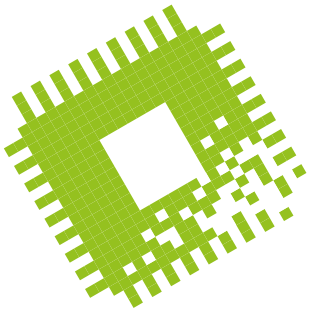
Bit-Rauschen

AMDs kommende GPU-Technik, ARM-CPUs und Intel-Lücken



AMD und Intel schauten bei öffentlichen Veranstaltungen mit Analysten weit in ihre jeweilige Zukunft. Bei Serverprozessoren kommt ARM deutlich stärker in Fahrt, während Intel weitere Lücken abdichtet.

Von Christof Windeck

Bald werden die ersten Ryzen-4000-Notebooks erwartet sowie Intels Zehnkerner Core i9-10900K alias Comet Lake-S auf neuen LGA1200-Mainboards. Aus technischer Sicht spannender sind aber Zen-3-Prozessoren, die später im Jahr wohl als „Milan"-Epycs für Server debütieren werden. Hier hat AMD klargestellt, dass der Auftragsfertiger TSMC nicht zwingend die Lithografie mit extrem-ultraviolettem (EUV-)Licht einsetzt. Das hatte man bisher erwartet, weil AMD bei Zen 2 von „7nm" und bei Zen 3 von „7nm+" gesprochen hatte. Mit letzterem meint AMD aber nur eine verbesserte 7-Nanometer-Fertigungstechnik.

AMD-CTO Mark Papermaster verriet Anfang März außerdem, dass bei Zen 4 dann 5-Nanometer-Technik zum Einsatz kommen wird – frühestens wohl 2021. Epyc-„Genoa"-Prozessoren mit Zen 4 sollen im Zwei-Exaflops-Supercomputer El Capitan rechnen, den Löwenanteil der Rechenleistung liefern darin aber Radeon-Instinct-Rechenbeschleuniger mit CDNA2-Mikroarchitektur. Mit CDNA – das „C" steht für Compute – ist eine für Rechenbeschleuniger optimierte Variante der Radeon-DNA-(RDNA-)Technik für Gaming-Grafikkarten gemeint. Die erste CDNA-Generation soll noch 2020 erscheinen, ebenso wie die zweite RDNA-Generation RDNA2. Letztere wiederum soll der von Nvidia erwarteten Ampere-GPU paroli bieten.

Den erwähnten El-Capitan-Supercomputer fertigt die HPE-Sparte Cray. Jeder Zen-4-Epyc bindet darin jeweils mehrere CDNA2-Chips an, und zwar Cache-kohärent per „Infinity Architecture", der Nachfolgerin des bisherigen Infinity Fabric. Auch Intel verspricht für den für 2021 geplanten Aurora-Supercomputer kohärente Links zwischen den „Sapphire Rapids"-Xeons und den „Ponte Vecchio"-Rechenbeschleunigern, nutzt dabei jedoch den Compute Express Link (CXL), der wiederum auf PCIe 5.0 aufsetzt.

ARM-Attacken

Die IT-Webseite Anandtech hat in der Amazon-Cloud AWS EC2 drei Server mit unterschiedlichen Prozessoren verglichen: Mit dem Intel-Platzhirsch Xeon Platinum 8259 (Cascade Lake), einem AMD Epyc der ersten Generation – der Epyc 7002 ist bei AWS noch nicht verfügbar – sowie mit dem Amazon-Eigengewächs Graviton2 mit ARM-Rechenkernen (siehe S. 38). Im Graviton2 stecken 64 Kerne vom Typ Neoverse N1, deren beeindruckende Rechenleistung Intel einige graue Haare wachsen lassen dürfte. Außerdem bringt Ampere noch den 80-Kerner Altra, der Zwei-CPU-Server mit 160 Kernen, 8 TByte RAM und PCIe 4.0 ermöglicht. Marvell setzt mit dem ThunderX3 noch einen drauf, hier sind es bis zu 96 Kerne mit je 4 SIMD-Einheiten und Vierfach-Multithreadring, also 768 logische Kerne im Dual-Socket-System.

Angesichts der ARM- und AMD-Übermacht streicht Intel die Cooper-Lake-Segel teilweise: Dieser dritte Aufguss des 14-Nanometer-Xeon-SP soll nur noch in Varianten für Server mit vier oder acht CPU-Fassungen kommen. In dieser Nische kann Intel noch punkten.

Schlüssel in Gefahr

Die Sicherheitsexperten Mark Ermolov und Maxim Goryachy von der russischen Firma Positive Technologies (PTE) graben seit Jahren immer tiefer in Intels Management Engine (ME), auch Converged Security and Management Engine (CSME) oder CSE genannt. Sie meinen nun, dass ein wichtiger kryptografischer Schlüssel von Intel-Prozessoren kurz vor der Enttarnung steht. Dieser „Hardware Key" ist laut den PTE-Leuten bei Prozessoren aus den Jahren 2011 bis heute identisch und lässt sich nicht durch Firmware-Updates gegen einen anderen austauschen. Würde der Schlüssel kompromittiert, könnten in der Folge einige ME-Funktionen unbrauchbar werden. Intel hatte bereits Ende 2019 Updates der CSME-Firmware verteilt, um Angriffe auf den Hardware-Schlüssel zu erschweren. Am 10. März kündigte Intel noch eine Fülle weiterer Updates an, etwa für Grafiktreiber mit Sicherheitslücken und auch BIOS-Updates für fast alle NUC-Mini-PCs. Auch eine weitere Sicherheitslücke der Spectre-Art wurde veröffentlicht: Load Value Injection (LVI) ist vor allem für verschlüsselte RAM-Enklaven gefährlich, die sich mit Software Guard Extensions (SGX) einrichten lassen. Intel begegnet LVI mit Compiler-Updates, die aber relativ viel Performance kosten, allerdings eben nur in Trusted Execution Environments (TEEs) mit SGX.

(ciw@ct.de) c't

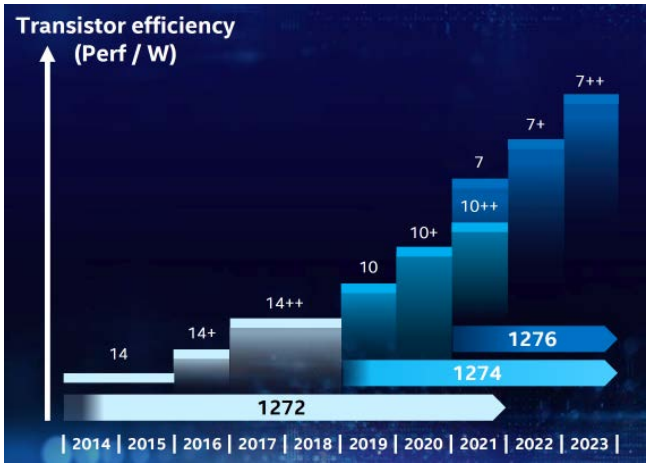


Bild: Intel

Auf die von Pannen und Verzögerungen geplagte 10-Nanometer-Technik soll bei Intel ab 2021 die 7-Nanometer-Fertigung folgen. Frühestens ab 2023 will man dann bei 5 Nanometern wieder der Konkurrenz voraus sein.