CrypTech

Designing a More Assured HSM and Obsessing About the Tool-Chain

Goals

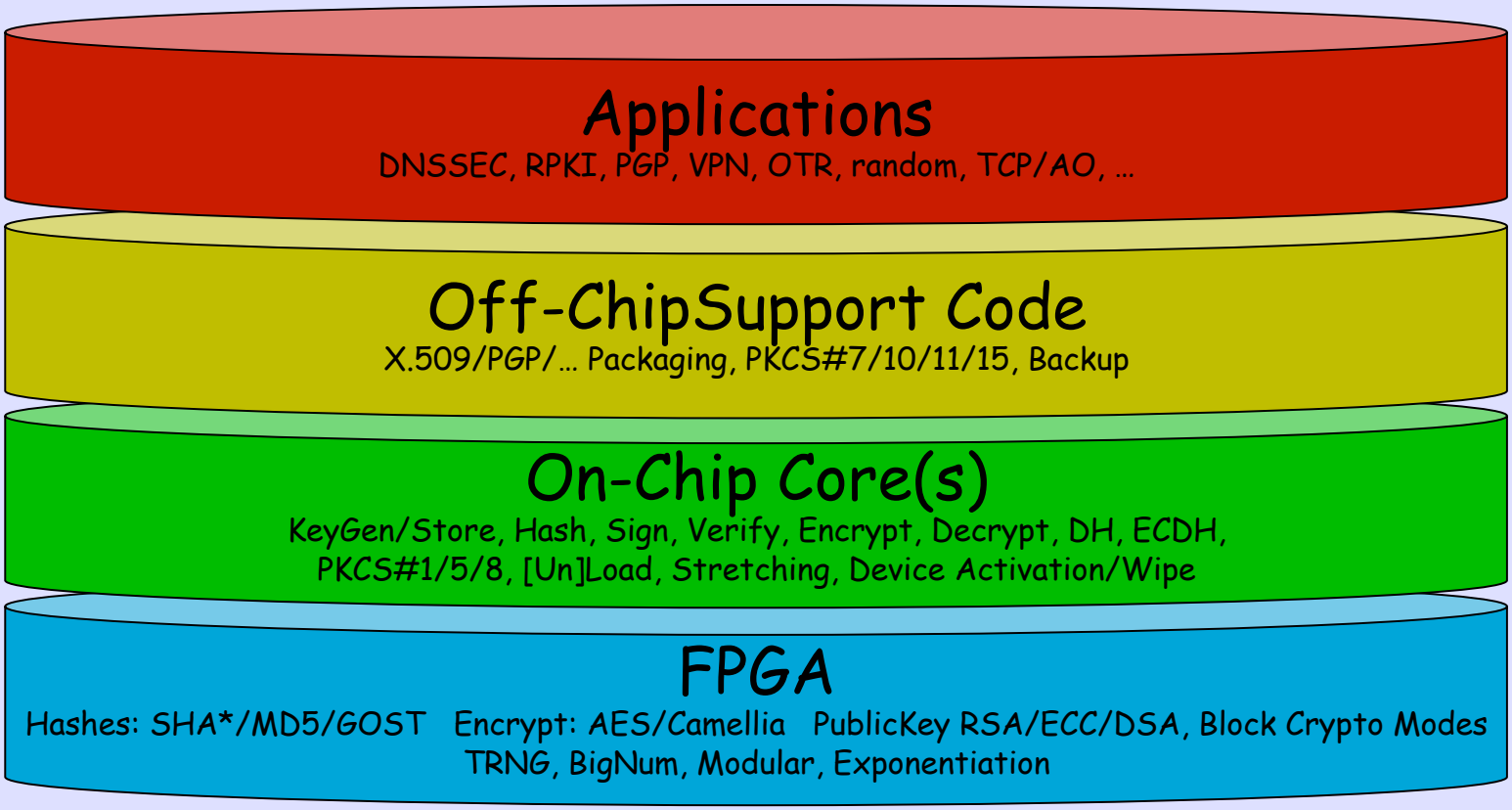
- **An open-source reference design for HSMs**
- Scalable, first cut in an FPGA and CPU, later allow higher speed options
- Composable, e.g. "Give me a key store and signer suitable for DNSsec"
- Reasonable assurance by being open, diverse design team, and an increasingly assured tool-chain

Open and Transparent

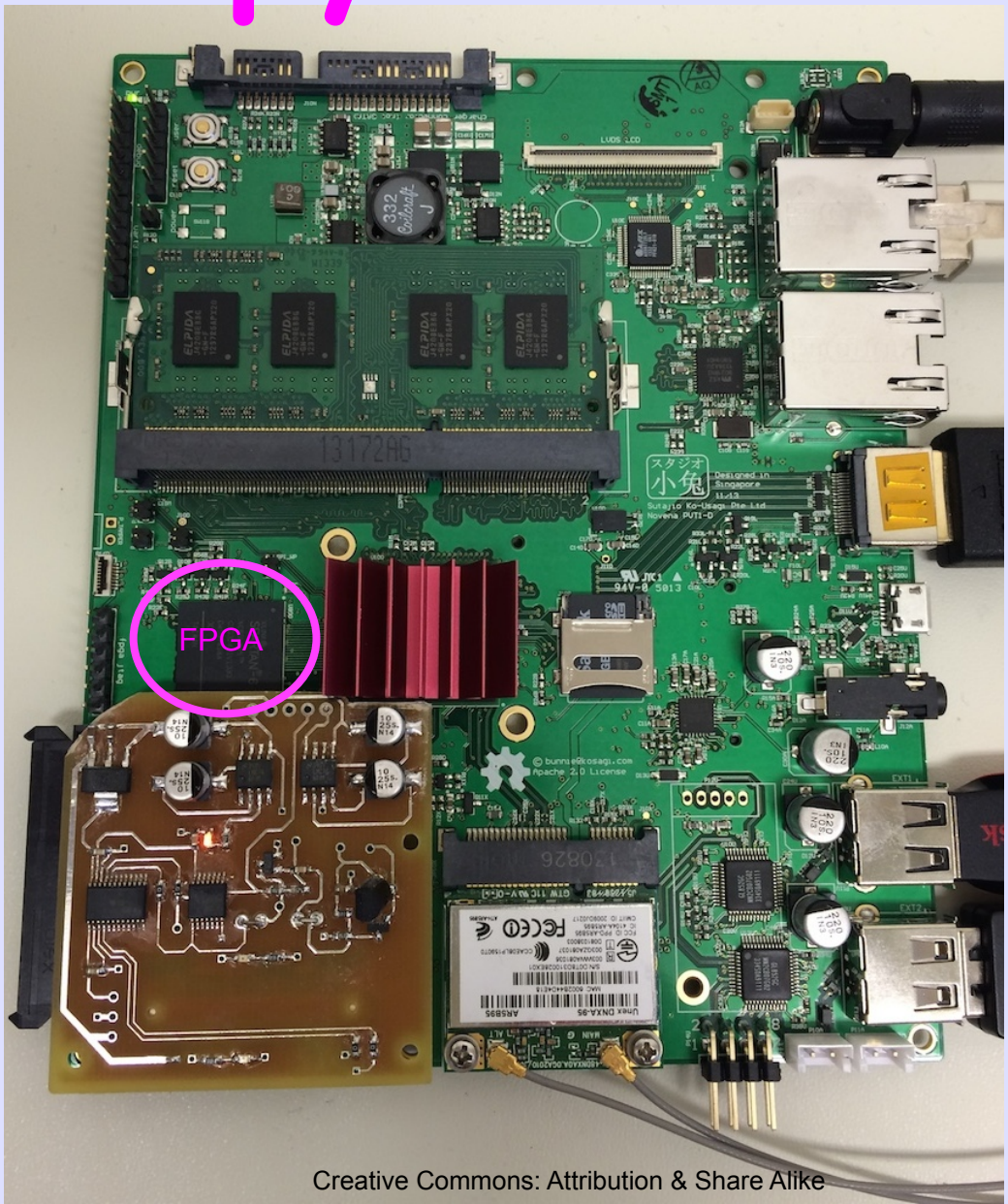
- The project is being run in a maximally **open, transparent** manner with traceability for all decisions etc.
- BSD and CC Licensed
- We do this in order to build trust in the project itself
- And **diverse**, engineering and funding

Funding (so far) From

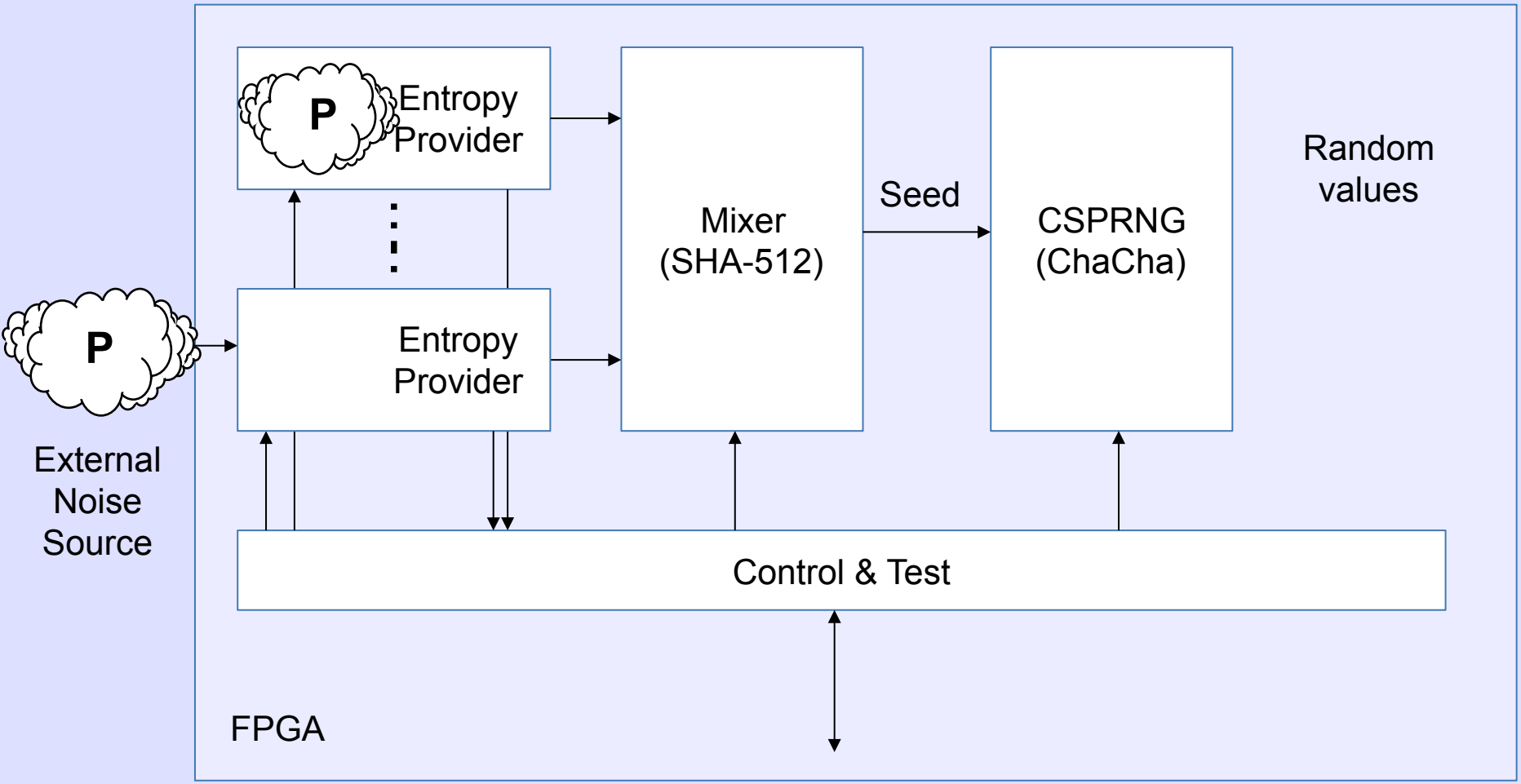
Layer Cake Model



Entropy on Novena



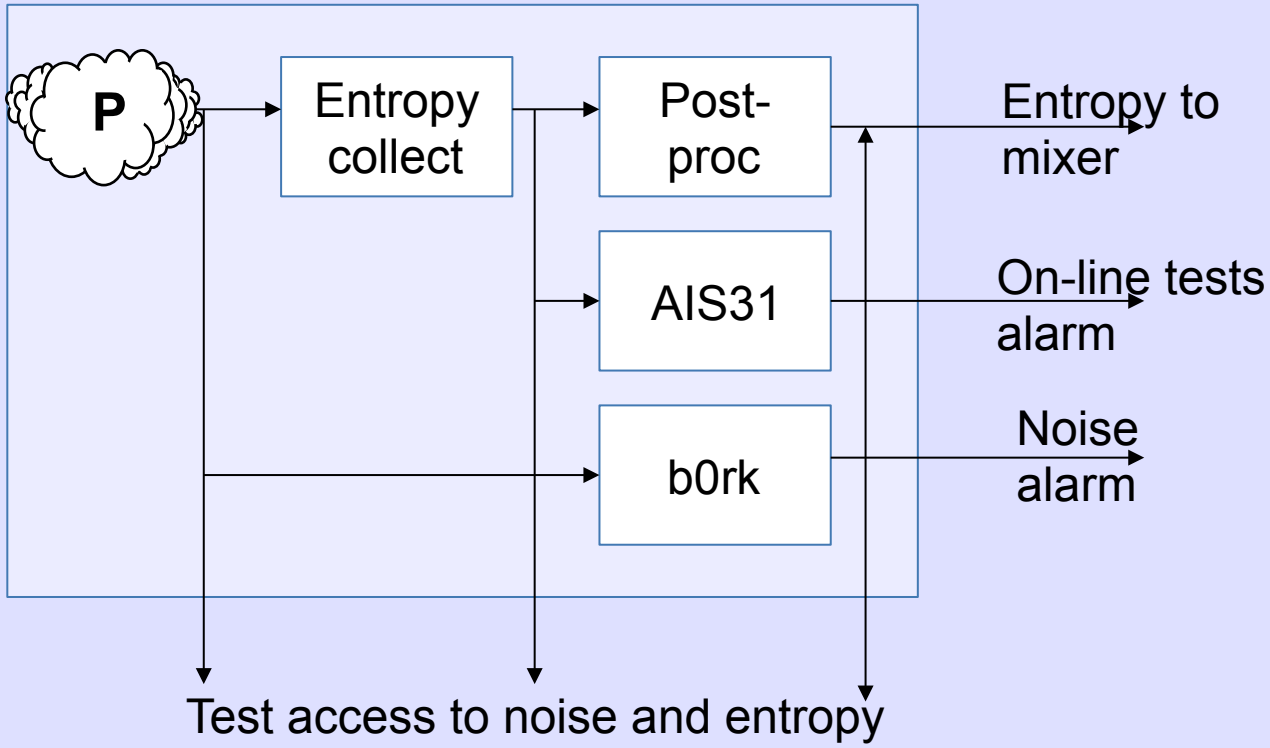
The TRNG Architecture



Test and Observability

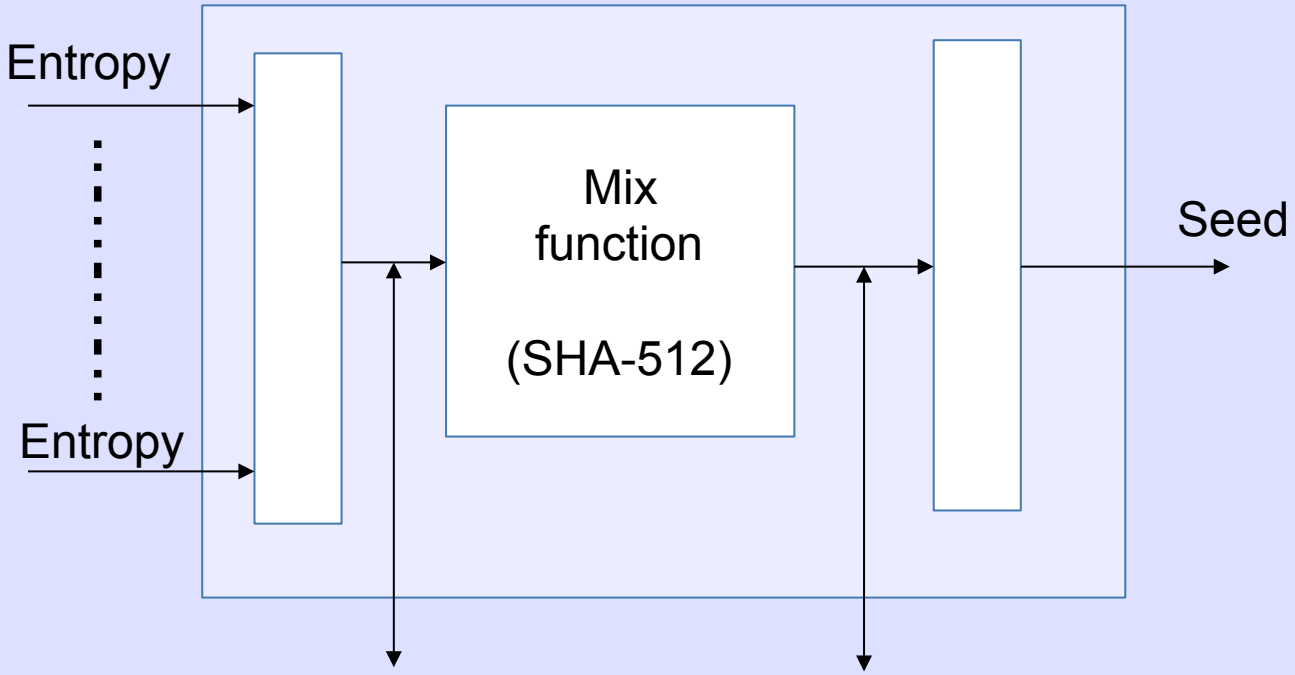
- Two modes
  - Production mode (PM) and Test mode (TM)
- Observability of entropy sources in PM
- Continuous on-line testing in PM
- Injection in stages and complete chain in TM
- Generation of a small number of values in TM
- Allows test of all digital functionality including continuous tests.
- Full restart when moving from TM from/to PM

Observability & Test of Entropy Sources



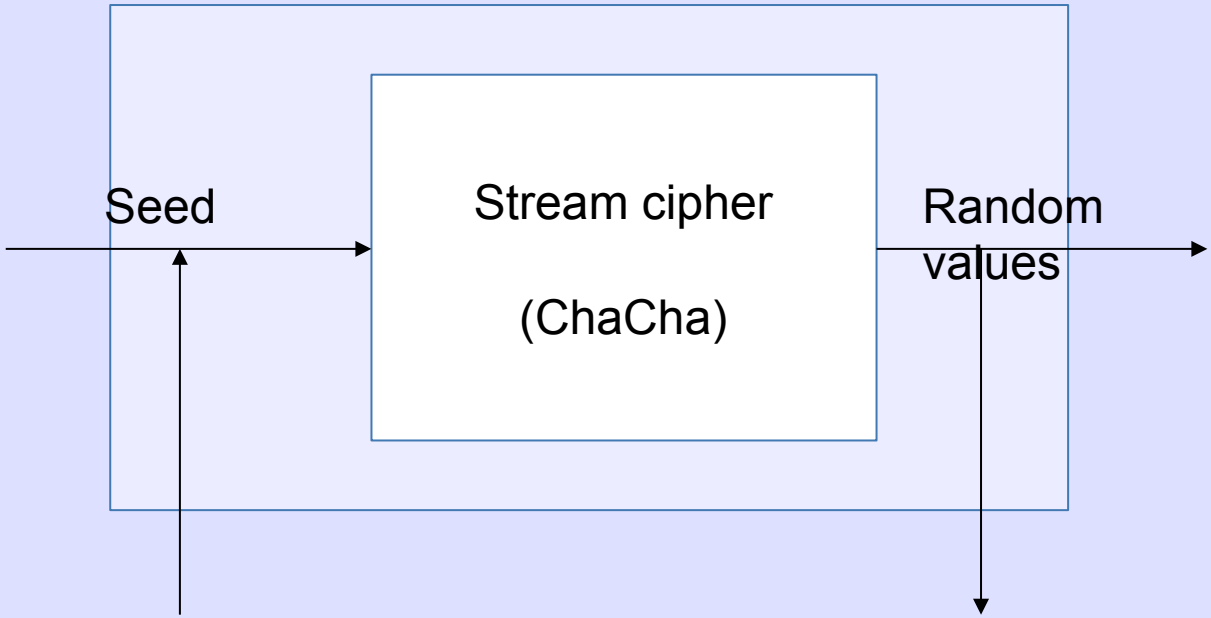
- Extract for off-line comprehensive testing
- Inject for functional testing in test mode

Observability & Test of Mixer



Inject for functional testing in test mode

Observability & Test of CSPRNG



Inject for functional testing in test mode

Some of the Fears

- ToolChain Poisoning
- Device Poisoning
- Side-Channel Attacks
- How can you tell if your vendor actually implemented CrypTech, and correctly?

Side Channel & Tampering

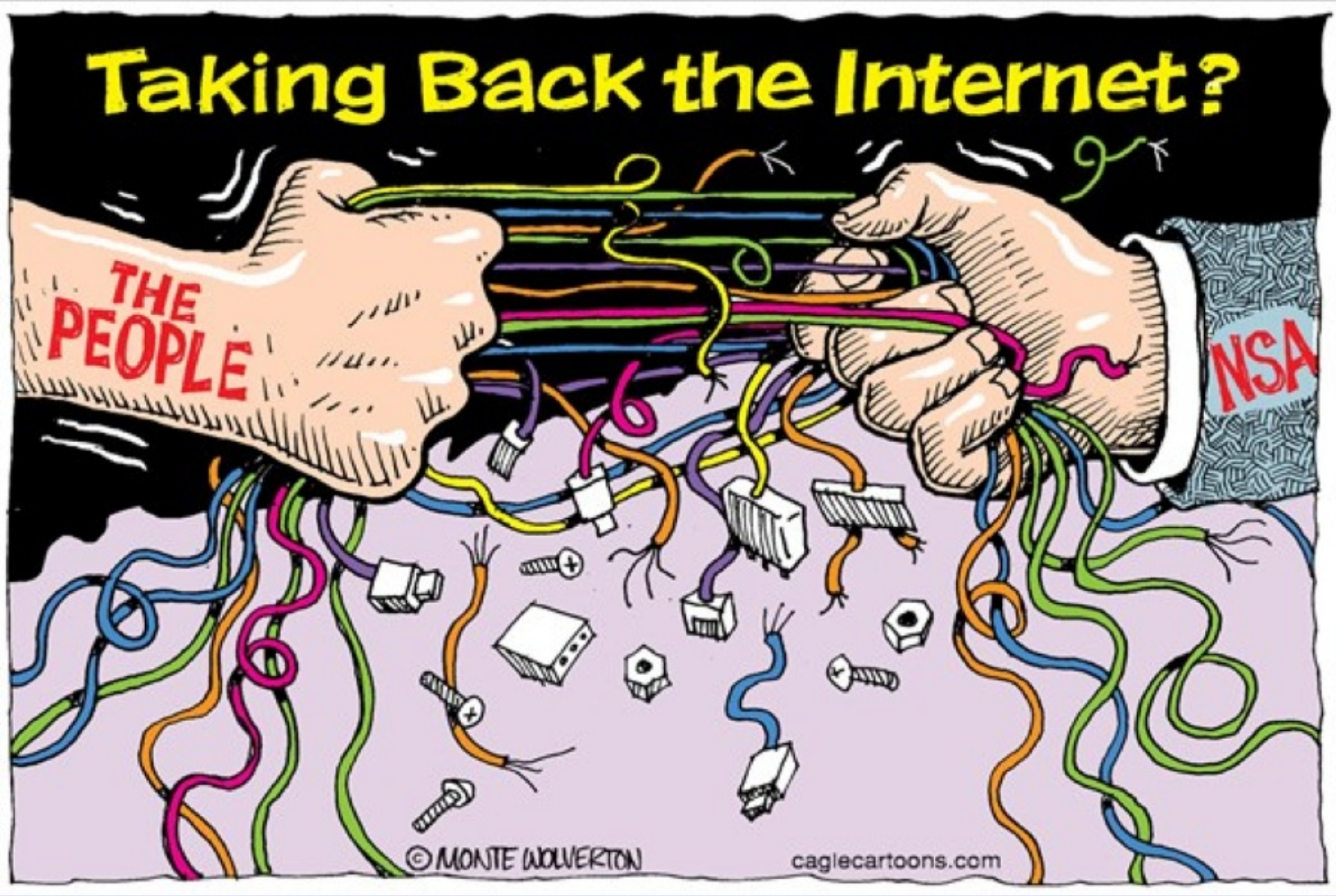
- Slide Deleted ☺

The Tool Chain

- When my laptop's fan goes on, I think it is the NSA, GCHQ, Israelis, Chinese, … fighting to see who will own me
- We have NO ASSURANCE of our tool set, from CPU to Kernel to Compiler to …
- When constructing assurance-critical tools, we need to maximize assurance in the tools used to build them

Some Phases

- First Year: Tool-chain, Basic Design, not all cyphers, not all protocols, prototype implementations on FPGAs and boards
- Second Year: Better Tool-chain, all needed cyphers, hashes, crypting, … and integration with some apps, DNSsec, RPKI, TLS, PGP, Tor
- Third Year: Solid packaging, ability to compose designs for use cases, etc.



https://cryptech.is/