256-bit

In computer architecture, **256-bit** integers, memory addresses, or other data units are those that are 256 bits (32 octets) wide. Also, 256-bit CPU and ALU architectures are those that are based on registers, address buses, or data buses of that size.

There are currently no mainstream general-purpose processors built to operate on **256-bit** integers or addresses, though a number of processors do operate on 256-bit data. CPUs feature SIMD instruction sets (Advanced Vector Extensions and the FMA instruction set etc.) where 256-bit vector registers are used to store several smaller numbers, such as eight 32-bit floating-point numbers, and a single instruction can operate on all these values in parallel. However, these processors do not operate on individual numbers that are 256 binary digits in length, only their registers have the size of 256-bits. Binary digits are found together in 128-bit collections.

Contents

Uses

- 256 bits is a common key size for symmetric ciphers in cryptography, such as Advanced Encryption Standard
- Modern GPU chips move data across a 256-bit memory bus.
- 256-bit processors could be used for addressing directly up to 2^{256} bytes. Already 2^{128} (128-bit) would greatly exceed the total data stored on Earth as of 2010, which has been estimated to be around 1.2 zettabytes (over 2^{70} bytes).[1]
- The Efficeon processor was Transmeta's second-generation 256-bit VLIW design which employed a software engine to convert code written for x86 processors to the native instruction set of the chip.[2][3]
- Increasing the word size can accelerate multiple precision mathematical libraries. Applications include cryptography.
- Researchers at the University of Cambridge use a 256-bit capability pointer, which includes capability and addressing information, on their CHERI capability system.[4]

Laptop computer using an Efficeon processor

History

The DARPA funded Data-Intensive Architecture (DIVA) system incorporated processor-in-memory (PIM) 5-stage pipelined 256-bit datapath, complete with register file and ALU blocks in a "WideWord" processor in 2002.[5]

See also

- Berkeley IRAM project
- Computational RAM

References

1. Rich Miller (May 2010). "Digital Universe nears a Zettabyte" (http://www.datacenterknowledge.com/archives/2010/05/04/digital-universe-nears-a-zettabyte/) *The Guardian*. datacenterknowledge.com Retrieved 16 September 2010.
2. Transmeta Efficeon TM8300 Processor (http://datasheets.chipdb.org/Transmeta/pdfs/brochures/efficeon_tm8300_processor.pdf)
3. Transmeta Unveils Plans for TM8000 Processor (http://www.pcworld.com/article/101516/transmeta_unveils_plans_for_tm8000_processor.html) PCWorld Martyn Williams, IDG News 29 May 2002
4. Robert N.M. Watson; Peter G. Neumann; Jonathan Woodruff; Jonathan Anderson; Ross Anderson; Nirav Dave; Ben Laurie; Simon W. Moore; Steven J. Murdoch; Philip Paeps; Michael Roe; Hassen Saidi. "CHERI: a research platform deconflating hardware virtualization and protection" (http://www.csl.sri.com/users/neumann/2012resolve-cheri.pdf) (PDF). *Unpublished workshop paper for RESoLVE'12, March 3, 2012, London, UK* SRI International Computer Science Laboratory.
5. Implementation of a 256-bit WideWord Processor for the Data-Intensive Architecture (DIVA) Processing-In-Memory (PIM) Chip (http://atrak.usc.edu/~changk/publications/esscirc02.pdf)
