QEMU support for Xtensa

- Git tree (view): http://jcmvbkbc.spb.ru/git/?p=dumb/qemu-xtensa.git;a=summary
- Git tree (clone): git://jcmvbkbc.spb.ru/dumb/qemu-xtensa.git / http://jcmvbkbc.spb.ru/dumb/qemu-xtensa.git
- Toolchain build scripts (view): http://jcmvbkbc.spb.ru/git/?p=dumb/xtensa-toolchain-build.git;a=summary
- Toolchain build scripts (clone): git://jcmvbkbc.spb.ru/dumb/xtensa-toolchain-build.git / http://jcmvbkbc.spb.ru/dumb/xtensa-toolchain-build.git
- Kernel and rootfs binary archive: http://jcmvbkbc.spb.ru/~dumb/ws/osll/qemu-xtensa/20110829/xtensa-dc232b_kernel_rootfs.tgz

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 qemu/target-xtensa implementation currently provides almost full instruction set support (enough to run linux/ThreadX), is fast and is available under BSD license.

It can be easily extended to support custom xtensa architecture variants and external hardware.

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

Now active

- usermode emulation
- FP coprocessor

TODO

- SMP support (interrupt distributor, WER/RER);
- ATOMCTL support;
- cache option implementation;
- cycle accurate pipeline;

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 mode;
  - cache options;
    - [-] memory attributes;
    - [-] 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;
      - [-] correct opcode timings?;
      - [+] 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;
- sample evaluation board;
  - [+] sim(dc232b) 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;
- simulation quality;
    - [+] pass command line arguments to argc/argv SIMCALLs (DAN branch only);
    - [+] TB chaining;
    - cycle accuracy;
        - [-] pipeline/SYNC group;
        - [-] memory access;
        - [-] exceptions;
- [+] external configuration (overlay reuse);
- [+] automatic regression test suite;

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 is available at ssh -p 3333 xtensa@jcmvbkbc.spb.ru with the following private key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA2ycE9iuEtWoNOmyLsx5aiEAPDx//MJlmMrx6o6qAUTj+wivk
kaKQE1yCZMUa/B40BMUST9KffHqIcV9jxDFjagM/dfbdbTxeiiNEKyjBsrEidEoU
ytM5fkpHFyg1DmCvkXdoUAAzeVCy5ILh6ZhqpQpe68Pb8vQLdj9QmwcvOpS7d97q
OMbGadIRdgOdlVAYQ/Rju8D+k9yygFn/TwZlTiT/glEpk/D4dq+8D1UlFNvohUH4
3VY/gVJ0CuEQx1OwS+NTJLSz25Z2eTaNTEE4sqqAy2zlBe23Ef4vQo0mWvmBBIkA
x6dPBqKsQZCW6gGcsHk7fMw0K4H1RSOLRiAuQwIDAQABAoIBAQDZQ1m743DxmW37
2di1fwYpxbgoOoR33dxfuFOtJj+IRoTqYzF64DsNtszesjoKcLcJc4av9BOBCMlz
/CmgO4Zfd1DW1iK3RP5E3KmcUA+X49xQhZEPc1CwT1sjLg1Lb7ce885KYaimQMbZ
nJfzSdOQQzPPcKEBv8gNNr/msby0ySFZ06sQNpSzaboD0u7TdssYz22BDaZ0E+4C
VgOLgFHo9qEMO5PlTElRvRd0JjVRF5Mn9SExSxqWKFzlFMNRkk63Fd3j34St+Z6U
VFc5OAMEoJt8pPEFNwpbzK0CZyYhWi02US2A8d5aPgodb1WQ0H1JdgO3u9b5YsJN
hcGjtDwhAoGBAO5/ySbW59vfUkmwI/s5WL3KgfdkzIUGKdG3yPL3MpUgnrOPPcnT
xZi67BWCPS0ac4AlKjMJ0Px85XZQChjEh43CH3cglf9bzneTTC+liHq7GfvoQITd
TOZTHFu1z6SCgUtTnUwQFdXZHJDs0C21VENcS/N0XudXLy0nIBwWKwzHAoGBAOs7
zfBA2IOFim3OHNaMjMUYvtpo+QQNGSwQJrw91rEbyrCd/09rUD5YLddPRhwq1jYJ
qRDGN6gqANRiTkJsZyvQz81aEqlp3WmG4hPWitymhlpgQ4mFmZU88IMYaQ9Dh8Vp
Dv6kT6zraAzBKc5nezjKisDItVzieDbly4TWMX6lAoGAJshOzGsL3vwspGDpKPQF
Uy93/OO+Qi9jY3/wRFogNpHMXMSBNq2iJxjWRRUdn5T6jS798ri47CXfJmMTkT18
EXgsp7F70r96DoW8UM8pJ1P/gLAetbxKwfVn2h3xev3hyn75SCIhetnIRGTN4XDo
```

```
F+ANVbRprlLGECCZnxeXvocCgYEAhLnfvvm3sK3+p2oul1gCbYtC1JV6O7DwTQ5n
7Lqvkort2K2tSrBwPF0gsGXIV0hMSX016YMOEFJy2WMGaTAlHnHZbjKuaOyUw2AZ
27un6kwDbqb2NHgvaidSRYXWcYhW6SoYDdHEKvtAYEH1RsLYofiWRaR5wIj/72nF
ZZQ9pQkCgYEA7I004D9SvsVytaeN4RdmbpXYhontoYTorL343B/hAXYgGENKEfTK
VfbweLGQ6Ga8K99YARbx2/3FOYqbGKUtUpgxVwhquyBtcUxq6+vr4riUP6M2Zw55
y3Cqme66+PO8Ka0NjjWxb+ksgO0hgcmEhlnz+3MWNODiacxHffH0ChM=
-----END RSA PRIVATE KEY-----
```

- 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

qemu