cryptech.is

IEPG Berlin 2016

https://xkcd.com/525/

What?

cryptech.is is an effort to create an open hardware cryptographic engine design and the tools needed to make it trustworthy.

Why?

RFC 7258/BCP 188
Pervasive Monitoring is an Attack

Who?

cryptech.is is a loose international collective of engineers trying to improve assurance and privacy on the Internet. It is funded diversely and is administratively quartered outside the US.

Internet Society™

Google

COMCAST

CISCO™

Your Public Interest Registry™

SURF NET

Afilias℠

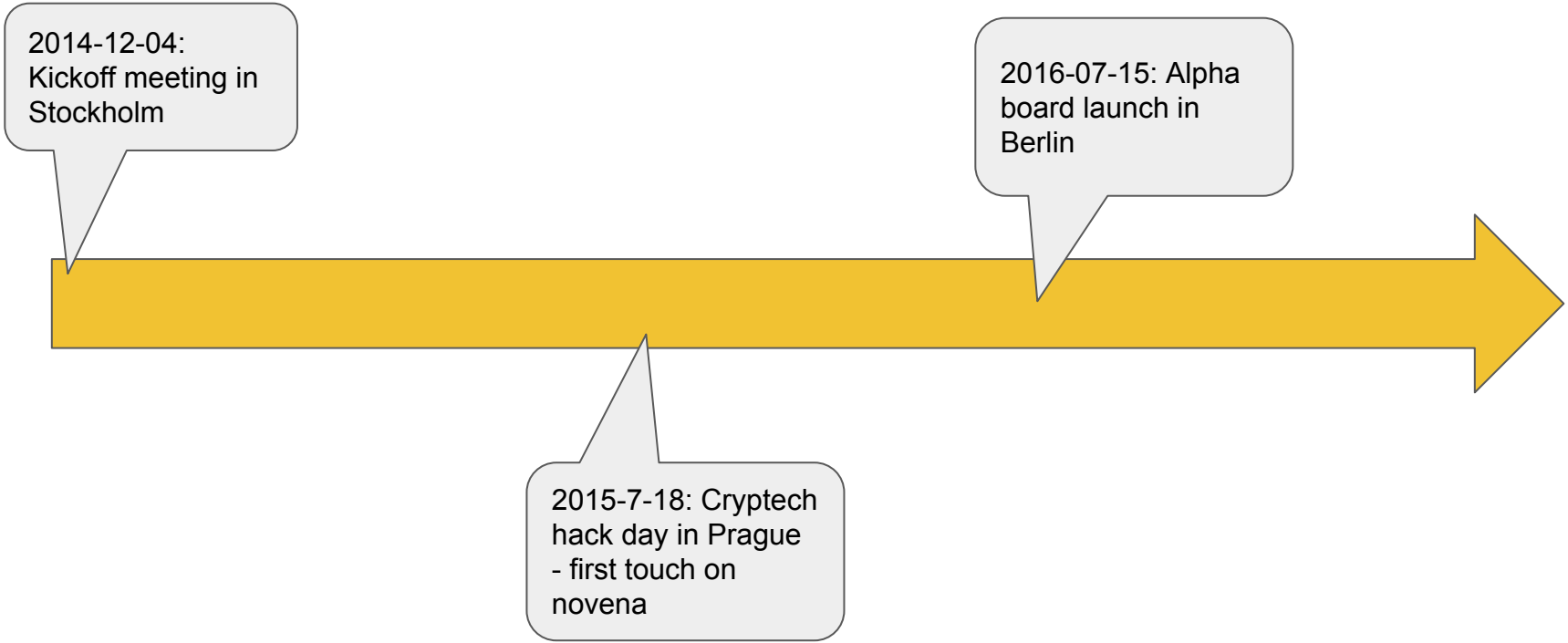
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

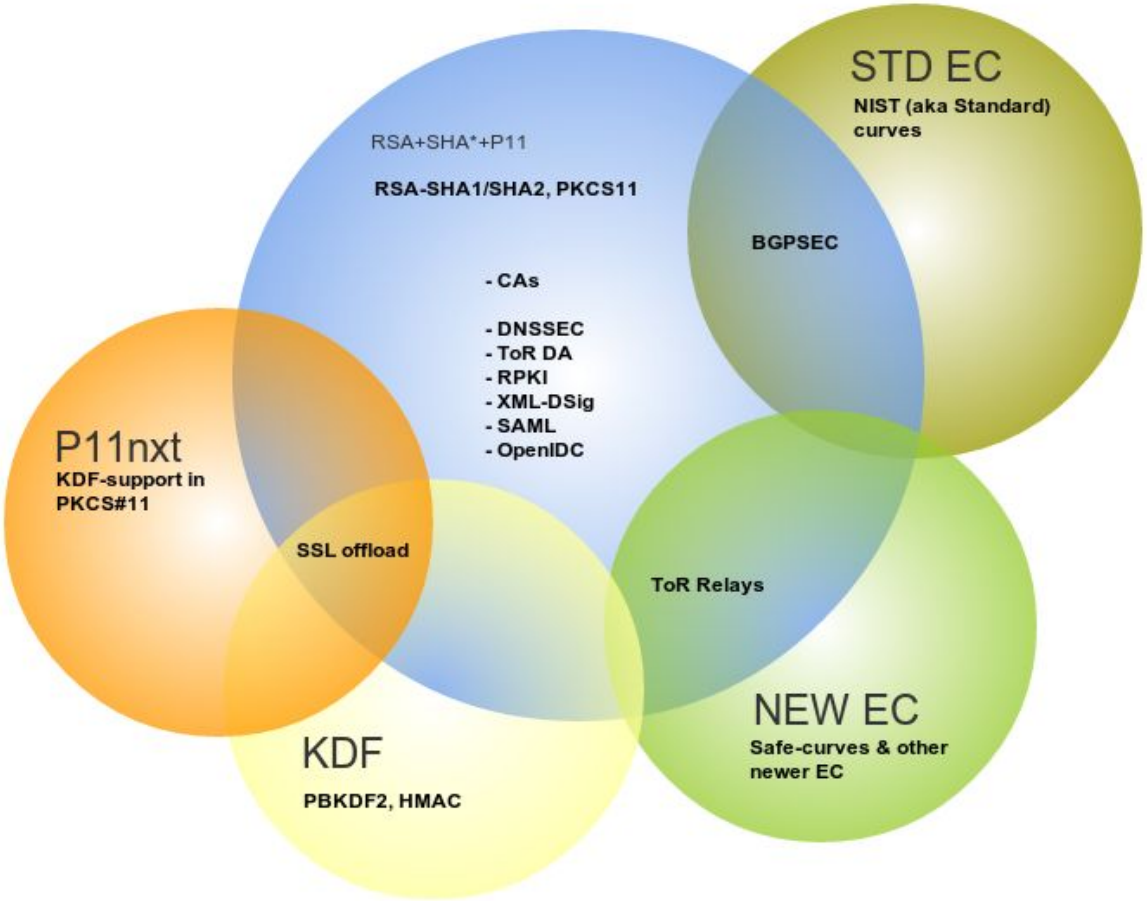
afnic

iis

ICANN

DuckDuckGo


2014-12-04: Kickoff meeting in Stockholm
2015-7-18: Cryptech hack day in Prague - first touch on novena
2016-07-15: Alpha board launch in Berlin


RSA+SHA*+P11
RSA-SHA1/SHA2, PKCS11
- CAs
- DNSSEC
- ToR DA
- RPKI
- XML-DSig
- SAML
- OpenIDC
STD EC
NIST (aka Standard) curves
BGPSEC
P11nxt
KDF-support in PKCS#11
SSL offload
ToR Relays
KDF
PBKDF2, HMAC
NEW EC
Safe-curves & other newer EC

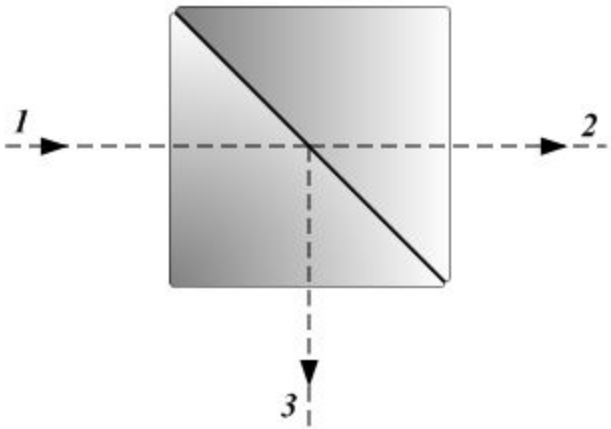
https://xkcd.com/824/

Cheap, fast, stable

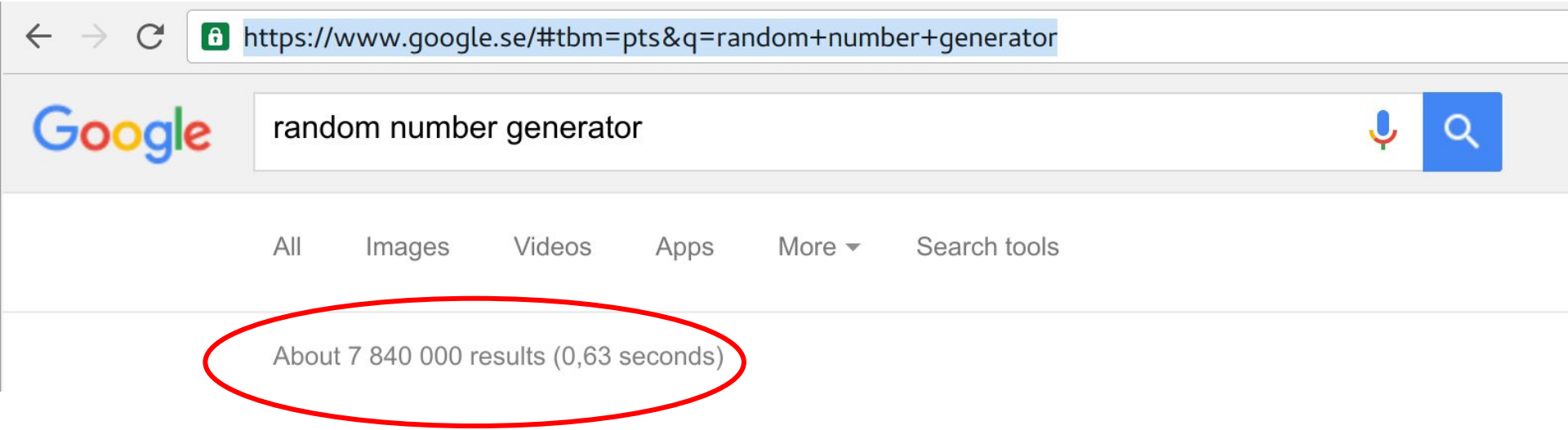
- Cheap to produce
- Hard to attack
- IPR-unencumbered

Method for seeding a pseudo-random number generator with a cryptographic hash of a digitization of a chaotic system

US 5732138 A


1
2
3

google patent search

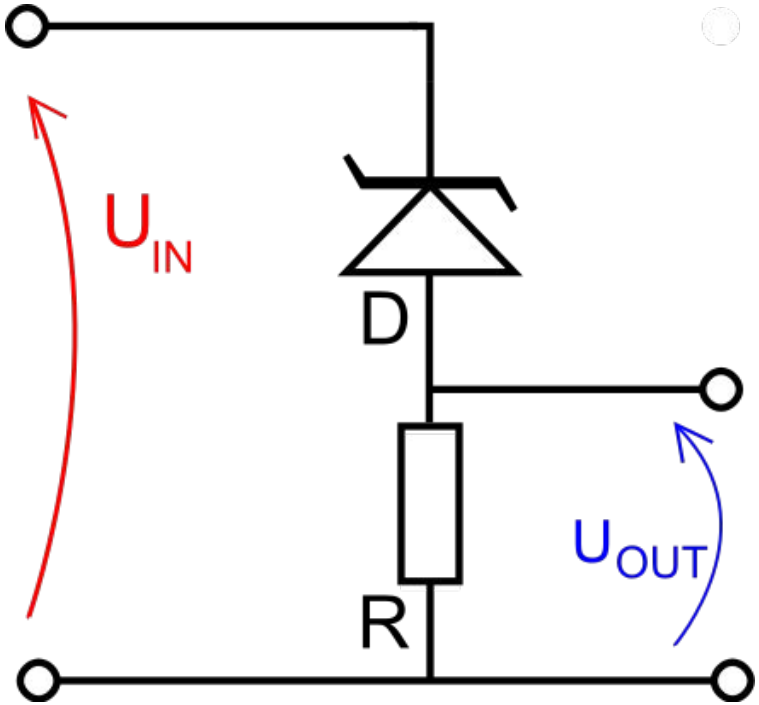


Only noisy diode good

(because the patent already expired)

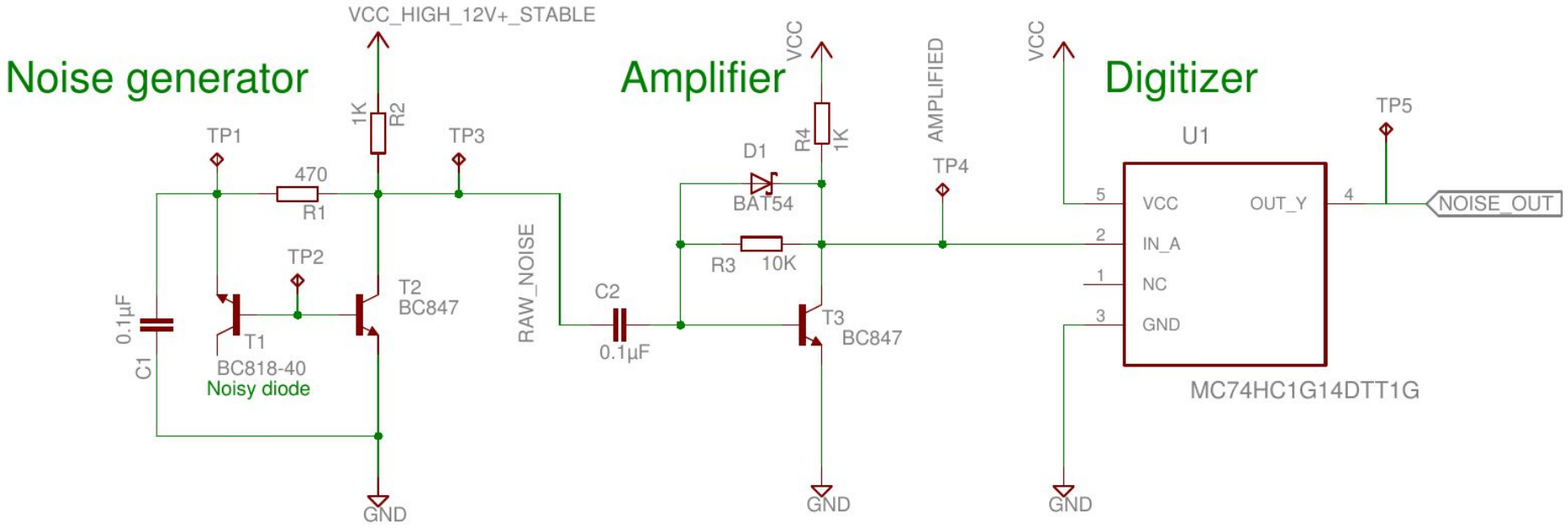
Cheap, fast, stable

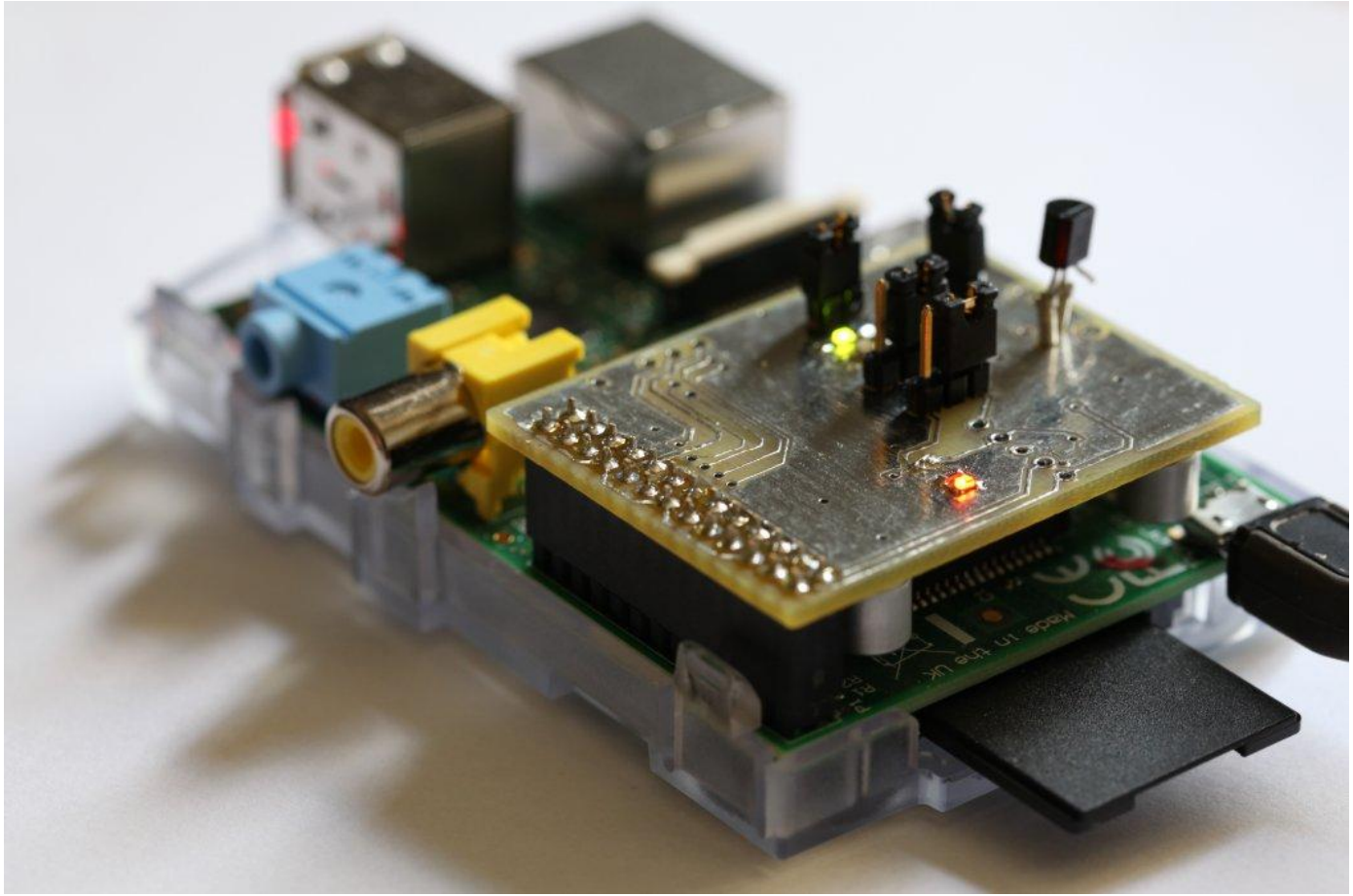
- Many many diodes to choose from
- Really really cheap
- Still quite hard to get it right...



Entropy

1. Pick a source (only noisy diode good)
2. Methodology - free running counter @50 MHz, sample LSB on noise flanks. Not ADC.
3. Sample without introducing artifacts (ARM DMA timer capture / FPGA)
4. De-correlate samples in software (whitening, lossy processing)

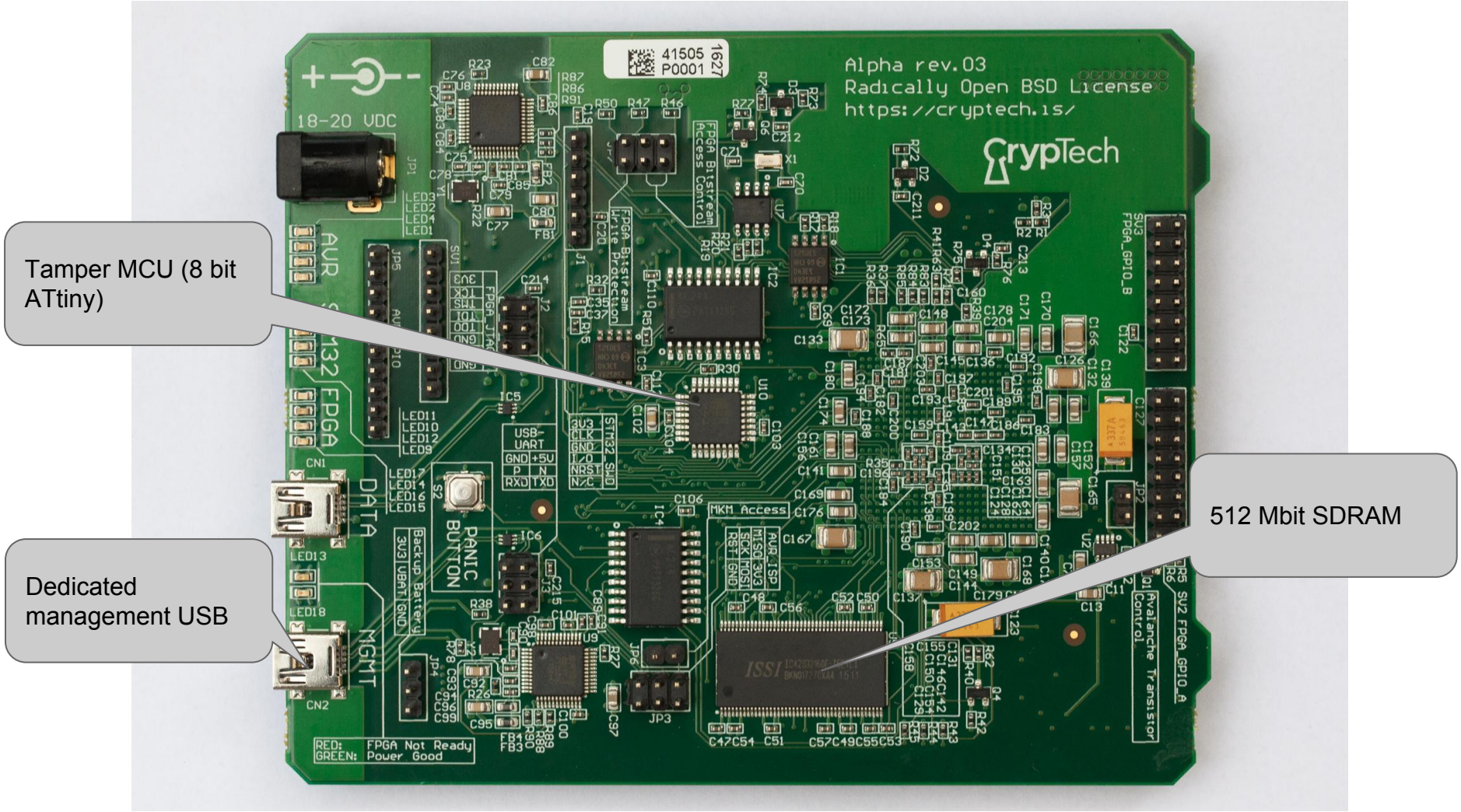

Noise generator
Amplifier
Digitizer
VCC_HIGH_12V+_STABLE
TP1
TP2
TP3
TP4
TP5
1K
R2
470
R1
0.1µF
C1
T1
BC818-40
Noisy diode
T2
BC847
GND
RAW_NOISE
C2
0.1µF
VCC
R4
1K
D1
BAT54
R3
10K
T3
BC847
GND
AMPLIFIED
VCC
U1
5
VCC
2
IN_A
1
NC
3
GND
OUT_Y
4
NOISE_OUT
MC74HC1G14DTT1G
GND



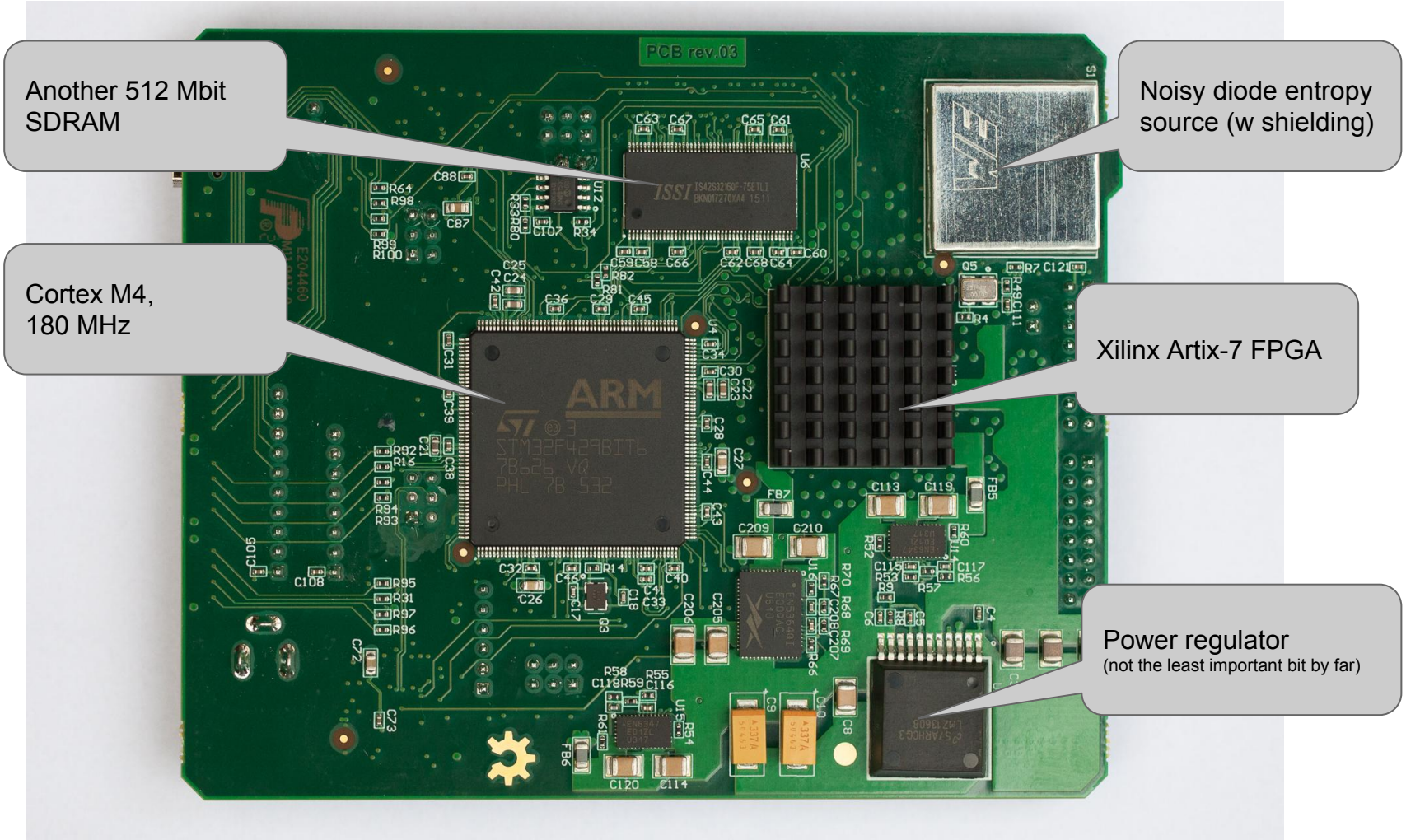
Noise-board on-a-Pi

And now...

Alpha rev.03
Radically Open BSD License
https://cryptech.is/
CrypTech
18-20 VDC
AVR STM32 FPGA
DATA
MGMT
PANIC BUTTON
USB-UART
MKM Access
FPGA Bitstream Access Control
FPGA Bitstream Write Protection
Avalanche Transistor Control
RED: FPGA Not Ready
GREEN: Power Good


Tamper MCU (8 bit ATtiny)
512 Mbit SDRAM
Dedicated management USB
Alpha rev.03
Radically Open BSD License
https://cryptech.is/
CryptTech
18-20 VDC
AVR
132 FPGA
DATA
MGMT
PANIC BUTTON
USB-UART
MKM Access
Avalanche Transistor Control
RED: FPGA Not Ready
GREEN: Power Good

PCB rev.03
ARM
STM32F429BIT6
ISSI
IS42S32160F-75ETLI
LM2596HVS-5.0
EN5364QI
EG0004C
A337A
S1
U1
U2
U4
U6
U8
U9
U10
U11
U14
U15
Q3
Q5
Q6
C1
C2
C3
C4
C8
C9
C10
C12
C60
C61
C63
C65
C67
C88
C87
C107
C105
C108
C72
C73
C120
C114
C113
C119
C115
C117
C116
C118
C209
C210
C206
C205
C208
C207
C32
C26
C25
C24
C42
C36
C29
C45
C31
C39
C38
C21
C22
C23
C30
C28
C27
C44
C43
C40
C41
C33
C17
C18
C46
R64
R98
R99
R100
R92
R16
R94
R93
R95
R31
R97
R96
R33
R80
R34
R82
R81
R14
R7
R4
R49
R60
R52
R53
R39
R57
R56
R70
R68
R69
R67
R66
R58
R59
R55
R54
R65
FB7
FB5
FB6
E204460
MU1 94V-0


Another 512 Mbit SDRAM
Noisy diode entropy source (w shielding)
Cortex M4, 180 MHz
Xilinx Artix-7 FPGA
Power regulator
(not the least important bit by far)
PCB rev.03
ARM

FPGA vs CPU

Why not spend $ on bigger CPU?

- FPGA gives you some benefits
  - constant-time implementations of crypto
  - no pointers or stack corruption
- Do you want your HSM to have an HDMI interface and a sound card?

Trade-off isn’t clear.

Part of the goal of the alpha is to figure this stuff out...

Do you ~~need~~ want one?

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

Maybe, if you...

- use HSMs today but think they are too …
  - expensive
  - complex
  - untrustworthy
  - …
- don’t use HSMs today but think you probably should/might want to
- have an application that needs to run custom code inside the trust boundary
- are looking for a platform for Verilog crypto primitives
- *want to reuse one of our designs but need a “dev board” to play with first*
- **want to help us make cryptech better!**

What it is not

- Production ready (but it might still be useful in your lab setup)
- Fast (but that will improve)

n€xt

- Make the FPGA pay for itself
- Work on tamper circuitry
- More features in the pkcs11 interface