QEMU support for Xtensa

- Git tree: https://github.com/OSLL/qemu-xtensa
- Toolchain build scripts: https://github.com/jcmvbkbc/xtensa-toolchain-build
- Kernel and rootfs binary archive: http://jcmvbkbc.spb.ru/~dumb/ws/osll/qemu-xtensa/20110829/xtensa-dc232b_kernel_rootfs.tgz
- Official QEMU wiki feature page: http://wiki.qemu.org/Features/Xtensa
- Official xtensa linux wiki page: http://wiki.linux-xtensa.org/index.php/Xtensa_on_QEMU

Description

qemu/target-xtensa is a project aimed at development of a free simulator for Tensilica Xtensa processor family.

Although xtensa instruction set specification is open and there's even linux port for xtensa there were no free simulator available.

The project was initiated to lower cost and to speed up development of one of the Motorola Solutions projects and has been carried out exclusively by the OSLL. Started in March 2011 it took 2 months to provide initial ThreadX support, 2 more months to provide linux support and 2 more months to get accepted into the qemu mainline.

Our goal is to make it usable (and preferable:) in real development/production environment.

Now active

- TIE support

TODO

- xtensa TCG backend

Implementation status

- core/basic opcodes implementation;
  - [+] and/or/xor/neg/abs;
  - [+] shifts;
  - [+] add[x*]/sub[x*]/add.n/addi.n;
  - [+] call0, callx0, j, b*;
  - [+] l32*, s32*;
  - [+] accurate SR write semantics;
- options

    - [+] windowed registers;
        - [+] call*/callx*, retw, rotw, rfwo, rfwu;
        - [+] accurate overflow triggering;
    - [+] loop option;
    - [+] extended L32R option;
    - [+] MAC16;
    - [+] coprocessors;
        - [+] floating point;
        - [+] boolean registers/commands;
    - [+] memory protection;
        - [+] no-MMU mode;
        - [+] region protection (with/without translation);
        - [+] MMU;
        - [+] MPU;
    - cache options;
        - [+] memory attributes;
        - [+] memory accessibility check;
        - [-] memory access timing;
    - [+] debug option;
    - exceptions;
        - [+] debug (only external);
        - [+] break;
        - [+] window overflow/underflow;
        - [+] user/kernel (invalid insn, privileged insn, alignment, division by 0,...);
        - [+] relocatable vectors;
        - [+] external interrupts;
        - [+] timer interrupts;
            - [+] qemu timer to avoid busy looping in waiti;
    - [+] FLIX;
    - [+] wide branches;
- gdbserver;
    - [+] read/write register, ~~xml register map~~ (not used by gdb);
    - [+] correct SR mapping;
    - [+] debug exception, single step mode;
    - [+] hw/sw breakpoints;
    - [+] gdbserver for different processor types;
- evaluation board;
    - [+] sim platform;
    - xt2000 platform;
        - [+] UART (reuse existing 16550 serial);
        - [+] xtsonic (reuse existing dp8393x NIC);
        - [-] LED;
    - [+] lx200/60/110 platform;
        - [+] UART (reuse existing 16550 serial);
        - [+] opencores ethernet;
    - [+] virt platform
        - [+] PCI controller
        - [-] hardcoded IRQ routing may connect legacy PCI IRQ to edge-triggered external IRQ line
    - [+] linux-user

- simulation quality;
  - [+] pass command line arguments to argc/argv SIMCALLs;
  - [+] TB chaining;
- [+] external configuration (overlay reuse);
- [+] automatic regression test suite;
- [+] SMP support (interrupt distributor, WER/RER);
- [-] cycle accurate pipeline;

Events

- 2011.04.20: C++ 'hello world' is working in qemu (stdio, stdlib, simcalls, windowed registers, loops, ext l32r) (:
- 2011.04.26: multithreaded ThreadX application is working in qemu (timer interrupts)
- 2011.04.30: preparation for qemu mainline submission started
- 2011.05.04: first RFC patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-05/msg00242.html
- 2011.05.18: first PATCH patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-05/msg01525.html
- 2011.06.19: linux boots, issues on userspace application startup
- 2011.06.22: successfull userspace app startup in linux
- 2011.06.29: xtensa linux session on qemu-xtensa was available at ssh -p 3333 xtensa@jcmvbkbc.spb.ru
- 2011.07.18: issue with gdb not able to read privileged SRs root-caused: http://sourceware.org/ml/gdb/2011-07/msg00073.html
- 2011.07.19: tensilica guys suggested the following solution for gdb:

```
I guess you can just make sure you don't mark new registers as PRIVILEGED in
   ./gdb/xtensa-config.c
```

- 2011.07.24: second PATCH patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-07/msg02529.html
- 2011.09.01: third PATCH patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-08/msg03888.html
- 2011.09.02: fourth PATCH patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-09/msg00165.html
- 2011.09.06: fifth PATCH patchset sent to qemu-devel http://lists.nongnu.org/archive/html/qemu-devel/2011-09/msg00695.html
- 2011.09.10: fifth PATCH patchset hit the qemu mainline: http://lists.nongnu.org/archive/html/qemu-devel/2011-09/msg01298.html
- 2011.09.27: linux booted up to rootfs mounting on the new emulated LX200 board
- 2011.10.01: complete linux bootup via NFS on the LX200
- 2011.10.10: lx60, opencores ethernet, overlay reuse and MAC16 patches sent to qemu-devel
- 2011.10.16: lx60, opencores ethernet, overlay reuse and MAC16 patches are merged
- 2011.10.29: lx60/lx200: u-boot starts from FLASH, linux kernel boots via TFTP
- 2011.11.03: emulation speed test for sha512sum running in linux on dc232b shows fantastic 266 MIPS
- 2011.11.22: linux for dc233c is working on qemu
- 2012.01.13: instruction breakpoints are working
- 2012.01.29: data breakpoints are working
- 2012.03.03: debug option is merged

- 2012.09.09: FP coprocessor series is posted to qemu-devel
- 2012.09.19: FP coprocessor series is in the mainline
- 2014.06.29: uImage/DTB/initrd loading on XTFPGA boards
- 2017.01.25: CCOUNT no longer counts instructions; RER/WER and RUNSTALL are in the mainline
- 2018.01.09: libisa and target disassembler series is in the mainline
- 2018.01.24: xtensa noMMU series is in the mainline
- 2018.03.17: xtensa linux-user series is in the mainline
- 2019.01.30: basic FLIX 'hello world' is working
- 2019.02.05: xtensa SMP support series is in the mainline
- 2019.03.01: xtensa FLIX support series is in the mainline
- 2019.09.12: xtensa call0 ABI is supported by linux-user in the mainline
- 2019.10.24: xtensa virt machine is in the mainline