References

[1] The lowRISC project. http://www.lowrisc.org/.

[2] Open processor foundation. http://0pf.org/.

[3] Jacob Appelbaum. A technical action plan. Video archives for Security in Times of Surveillance conference, https://projectbullrun.org/surveillance/2015/video-2015.html#appelbaum, 2015.

[4] Genode developers. An in-depth look into the ARM virtualization extensions. http://genode.org/documentation/articles/arm_virtualization, 2015.

[5] Google Chromium Project. Chromium embedded controller (EC) development. https://www.chromium.org/chromium-os/ec-development.

[6] J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Lest we remember: Cold boot attacks on encryption keys. In Proc. 2008 USENIX Security Symposium, https://citp.princeton.edu/research/memory/, 2008.

[7] ENE Technology Inc. KB3930 for OLPC keyboard controller data sheet. http://dev.laptop.org/~rsmith/KB3930_OLPC_v02_20100503.pdf.

[8] Joanna Rutkowska. Nushu: Passive covert channels implementation in Linux kernel. Presented at the Chaos Communication Congress, https://events.ccc.de/congress/2004/fahrplan/files/319-passive-covert-channels-slides.pdf, 2004.

[9] Joanna Rutkowska. More thoughts on CPU backdoors. The Invisibe Things Blog, http://blog.invisiblethings.org/2009/06/01/more-thoughts-on-cpu-backdoors.html, 2009.