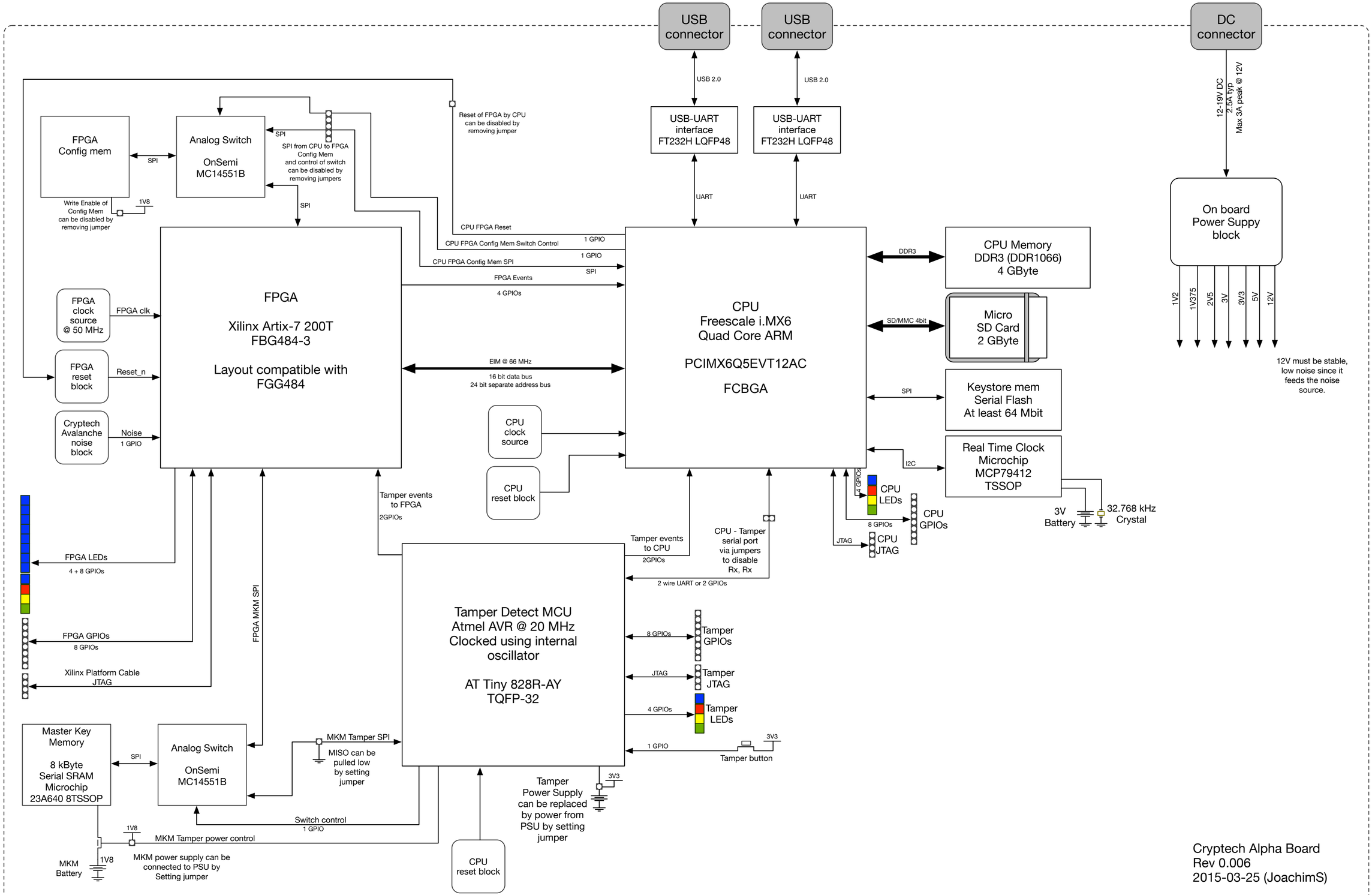
USB connector
USB connector
DC connector
USB 2.0
USB 2.0
USB-UART interface FT232H LQFP48
USB-UART interface FT232H LQFP48
UART
UART
12-19V DC
2.5A typ
Max 3A peak @ 12V
On board Power Suppy block
1V2
1V375
2V5
3V
3V3
5V
12V
12V must be stable, low noise since it feeds the noise source.
FPGA Config mem
SPI
Analog Switch
OnSemi MC14551B
SPI
SPI from CPU to FPGA Config Mem and control of switch can be disabled by removing jumpers
Reset of FPGA by CPU can be disabled by removing jumper
Write Enable of Config Mem can be disabled by removing jumper
1V8
SPI
CPU FPGA Reset
CPU FPGA Config Mem Switch Control
1 GPIO
CPU FPGA Config Mem SPI
1 GPIO
SPI
FPGA Events
4 GPIOs
FPGA clock source @ 50 MHz
FPGA clk
FPGA reset block
Reset_n
Cryptech Avalanche noise block
Noise
1 GPIO
FPGA
Xilinx Artix-7 200T
FBG484-3
Layout compatible with FGG484
EIM @ 66 MHz
16 bit data bus
24 bit separate address bus
CPU clock source
CPU reset block
CPU
Freescale i.MX6
Quad Core ARM
PCIMX6Q5EVT12AC
FCBGA
DDR3
CPU Memory
DDR3 (DDR1066)
4 GByte
SD/MMC 4bit
Micro SD Card
2 GByte
SPI
Keystore mem
Serial Flash
At least 64 Mbit
I2C
Real Time Clock
Microchip
MCP79412
TSSOP
3V Battery
32.768 kHz Crystal
4 GPIOs
CPU LEDs
8 GPIOs
CPU GPIOs
JTAG
CPU JTAG
Tamper events to FPGA
2GPIOs
Tamper events to CPU
2GPIOs
CPU - Tamper serial port via jumpers to disable Rx, Rx
2 wire UART or 2 GPIOs
FPGA LEDs
4 + 8 GPIOs
FPGA GPIOs
8 GPIOs
Xilinx Platform Cable JTAG
FPGA MKM SPI
Tamper Detect MCU
Atmel AVR @ 20 MHz
Clocked using internal oscillator
AT Tiny 828R-AY
TQFP-32
8 GPIOs
Tamper GPIOs
JTAG
Tamper JTAG
4 GPIOs
Tamper LEDs
1 GPIO
3V3
Tamper button
Master Key Memory
8 kByte
Serial SRAM
Microchip
23A640 8TSSOP
SPI
Analog Switch
OnSemi MC14551B
MKM Tamper SPI
MISO can be pulled low by setting jumper
Switch control
1 GPIO
1V8
MKM Tamper power control
MKM Battery
1V8
MKM power supply can be connected to PSU by Setting jumper
CPU reset block
Tamper Power Supply can be replaced by power from PSU by setting jumper
3V3
Cryptech Alpha Board
Rev 0.006
2015-03-25 (JoachimS)