Cryptowarez

A survey of Hardware Crypto Devices

BSidesPDX

Updated: 17 September 2016

cryptotronix

Overview

1. Introduction
2. Classical
3. Big Iron
4. Embedded

Introduction

Hi, I'm Josh!

○ Owner of Cryptotronix

○ Went around-the-world on a submarine

○ I get sea sick.

I can haz cryptowarez?

So, why do we want crypto hardware?

○ Crypto offloading (algorithm acceleration).

○ Key Protection.

THOSE TWO ITEMS ARE THE FOUNDATION

From those, more advanced security features are built.

Of course, if you undermine those . . . .

Classical

Modern Crypto Hardware

ENIGMA

- ○ First wide-spread modern dedicated crypto hardware
- ○ Performs encipherment and decipherment in human time.
- ○ Key management was a bit of a challenge
- ○ *Not recommended for new designs!!*

Source:
`https://en.wikipedia.org/wiki/Enigma_machine`

Big Iron

Hardware Security Modules

Source: `https://www.thales-esecurity.com`

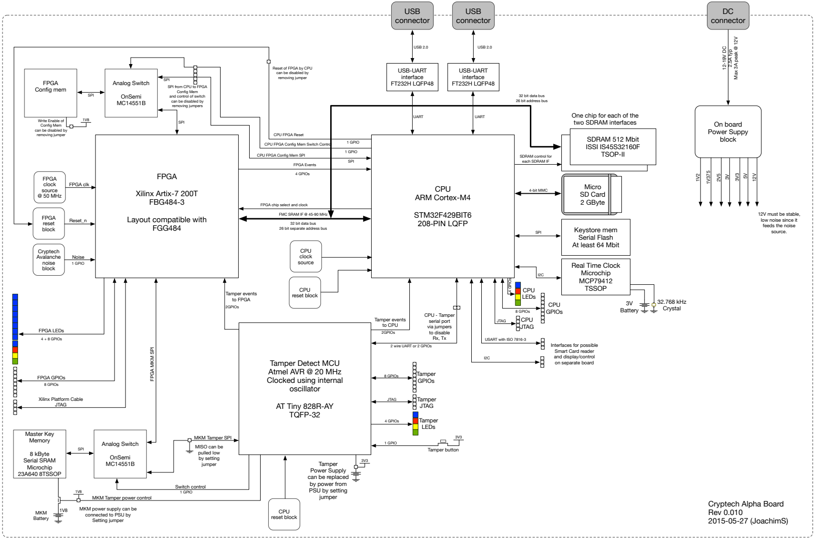
- Up to FIPS 140-2 Level 3
- PKCS#11 Interface, OpenSSL Engine, Java JCE, Microsoft CAPI and CNG.
- Uses: PKI management, code signing, payment processing, file encryption.
- Expensive.
- Cloud providers have some integration now: Azure & AWS.
- Heavily proprietary.

Cryptech: HSMs for the people!

Source: `https://www.crowdsupply.com/cryptech/open-hardware-security-module`

- PKCS#11 over USB
- SHA-1 and 2, RSA and ECDSA (NIST)
- TRNG
- Contains an Artix-7 FPGA, ARM Cortex-M4 and ATtiny828 (for tamper detect)
- Heavily Open: Everything under BSD or CC license

Cryptech: Architecture



USB connector

USB 2.0

USB-UART interface FT232H LQFP48

UART

USB connector

USB 2.0

USB-UART interface FT232H LQFP48

UART

DC connector

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

SPI

Write Enable of Config Mem can be disabled by removing jumper

1V8

Reset of FPGA by CPU can be disabled by removing jumper

CPU FPGA Reset

1 GPIO

CPU FPGA Config Mem Switch Control

1 GPIO

CPU FPGA Config Mem SPI

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

FPGA chip select and clock

FMC SRAM IF @ 45-90 MHz

32 bit data bus
26 bit separate address bus

32 bit data bus
26 bit address bus

One chip for each of the two SDRAM interfaces

SDRAM 512 Mbit
ISSI IS45S32160F
TSOP-II

SDRAM control for each SDRAM IF

CPU
ARM Cortex-M4

STM32F429BIT6
208-PIN LQFP

4-bit MMC

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

CPU clock source

CPU reset block

4 GPIOs

CPU LEDs

8 GPIOs

CPU GPIOs

JTAG

CPU JTAG

USART with ISO 7816-3

I2C

Interfaces for possible Smart Card reader and display/control on separate board

Tamper events to FPGA

2GPIOs

Tamper events to CPU

2GPIOs

CPU - Tamper serial port via jumpers to disable Rx, Tx

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 0.010
2015-05-27 (JoachimS)

Interns have fun projects!

Digilent Zybo Zynq-7000

IP Core	LUTs	FF
CHACHA20[1]	3585	3727
SHA1[2]	1717	1563
SHA256[3]	2296	1856
SHA512[4]	5310	3735

[1] 50MHz core clock and 250MHz AXI bus (1 round of encryption per core clock) For salsa20, its 20 rounds per block

[2] 100MHz core clock and 100MHz AXI bus (1 round of encryption per core clock)

[3] 70MHz core clock and 70MHz AXI bus (1 round of encryption per core clock)

[4] 60MHz core clock and 60MHz AXI bus(1 round of encryption per core clock)

Embedded

Secure MCUs

Vendor	Product	Proc	Notes
Freescale (NXP)	K80	M4	HRNG, AES, MPU, encrypted flash
STMicro	ST33G1M2A	M3	HRNG, AES, NESCRYPT
Infineon	P SLJ 52ACA	16-bit	AES,ECC,RSA,EAL5+
Microchip	CEC1302	M4	ECC,RSA,SHA,AES,HWRNG, No flash
Maxim	MAX32550	M3	AES,SHA,HWRNG,Secure Boot

Crypto SideCars

Vendor	Product	Notes
Atmel	ATSHA204A	SHA256, HMAC, Open Datasheet
Atmel	ATAES132A	Encrypted 32K EEPROM, Open Datasheet
Atmel	ATECC508A	ECDSA, ECDH, P-256
ST	STSAFE-A100	EAL5+, AES256 KW, ECDSA/ECDH

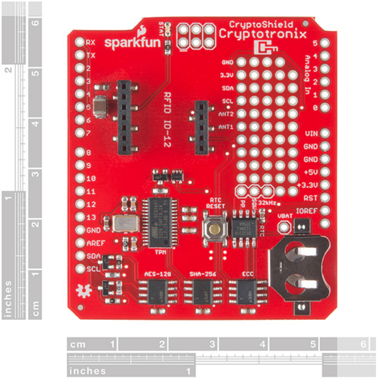
○ 204/508 kernel driver: `https://github.com/cryptotronix/atsha204-i2c`

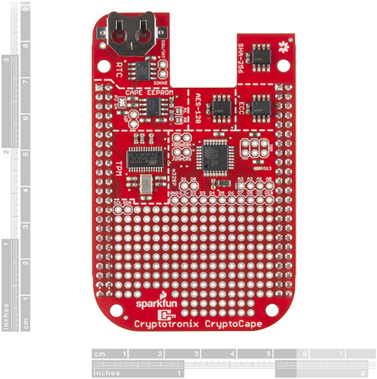
○ 204 cli: `https://github.com/cryptotronix/hashlet`

○ 204/508 lib cli: `https://github.com/cryptotronix/libcrypti2c`

○ 508 cli: `https://github.com/cryptotronix/EClet`

CryptoThings





But wait, there's more!

Lots of other hardware crypto areas, but you know, 20 minutes :(

1. Smart Cards
2. Secure Elements and NFC Controllers
3. PKI USB Tokens
4. U2F Tokens
5. Bitcoin Hardware Wallets
6. A smart card that runs BASIC and ECDSA
7. Crypto IP in most radio MCUs

Growth of hardware crypto

Hardware crypto is growing with IoT. Silicon vendors are expanding the IP which is trickling down to custom ASICs and COTS ICs.

But is that a good thing?

1. Dedicated crypto hardware may reduce software exploits, but it may *increase* hardware attack vectors.
2. Hardware is well, hard to change.
3. Few vendors providing non-NDA and open-distributor access.
4. *A2: Analog Malicious Hardware*

Conclusion

Security Engineering still required

Hardware crypto does not alleviate proper threat modeling and risk mitigation.

We need more Open Crypto!

Vendors have their part in adding security, but tools, knowledge, and application are what will turn the ship.

Das Ende

- ○ `www.cryptotronix.com`
- ○ Just ask for Josh ;)