[10] Joanna Rutkowska. Intel x86 considered harmful. http://blog.invisiblethings.org/papers/2015/x86_harmful.pdf, 2015.

[11] Joanna Rutkowska and Alexander Tereshkin. Evil Maid goes after TrueCrypt! The Invisibe Things Blog, http://blog.invisiblethings.org/2009/10/15/evil-maid-goes-after-truecrypt.html, 2009.

[12] Joanna Rutkowska and Rafał Wojtczuk. Qubes OS architecture. http://files.qubes-os.org/files/doc/arch-spec-0.3.pdf, 2010.

[13] thaddeus t. grugq. P.O.R.T.A.L.: Personal onion router to assure liberty. https://github.com/grugq/portal, 2012.

[14] The coreboot project. coreboot: fast and flexible open source firmware. http://coreboot.org/.

[15] The OpenSSD Project. OpenSSD wiki. http://www.openssd-project.org/wiki/The_OpenSSD_Project.

[16] The Qubes OS Project. Qubes OS: A reasonably secure desktop os. https://qubes-os.org.

[17] Wikipedia. ARM architecture. https://en.wikipedia.org/wiki/ARM_architecture.