Cryptech Alpha hardware overview

fredrik@thulin.net

Berlin, 2016-07

Revisions

- rev01 - dev-bridge board
  - schematics made in Eagle CAD
- rev02 - 4” by 4” NUC form factor
  - schematics converted to Altium Designer
- rev03 - 120 by 100 mm Eurocard form factor
  - Moved power connector to the same side as USB connectors
  - Removed non-functional RX/TX LEDs
  - Added copper polygons around USB connectors

Main components

- Xilinx Artix-7 FPGA
- STM32 ARM Cortex-M4
- AVR ATtiny 828 8-bit tamper subsystem MCU

- FTDI FT232H USB UART chips

- 2x512 Mbit SDRAM (2x64 MByte)
- Volatile master key memory
- Non-volatile keystore memory (64 Mbit / 8 MByte)

- Avalanche Noise entropy source

FPGA

- Because trusting MCUs is hard
- Great speed potentials, but maybe not there yet
- Ours is huge, to not limit development
- Currently a big part of the BOM cost
- 16 length-matched high speed GPIOs

STM32 MCU

- Some things are really hard to do in an FPGA
  - Primality testing
  - POST testing of entropy
  - …
- Wanted to use A7 / A9, DDR3 memory too complex
- Took the largest, fastest M4 we could find
  - 180 MHz
  - 32 bit data + 24 bit address FMC bus
  - 2 MByte internal flash for code
- Could definitely use more speed here

Tamper MCU

- Deliberately not field upgradable
    - Can be flashed with Arduino, R-Pi or https://www.sparkfun.com/products/9825

- Controls the FPGAs access to the master key memory
- PANIC button
- 8 GPIOs

FTDI UART chips

- Black-box chips to do UART<->USB
- Conceptually outside the security boundary
- Peter Stuge is proposing a somewhat less black-box alternative

Memories

- Volatile master key memory, connected to the FPGA
    - Need not be bigger than a few hundred bytes
- Non-volatile keystore memory, connected to the STM32
    - Current chip should allow storage of
        - 3000 RSA-8192 keys
        - 6000 RSA-4096 keys
        - 80000 EC P-256 keys
- 128 MByte SDRAM, allows for serious POST testing of entropy

Avalanche noise source

- One of two noise sources currently
- Produces ~15 kbit noise per second
- Samples 50 MHz timer LSB on rising flanks
- Shielded
- Might age

Power

- The Alpha accepts approximately 17-20 VDC
- Uses somewhat expensive DC-DC step-down converters with low noise
- Intermediate 5 volts
- 1V0, 1V8 and 3V3 rails
- 15V for entropy source