

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>

Things to do

- 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;

- gdbserver;
 - [+] xml register map, read/write register;
 - [+] correct SR mapping;
 - [+] debug exception, single step mode;
 - [+] hw/sw breakpoints;
 - [+] gdbserver for different processor types;
- sample evaluation board;
 - [+] memory mapping, ELF loader;
 - [-] standard peripherals;
 - [+] dc232b;
- simulation quality;
 - [+] pass command line arguments to argc/argv SIMCALLs (DAN branch only);
 - [+] TB chaining;
- [+] external configuration (a-la xtensa overlay)?
- [-] 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-----
MIIEpQIBAACAQEA2ycE9iuEtWoN0myLsx5aiEAPDx//MJlmMrx6o6qAUTj+wivk
kaKQElyCZMUa/B40BMUST9KffHqIcV9jxDFjagM/dfbdbTxeiiNEKyjBsRidEoU
ytM5fKpHFyg1DmCvkXdoUAAzeVCy5ILh6ZhqpQpe68Pb8vQLdj9QmwcV0pS7d97q
OMbGadIRdg0dlVAYQ/Rju8D+k9yygFn/TwZlTiT/gLEpk/D4dq+8D1UlFNvohUH4
3VY/gVJ0CuEQx10wS+NTJLSz25Z2eTaNTEE4sqQy2zlBe23Ef4vQo0mWvmBBiKA
x6dPBqKsQZCW6gGcsHk7fMw0K4H1RSOLRiAuQwIDAQABAoIBAQQDZQ1m743DxmW37
2di1fwYpxbgo0oR33dxfuF0tJj+IRoTqYzF64DsNtszesjoKcLcJc4av9B0BCmLz
/Cmg04Zfd1DW1iK3RP5E3KmcUA+X49xQhZEPc1CwT1sjLg1Lb7ce885KYaimQMbZ
nJfzSd0QQzPPcKEBv8gNNr/msby0ySFZ06sQNpSzaboD0u7TdssYz22BDaZ0E+4C
VgOLgFH09qEM05PlTELrVrd0JjVRF5Mn9SEsXqWKFzLFMNRkk63Fd3j34St+Z6U
VFc50AMEoJt8pPEFNwpbzK0CZyYhwi02US2A8d5aPgodb1WQ0H1Jdg03u9b5YsJN
hcGjtdWhAoGBA05/ySbW59vfUkmwI/s5WL3KgfdkzIUGKdG3yPL3MpUgnr0PPcnT
xZi67BWCPS0ac4AlKjMJ0Px85XZQChjEh43CH3cgLf9bzneTTC+liHq7GfvoQITd
TOZTHFu1z6SCgUtTnUwQFdXZHJDs0C21VENcS/N0XudXLY0nIBwWKwzHAoGBA0s7
zfBA2IOFim30HNaMjMUyvtPo+QQNGSwQJrW91rEbyrCd/09rUD5YLddPRhwq1jYJ
qRDGN6gqANRiTkJsZyvQz81aEqLp3WmG4hPWitymhlpgQ4mFmZU88IMYaQ9Dh8Vp
Dv6kT6zraAzBKc5nezjKisDItVzieDbly4TWMX6LAoGAJsh0zGsL3vwspGDpKPQF
```

```
Uy93/00+Qi9jY3/wRFogNpHMXMSBNq2iJxjWRRUdn5T6jS798ri47CXfJmMTkT18
EXgsp7F70r96DoW8UM8pJ1P/gLAetbxKwfVn2h3xev3hyn75SCIhetnIRGTN4XDo
F+ANVbRprlLGECCZnxeXvocCgYEAhLnfvvm3sK3+p2oul1gCbYtC1JV607DwTQ5n
7Lqvkort2K2tSrBwPF0gsGXIV0hMSX016YM0EFJy2WMGaTAlHnHZbjKua0yUw2AZ
27un6kwDbqb2NHgvaidSRyXWcYhW6SoYDdHEKvtAYEH1RsLYofiWRaR5wIj/72nF
ZZQ9pQkCgYEA7I004D9SvsVytaeN4RdmbpXYhontoYTorL343B/hAXYgGENKEfTK
VfbweLGQ6Ga8K99YARbx2/3F0YqbGKUtUpgxVwhquyBtcUxq6+vr4riUP6M2Zw55
y3Cqme66+P08Ka0NjjWxb+ksg00hgcmEhlnz+3MWN0DiacxHffH0ChM=
-----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

[qemu](#)

From:

<http://wiki.osll.ru/> - Open Source & Linux Lab

Permanent link:

<http://wiki.osll.ru/doku.php/etc:users:jcmvbkbcb:qemu-target-xtensa?rev=1311524895>

Last update: **2011/07/24 20:28**

