Set Reference, W-Z
Volume 3A: System Programming Guide, Part 1
Volume 3B: System Programming Guide, Part 2
Volume 3C: System Programming Guide, Part 3
Volume 3D: System Programming Guide, Part 4
Volume 4: Model-Specific Registers

MultiProcessor Specification

Acronyms

https://doc.coreboot.org/acronyms.html

ACM	Authenticated Code Modules		https://doc.coreboot.org/security/intel/acm.html
ACPI	Advanced Configuration and Power Interface		https://en.wikipedia.org/wiki/ACPI
AL	After life	UEFI boot phase	
AMT	Active Management Technology		https://en.wikipedia.org/wiki/Intel_Active_Management_Technology

APIC	Advanced Programmable Interrupt Controller		https://en.wikipedia.org/wiki/Advanced_Programmable_Interrupt_Controller
ARM	Advanced RISC Machines		https://en.wikipedia.org/wiki/ARM_architecture_family
BDS	Boot Device Selection	UEFI boot phase	
BFV	Boot Firmware Volume	UEFI	
BIOS	Basic Input/Output System		https://en.wikipedia.org/wiki/BIOS
BKC	Best Known Configuration		
BMC	Baseboard management controller		https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface#Baseboard_management_controller
BTX	Balanced Technology Extended Interface	intel	
CAR	Cache-as-RAM		
CBFS	coreboot file system	coreboot	
CCT	Intel® Clock Commander	Tool found in BKC Intel® CSME kit	
CDI			
CPU	Central processing unit		https://en.wikipedia.org/wiki/Central_processing_unit
CSME	Converged Security and Management Engine	intel	
DMI	Direct Media Interface	intel	https://en.wikipedia.org/wiki/Direct_Media_Interface
DTS	digital thermal sensors		
DXE	The Driver Execution Environment	UEFI boot phase	
EC	Embedded controller		https://en.wikipedia.org/wiki/Embedded_controller
EOP	End-of-POST	Message	
FDI	Flexible Display Interface	intel	https://en.wikipedia.org/wiki/Flexible_Display_Interface
FFS	Firmware File System	UEFI	
FIT	Intel® Flash Image Tool	intel	
FV	firmware volume	UEFI	
GOP			
GUID	Globally Unique Identifier		
HECI	Host Embedded Controller Interface		https://en.wikipedia.org/wiki/Host_Embedded_Controller_Interface
HID	Human interface device		https://en.wikipedia.org/wiki/Human_interface_device
HLK		intel HLK Validation	
HOB	Hand-Off Block		
HSIO	High Speed Input/Output		
IBB	Initial Boot Block	coreboot	https://doc.coreboot.org/security/intel/txt_ibb.html
ICH	I/O Controller Hub		https://en.wikipedia.org/wiki/I/O_Controller_Hub

ILM	Independent Loading Mechanism	intel mb	
IOC	Intel Online Connect		
IPC	Instructions per cycle		https://en.wikipedia.org/wiki/Instructions_per_cycle
IRQ	Interrupt request		https://en.wikipedia.org/wiki/Interrupt_request_(PC_architecture)
ITSS	interrupt and timer subsystem		
KOZ	Keepout Zones	intel mb	
KSC			
ME	Intel Management Engine		https://en.wikipedia.org/wiki/Intel_Management_Engine
MIPS	Microprocessor without Interlocked Pipelined Stages		https://en.wikipedia.org/wiki/MIPS_architecture
MMU	Memory management unit		https://en.wikipedia.org/wiki/Memory_management_unit
OPI	On Package DMI interconnect Interface		
PCH	Platform Controller Hub		https://en.wikipedia.org/wiki/Platform_Controller_Hub
PCL	Platform Component List	intel	
PCT	Intel® Platform Configuration Tool		
PD	Power Delivery		
PE	Portable Executable	file format	
PECI	Platform Environment Control Interface		https://en.wikipedia.org/wiki/Platform_Environment_Control_Interface
PEI	The Pre-EFI Initialization	UEFI boot phase	
PEIM	Pre-EFI Initialization Module	UEFI	
PFAT			
PMC	Power Management Controller	intel	
PPI	PEIM-to-PEIM Interface	UEFI	
PV	Production Version		
RT	runtime	UEFI boot phase	
SCH	System Controller Hub		https://en.wikipedia.org/wiki/System_Controller_Hub
SEC	Security phase		
SKU	Stock Keeping Unit	common	
SPI	Serial Peripheral Interface	common	https://en.wikipedia.org/wiki/Serial_Peripheral_Interface
TE	Terse Executable	UEFI file format is a stripped-down version of the PE format	https://uefi.org/sites/default/files/resources/PI_Spec_1_6.pdf
TPM	Trusted Platform Module		

TSL	Transient System Load	UEFI boot phase	
TXT	Intel Trusted Execution Technology		https://doc.coreboot.org/security/intel/txt.html
UEFI	Unified Extensible Firmware Interface		https://en.wikipedia.org/wiki/UEFI
VIP	Intel® Validation Internet Portal		

bios, x86, uefi, fsp, apic