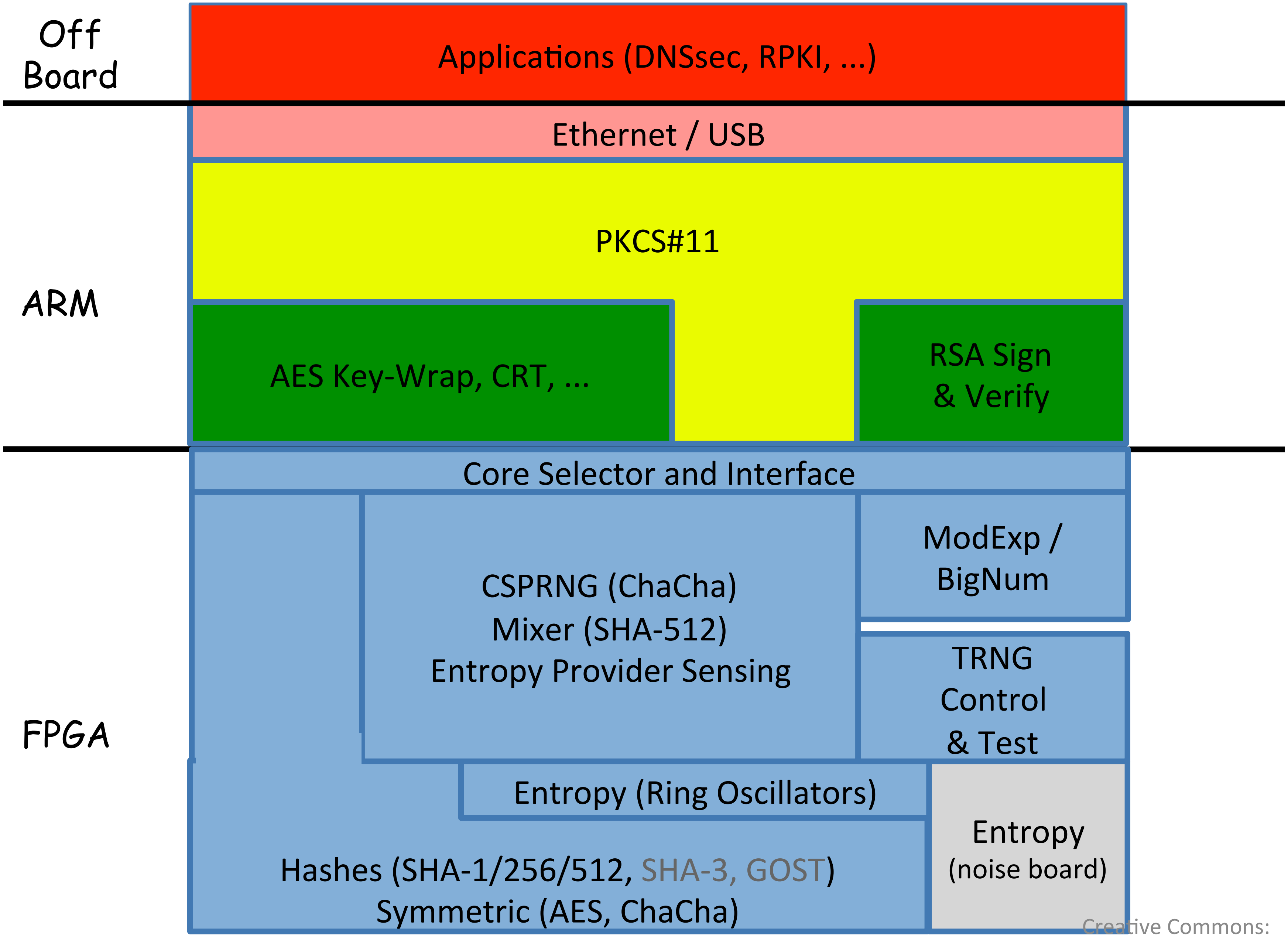
Intro to CrypTech

22 July 2015

cfrg @ IETF93

CrypTech

- Motivated by loss of trust in cryptographic algorithms and products
    - Resulting from revelations on pervasive monitoring and potentially compromised algorithms and products
- Open source cryptographic hardware engine design
    - Transparent development and funding
    - Resulting in an open source reference design
    - Anyone can then adapt to their own products or requirements
- Project estimated timeline of three years
    - 1.5 years completed



Off Board

Applications (DNSsec, RPKI, ...)

Ethernet / USB

ARM

PKCS#11

AES Key-Wrap, CRT, ...

RSA Sign & Verify

FPGA

Core Selector and Interface

CSPRNG (ChaCha)
Mixer (SHA-512)
Entropy Provider Sensing

ModExp / BigNum

TRNG Control & Test

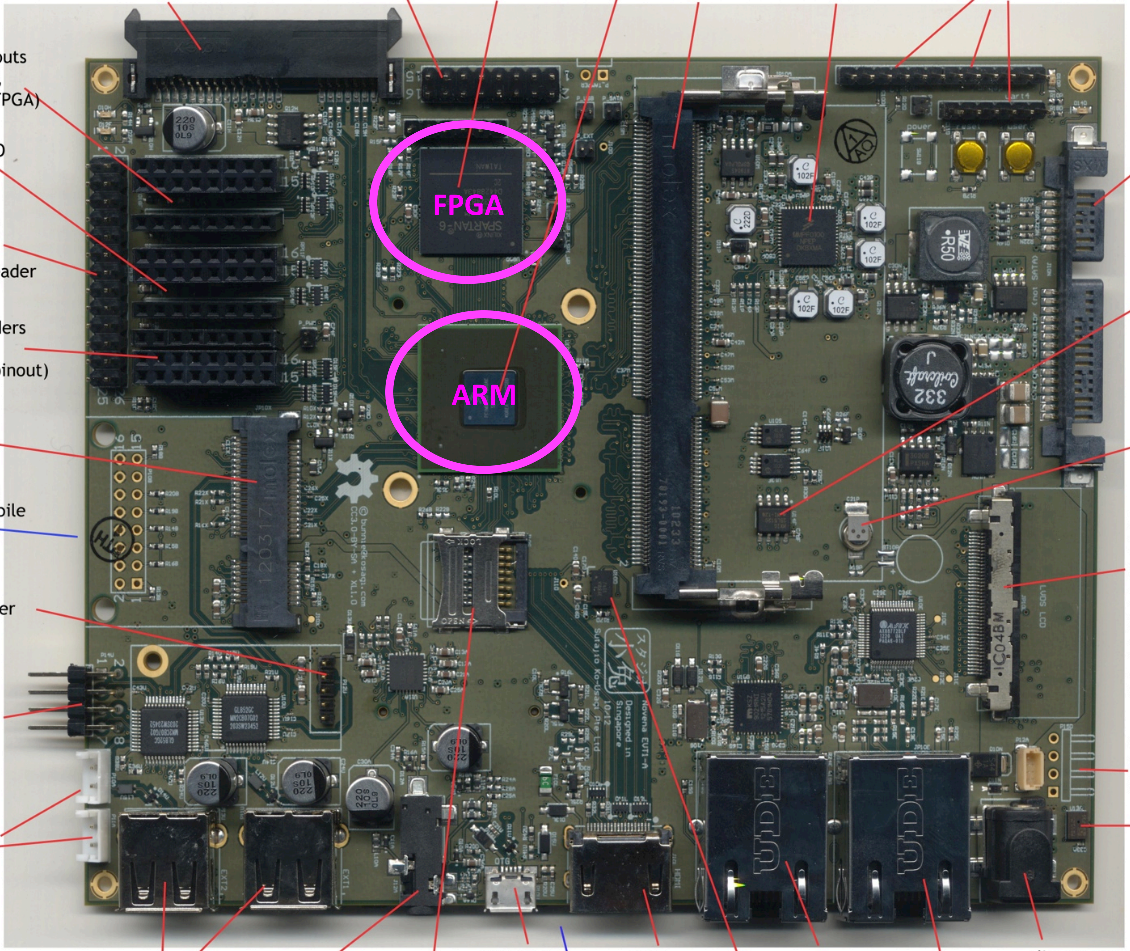
Entropy (Ring Oscillators)

Hashes (SHA-1/256/512, SHA-3, GOST)
Symmetric (AES, ChaCha)

Entropy
(noise board)

Novena Spartan ‘Laptop’

Slide from
Randy Bush



SATA-II

Supplemental
digital I/O port
(via CPU)

Spartan 6 FPGA
CSG324 pinout

i.MX6 CPU (1.2 GHz quad Cortex A9 capable)

DDR3 SO-DIMM

PMIC

3x UART ports
(FTDI pinout)

8x Analog inputs
(up to 12 bit,
200ksps via FPGA)

8x digital I/O
(via FPGA)

Raspberry-Pi
compatible
expansion header
(via CPU)

8x PWM headers
(ESC/servo
compatible pinout)
(via FPGA)

mPCIe

UIM (bottom
side) for mobile
data cards

USB wifi
module header
(AW-NU137)

2x internal
USB ports
(for KB &
mouse)

Internal
amplified
speaker
drivers
(1.1W into
8 ohms)

Battery
board
interface

Utility
EEPROMs
(crashlogs,
etc.)

RTC backup
supercap
(optional
battery)

LVDS LCD
port: dual-
channel,
EIA-644A
plus USB
for camera &
LED backlight
(up to
QXGA res)

direct drive
for resistive
touchscreen

digital
microphone

USB2.0 ports
(high-current capable)

headphone +
mic (compatible
with most mobile
phone kits)

microSD
boot FLASH

USB OTG

SD card socket
(bottom side)

HDMI

3-axis accelerometer

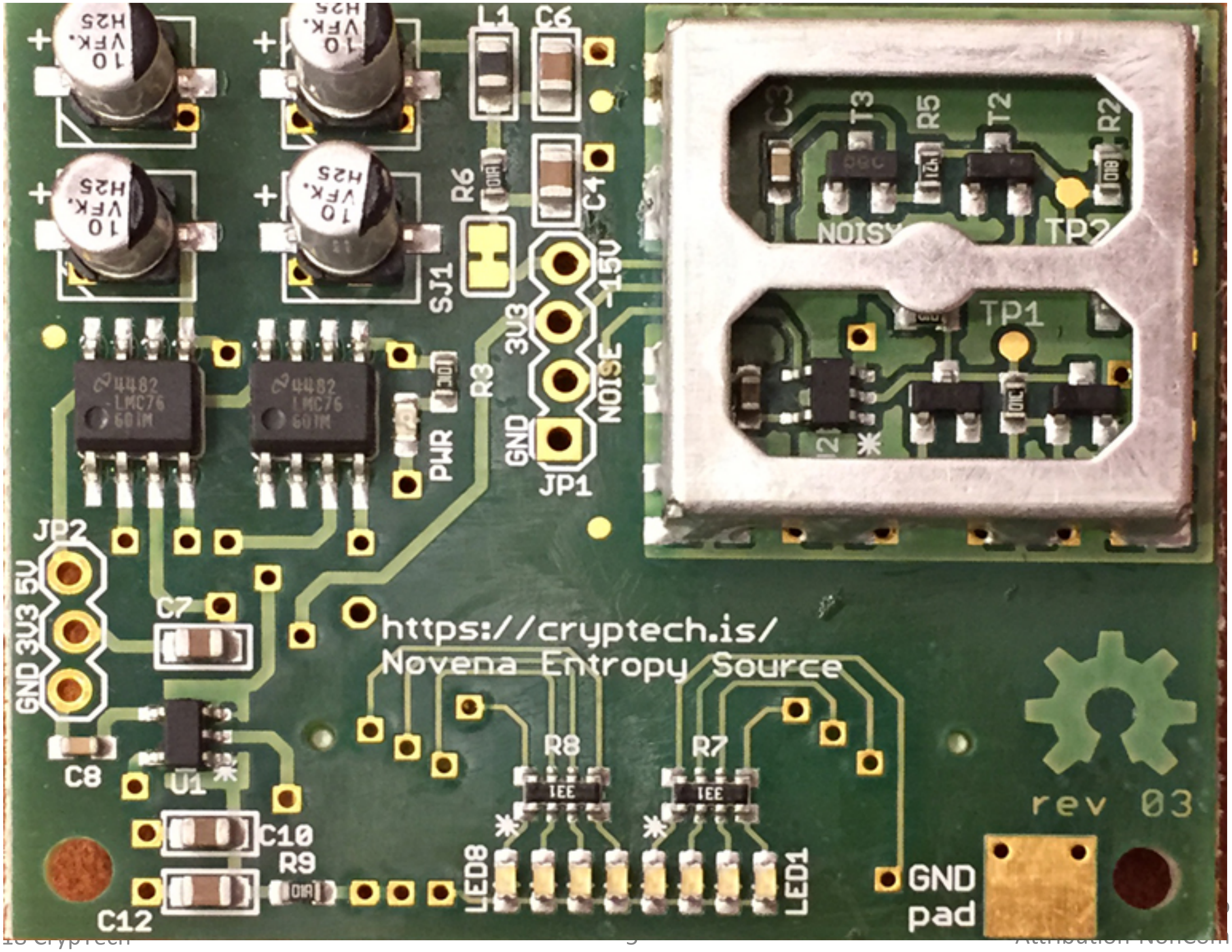
1 Gbit
ethernet

100 Mbit
ethernet

direct power
(for configurations
without battery)

150718 CrypTech
Creative Commons: Attribution-NonCommercial-ShareAlike 2.0
4

Avalanche Noise Board



For More Information:

- Nerds who are still here
  - Randy Bush, Rob Austein, other members of the core team

- Links:
  - Main website: https://cryptech.is
  - Project wiki: https://trac.cryptech.is/wiki
  - Slide set from Saturday's workshop: http://archive.psg.com/150718.cryptech.pdf
  - Blog post on one experience at Saturday's workshop https://blog.apnic.net/2015/07/21/its-alive-blinkenlights-in-cryptech-ietf93/

How can you participate?

- Contribute to the development effort (send verilog!).
  - Participate in the public mailing list…
  - Submit use cases

- Discuss how to help others transition this design into products?

- Support fund raising activities.
  - Original budget $1M/year, currently operating at $500K/year
    1. Are there specific people or resources that might be engaged to help the fund raising effort?
    2. Are there any suggested contacts that should be pursued for funding.
    3. Are there other approaches or venues that we haven't thought about.
  - Donations can be made to CrypTech via NORDUnet or the Internet Society.
    - https://cryptech.is/funding/
    - Click on "How to donate to the CrypTech project" link.