RISC-V Glossary

RISC-V acronyms and terms

This glossary includes definitions of terms specific to RISC-V in addition to terms that are useful in understanding the architectures and technologies in use by RISC-V contributors and users.

ABI

Application binary interface. Abstractions and interfaces for applications that allow interactions without the need to know the details about what takes place in the lower networking layers. For RISC-V, the ABI provides abstractions of S or M modes.

AEE

Application execution environment—the environment, from bare metal to full operating system, in which an application runs.

AIA

xxx

AIS 31

Information Security service for Europe and the global finance industry (for bank cards), written by BSI.

ALU

Arithmetic Logical Unit.

ASIC

Application-Specific Integrated Circuit.

AT

xxx

ATA

Advanced Technology Attachment.

ATM

Asynchronous Transfer Mode.

Atomic Layer Deposition

A layer-by-layer process that results in the deposition of thin films one atomic layer at a time in a highly controlled manner.

ATX

Advanced Technology eXtended.

BF

Refers to Brain Float or Brain Floating Point, used in BFLOAT16.

BFLOAT16

Brain floating point 16 bit—a vector (V) extension representing a wide dynamic range of numeric values by using a floating radix point. See en.wikipedia.org/wiki/Bfloat16_floating-point_format.

BSI

German Federal Information Security service.

CLIC

Core-Local Interrupt Controller—A low-latency, vectored, preemptive interrupt controller for RISC-V systems.

CPL

Cost Per Load.

CPU Cache

Many CPUs three kinds of caches to speed up data retrieval: an instruction cache for executable instruction fetch, a data cache for data store and fetch, and a translation lookaside buffer (TLB) for virtual-to-physical address translation for executable instructions and data.

CMOS

Complementary Metal Oxide Semiconductor.

Chemical Vapor Deposition

A chemical deposition process in which the wafer is exposed to one or more volatile precursors, which react and/or decompose on the substrate surface to produce the desired film.

Consistency Model

A computing system supports a specific consistency model if operations on memory follow specific rules. For example, high level languages like C++ and Java, partially maintain the contract by translating memory operations into low-level operations while preserving memory semantics. To hold to the contract, compilers may reorder some memory instructions, and library calls like `pthread_mutex_lock()` encapsulate required synchronization.

DM

Deg=bug Module--

DRAM

Dynamic Random Access Memory.

eDRAM

Embedded DRAM.

ELEN

Element length.

ES

Entropy Source—an input or a measured characteristic that supplies random bits for an I/O device on a computer, usually used to supply bits that an attacker cannot know, as part of security.

Flip-flop

Electronic circuitry with two stable states for use in storing binary data. Data stored in flip-flops is changed by applying specific inputs. Both flip-flops and latches are building blocks that are used in digital computing.

FLOPS

Floating Point Operations per Second--

GE

Gate Equivalent.

HART

Hardware Thread—at machine-mode level each hart is a real hardware thread, either one hart per core without hardware multithreading, or multiple harts per core with hardware multithreading, and 'hart' represents the hardware resource. It is possible to emulate harts in software, for example, privileged execution environments can multiplex lesser-privileged harts onto physical hardware using timer interrupts. Note that co-operative multithreading within the same privilege level is not a compliant implementation. Across all implementation choices, we retain the concept of a hart as a resource abstraction representing an independently advancing RISC-V execution context within a RISC-V execution environment.

HBI

Hypervisor Binary Interface—an interface abstraction for hypervisors to run.

HEE

hypervisor execution environment—the environment in which a hypervisor runs.

IC

Integrated Circuit.

ID Synchronization

The mechanisms by which code generated on a core (e.g., by a JIT compiler) is made visible to other cores.

IEEE 754

a technical standard for floating-point arithmetic established in 1985 by the Institute of Electrical and Electronics Engineers.

IIRC

The International Integrated Reporting Council (IIRC) (previously the International Integrated Reporting Committee). was formed in August 2010 and aims to create a globally accepted framework for a process that results in communications by an organization about value creation over time.

IMSIC

International Mobile Subscriber Identity Code.

IRC

The IRC—Internet Relay Chat protocol is for use with text based conferencing; the simplest client being any socket program capable of connecting to the server.

ISA

Programmer visible state and operations on that state, the boundary between hardware and software.

Instruction Set

A group of commands for a CPU in machine language that can refer to all possible instructions for a CPU, or a subset of instructions to enhance its performance in specific situations, and includes:

- Instruction length—which can vary, Opcodes—the command to be carried out.
- Operands—on which the command will operate.
- Registers—internal locations that are limited in number and ability while quick to access.
- Memory—external storage—a larger and more versatile number of locations that are slower to access.

J Extension

a RISC-V extension that provides a form of sandboxing that can be implemented by the pointer masking proposal where runtime and sandboxed code all run within user mode and the sandboxed code has been checked by the runtime to be unable to change pointer masks.

Latch

A circuit that has two stable states that is used to store state information, known as a bistable multivibrator.

LL/SC

Load Link/Store Conditional or Load Locked/Store conditional—see LR/SC.

LR/SC

Load Reserve/Store Conditional, also LL/SC --a pair of instructions used in multithreading to achieve synchronization. Load-link returns the current value of a memory location, while a subsequent store-conditional to the same memory location will store a new value only if no updates have occurred to that location since the load-link. Together, these implement a lock-free atomic read-modify-write operation.

LSA

load–store architecture—a design that is architecturally neutral and that uses bit patterns in IEEE 754 floating-point to speed sign extension in ways that simplify the multiplexers in a CPU—by placing most-significant bits at a fixed location.

M

used to indicate Machine Mode—a mode to which machines boot that allows programmer access to everything. The M is required in all RISC-V implementations.

MCM

Multi-Chip Module.

MIPS

Microprocessor without Interlocked Pipelined Stages—a reduced instruction set computer (RISC) instruction set architecture developed by MIPS Computer Systems, now MIPS Technologies, based in the United States, that influenced later RISC architectures.

MMU

Memory Management Unit.

MXLEN

Machine XLEN.

NAND

Not-and.

NIST

Keeps the standard time for America, defines 1 inch, and also cryptographic standards.

Non-ISA

Non-Standard Extension—primarily programmer visible software conventions to ensure interoperability, but also HW protocols not directly visible to programs, e.g. HW external debug protocols

NOR

Logical NOR, known as Pierce's Equivalent, Quine's Dagger, the ampcheck (from the Greek for "cutting

both ways"), joint denial, or neither-nor, operates on two logical values, typically from two propositions, that produces a value of true if and only if both operands are false. In other words, it produces a value of false if and only if at least one operand is true.

OS-level Sandboxing

a form of sandboxing implemented by the pointer masking proposal. There is no guarantee that sandboxed code cannot modify the pointer mask and therefore the sandbox does not allow modifying pointer masks in user mode.

Page fault

a type of exception raised by computer hardware when a running program accesses a memory page that is not currently mapped by the memory management unit (MMU) into the virtual address space of a process.

Photolithography

In microprocessor manufacturing, a process of using light to transfer a geometric pattern from a photomask (also called an optical mask) pattern parts to a photosensitive substrate on a thin film (substrate or wafer). The process can also make use of chemical photoresist on the substrate.

Platform

A System Platform is a set of features users can depend on working together that includes things like ISA Profiles, software components, hardware system components, standardized hardware/software interfaces, and other features. Currently RISC-V has defined two Platform types—OS/A and M (naming TBD).

PLIC

Progressive Lossless Image Coding.

PPO

Preserved Program Order—strict sequential consistency that demands that operations be seen in the order in which they were issued.

PQC

Post-Quantum Cryptography, due to replace RSA and ECC in NIST cryptography [PQC] as well as military [NSA].

Privileged

Provides security isolation, and a means to reduce code defects because code does not have to check for illegal values. Privileged contains state, is used primarily to run applications and can be used to debug implementations. It defines CSR address space and content trap when taken increases privilege mode (say from U to S) trap when taken stays at the current privilege mode access more than even M mode. Its addresses reserved in ISA. address includes highest mode that access the CSR and if it is `r/w/rw/none` preserve bits already there when you change a field.

Profile

(ISA Profile) a set of extensions (instructions, state and behaviors) that users can depend on working together. Extensions are either required, optional, unsupported, or incompatible. RISC-V has defined two Profile types: Application (RVAyy)--appropriate for Linux-class and other embedded designs with more sophisticated ISA needs—and Micro-controller (RVMyy)--appropriate for cost-sensitive application-optimized embedded designs running bare-metal or simple RTOS environments.

Psuedo Instructions

special commands to the assembler about the positioning of the program, the address the program should presumed to be assembled at, the name of the module, data declarations, the title and printing options for the program, defining and calling macros, macro looping and test, and end of source ...

PTE

Page Table Entry—an entry in the data structure used by a virtual memory system in a computer operating system to store the mapping between virtual addresses (used by the program executed by the accessing process) and physical addresses (used by the hardware, or more specifically, by the RAM subsystem), that enables access data in memory.

PTEP

Parallel Telemetry Processor—a high- speed virtual processor architecture.

PTG.2

A physical random number generator class defined in AIS 31/CC.

PUD

Patch update?

QEMU

QEMU (Quick EMUlator) is a free and open-source emulator and virtualizer that can perform hardware virtualization.

Register

A group of flip-flops with each flip-flop capable of storing one bit of information. The simplest register is one that consists of only flip-flops with no external gates.

RISC

Reduced Instruction Set Computer architecture. Information processing using any of a family of microprocessors that are designed to execute computing tasks with the simplest instructions in the shortest amount of time possible. RISC-based machines execute one instruction per clock cycle as opposed to CISC (Complex Instruction Set Computer) machines that can have special instructions as well as instructions that take more than one cycle to execute.

Rocket

Parameterized SoC generator written in Chisel, designed to helps tune the design under different performance, power, area constraints, and diverse technology nodes.

RV

Reliability verification is a category of physical verification that helps ensure the robustness of a design by considering the context of schematic and layout information to perform user-definable checks against various electrical and physical design rules that reduce susceptibility to premature or catastrophic electrical failures, usually over time.

RVWMO

RISC-V Weak Memory Ordering—Default memory ordering model that loads return value written by latest store to the address of the later of in-program and memory order (see specifications for list of axiomatic and operational rules).

SBI

Sytem Binary Interface—abstracts the interfaces that are required to run operating systems.

Scala

a statically-typed, general-purpose programming language that supports both object-oriented programming and functional programming. Designed to be concise, Scala's design aims to address criticisms of Java, and it provides language interoperability with Java so that libraries written in either language can be referenced

directly in both Scala and Java code. Scala source code can be compiled to Java bytecode and run on a Java virtual machine (JVM).

SEE

supervisor execution environment—environment in which operating systems run, which can but are not required to be BIOS style interfaces.

Segmentation fault

a failure condition caused by a memory access violation in hardware operating with memory protection. The fault process notifies the operating system (OS) that software has attempted to access a restricted area of memory.

SFENCE

Orders processor execution relative to all memory stores prior to the SFENCE instruction. The processor ensures that every store prior to SFENCE is globally visible before any store after SFENCE becomes globally visible. The SFENCE instruction is ordered with respect to memory stores, other SFENCE instructions, MFENCE instructions, and any serializing instructions (like CPUID instructions), and it is **not** ordered with respect to either memory loads or the LFENCE instruction.

SFENCE.VMA

(instruction wrapper?)

SHA

Secure Hash Algorythms—a family of cryptographic hash functions published by the National Institute of Standards and Technology as a U.S. Federal Information Processing Standard that started with what is now known as SHA-0, a retronym used for the original (1993) 160-bit hash function published under the name "SHA".

SoC

System on Chip.

SP 800 90B

Used in military & USGOV random security evaluations, written by NIST.

SRAM

Static Random Access Memory.

Standard Extension

for RISC-V, ...

TLB

Translation Lookaside Buffer—a memory buffer that enhances speed in retrieving a value by storing a memory address.

TRNG

True Random Number Generator—also known as HRNG, or Hardware Random Number Generator—a device that generates random numbers from a physical process, rather than by means of an algorithm. Such devices are often based on microscopic phenomena that generate low-level, statistically random "noise" signals, like thermal noise, the photoelectric effect involving a beam splitter, and other quantum phenomena.

Unpriveleged

User-space—describes

VM

Virtual Machine.

VMA

Virtual Memory Allocation--

WARL

Weighted Average Run Length--

XLEN

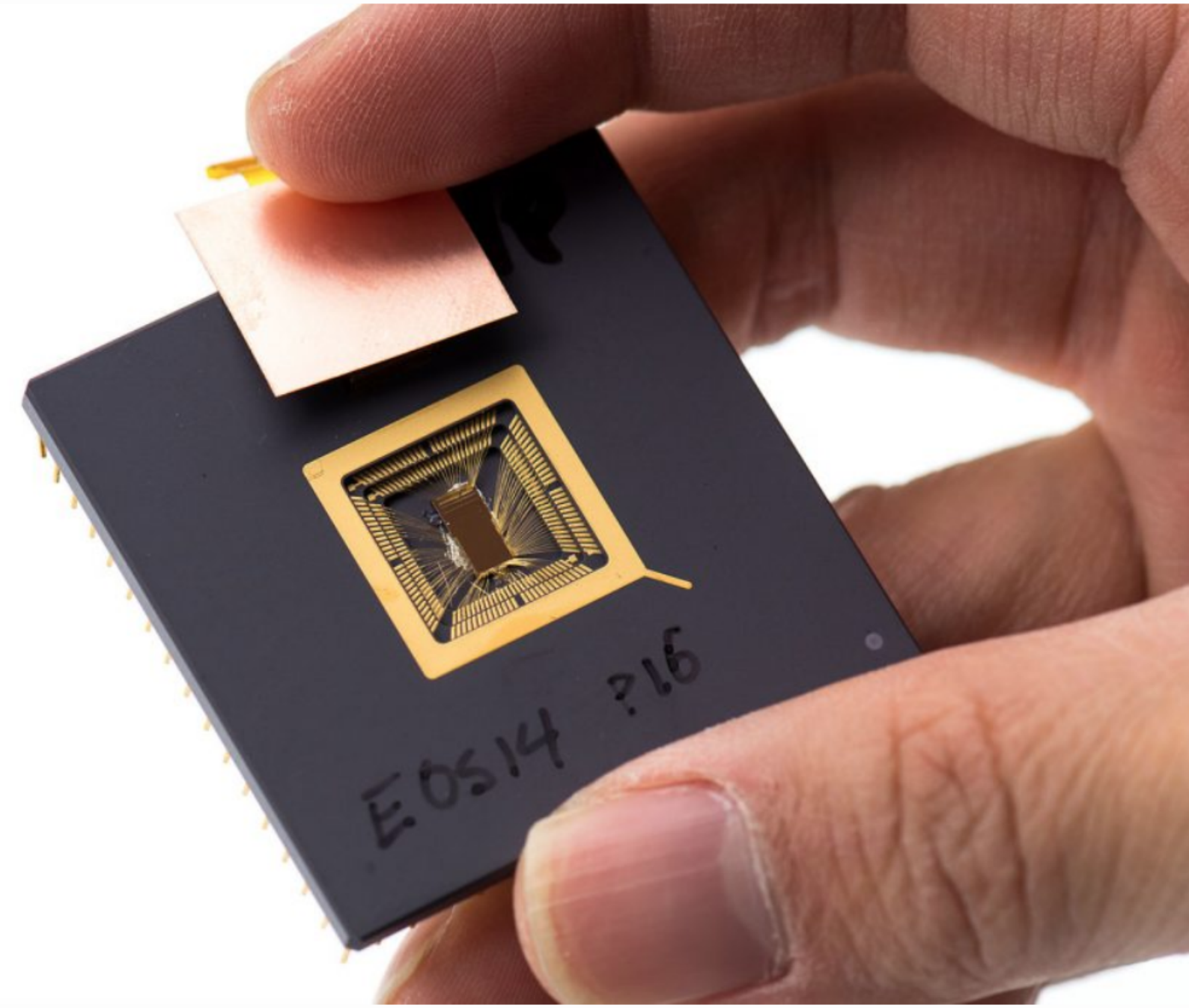
Register width—etymology involves reference to mathematical X and abbreviation of the word "length."

ZBT

Zero Bus Turnaround

ZFew

xxxx


EOS14 ?16