Bit-Rauschen

Lebenszeichen von VIA, optimierte Bibliotheken und RISC-V-Umzug

Der VIA-Ableger Centaur baut eine AVX-512-CPU. Einige Programmierer wundern sich über Nachteile von Intel-Code auf AMD-CPUs. AMD kämpft mit RAM-Verschlüsselung und RISC-V zieht es in die Alpen.

Von Christof Windeck

Die Supercomputer-Konferenz SC'19 brachte außer der jüngsten Top500-Liste (siehe S. 44) auch ein Lebenszeichen der taiwanischen Prozessorfirma VIA: Ihr texanischer Ableger Centaur überraschte mit der Ankündigung eines achtkernigen x86-Prozessors mit KI-Erweiterung. Noch erstaunlicher sind die AVX-512-Erweiterungen der centaurischen x86-Kerne, weil es AVX-512 bisher nur bei Intel gibt. Unklar ist, ob und wann AMD nachzieht. AMD-Serverchef Forrest Norrod versprach kürzlich, dass Zen-3, also die 2020 erwarteten Ryzen 4000 (alias Vermeer) und Epyc 7003 (Milan), eine „neue Mikroarchitektur" bringen werde mit rund 15 Prozent mehr Performance. Da käme AVX-512 durchaus in Betracht, aber etwa auch das für KI gedachte Gleitkomma-Datenformat Bfloat16.

Mittlere Aufregung erregte derweil, dass hochoptimierte Mathematik-Softwarebibliotheken von Intel auf AMDs Zen-CPUs langsamer laufen. Für Aufregung besteht aber kaum Anlass, weil sich das einerseits per Skript beheben lässt und andererseits der dänische Forscher Agner Fog schon vor zehn Jahren darüber schrieb. Die US-Wettbewerbskommission FTC hatte Intel seinerzeit dazu verpflichtet, die Optimierungen der Math Kernel Library (MKL) für Intel-Chips zu dokumentieren: Read the Fucking Manual (RTFM), kann man da nur sagen.

Spezielle Compiler braucht auch der KI-Chip der jungen Firma Groq, um in beeindruckende Leistungsdimensionen vorzustoßen: 1 Billiarde Operationen pro Sekunde (Ops/s) soll er liefern. Dabei geht es vermutlich um 8-Bit-Ganzzahlen (Int8), Groq verrät das nicht genau. Angeblich kann Groq dank des Compilers die bei anderen Prozessoren nötige Steuerlogik weglassen, sodass mehr Transistoren tatsächlich rechnen. Im kaum noch überschaubaren Gewusel Dutzender KI-Chip-Start-ups erfuhr Groq besondere Aufmerksamkeit, weil Mitgründer Jonathan Ross zuvor bei Google an der Entwicklung der Tensor Processing Unit (TPU) beteiligt war.

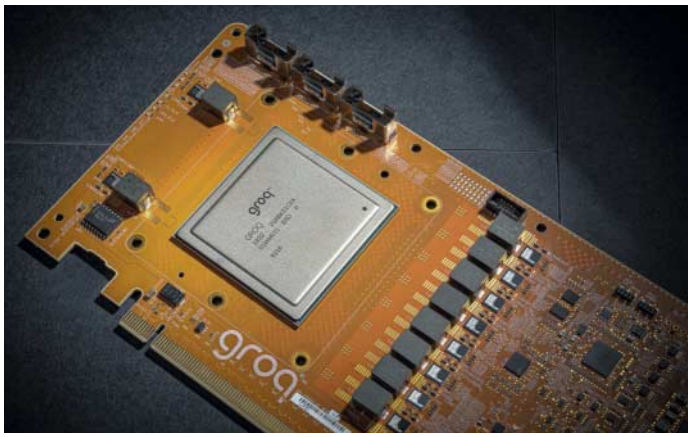
AMD-PSP-Löcher

In c't 25/2019 berichteten wir über Sicherheitslücken in Trusted Platform Modules (TPMs) von ST und Intel. Dabei ging etwas unter, dass TPM-Pannen keine Seltenheit sind. Berühmt wurde 2017 der ROCA-Bug im RSA-Algorithmus von Infineon-TPMs. Doch auch das Firmware-TPM (fTPM 2.0) im AMD Secure Processor alias Platform Security Processor (PSP) zeigte Anfang 2018 eine Lücke, die AMD mit BIOS-Updates schloss. Und in der RAM-Verschlüsselungsfunktion der Epycs für Server, der Secure Encrypted Virtualization (SEV), tauchte schon die zweite Schwachstelle auf. Unter CVE-2019-9836 war im Juni bekannt geworden, dass sich der geheime Schlüssel für SEV-verschlüsseltes RAM durch trickreiche Rechnereien ermitteln lässt. Nun meldet ein Team um Robert Buhren von der TU Berlin, dass sich nicht sicher per „Remote Attestation" aus der Ferne prüfen lässt, ob SEV das RAM einer Cloud-VM überhaupt schützt. Das wiederum unterminiert den Sinn von SEV grundsätzlich.

Genau wie Intels SGX zielt AMD SEV auf die sichere Nutzung von Cloud-Servern, selbst wenn man dem Betreiber nicht vertraut – dort könnte sich ja ein böser Administrator eingeschmuggelt haben. Stattdessen muss man aber kryptografischen Zertifikaten vertrauen, die eine vermeintlich sichere Kette bis zu Servern von AMD oder Intel ziehen, dazu aber möglicherweise Firmware, Software und Zertifikate von Dritten einbinden.

Das ist dermaßen kompliziert, dass Kritiker grundsätzlich an diesem Konzept zweifeln. Letztlich geht es wohl eher darum, Verantwortung für den Datenschutz abzuwälzen oder abstrakte Sicherheitsvorschriften zu erfüllen. Doch auch in aufwendig überprüfter IT-Sicherheitstechnik stecken Bugs: Dem lückenhaften ST-TPM hatte eine Sparte des französischen Rüstungskonzerns Thales Sicherheit nach Common Criteria Evaluation Assurance Level 4+ (CC EAL 4+) bescheinigt, aber dabei die Schwäche für einen Timing-Angriff übersehen, dessen technisches Prinzip altbekannt ist.

Höhere Sicherheit durch offenes Design verspricht RISC-V-Technik, die deshalb auch schon für mehrere sicherheitskritische Chips eingeplant ist. Dazu gehören Googles OpenTitan oder das SSITH-Projekt der US-DARPA unter anderem für sichere Wahlmaschinen. Die RISC-V Foundation plant nun, ihren Sitz aus den USA in die Schweiz zu verlagern, weil einige ihrer Mitglieder sich vor Strafaktionen der unberechenbaren US-Regierung fürchten. Republikanische Politiker aus den USA vermuten chinesische Firmen hinter dieser Entscheidung, aber auch die European Processor Initiative (EPI) dürfte den Schritt begrüßen. *(ciw@ct.de)* c't



Die junge Firma Groq verspricht eine Billiarde Operationen pro Sekunde für ihren neuartigen KI-Chip.

Bild: Groq