

Brute-Forcing Lockdown Harddrive PIN Codes

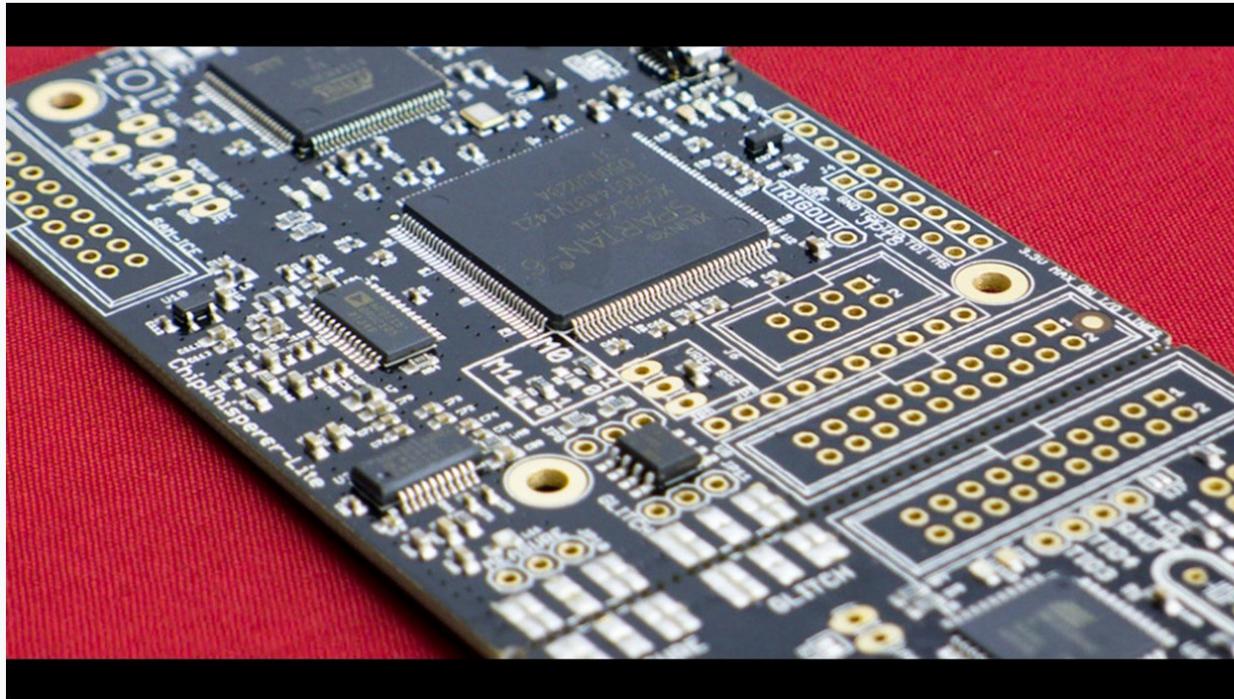


Colin O'Flynn



About Me

ChipWhisperer-Lite: A New Era of Hardware Security Research



Embedded security - is it an oxymoron? Learn the truth through a series of hands-on labs targeting computer and electrical engineers.

Created by

Colin O'Flynn



331 backers pledged \$88,535 CAD to help bring this project to life.

TYPES OF SECURE DRIVES



Previous Work

Joffrey Czarny & Raphaël Rigo

Presentation at Hardwear.io:

http://hardwear.io/wp-content/uploads/2015/10/Slide-hardware_re_for_software_reversers-By-Czarny-Rigo.pdf

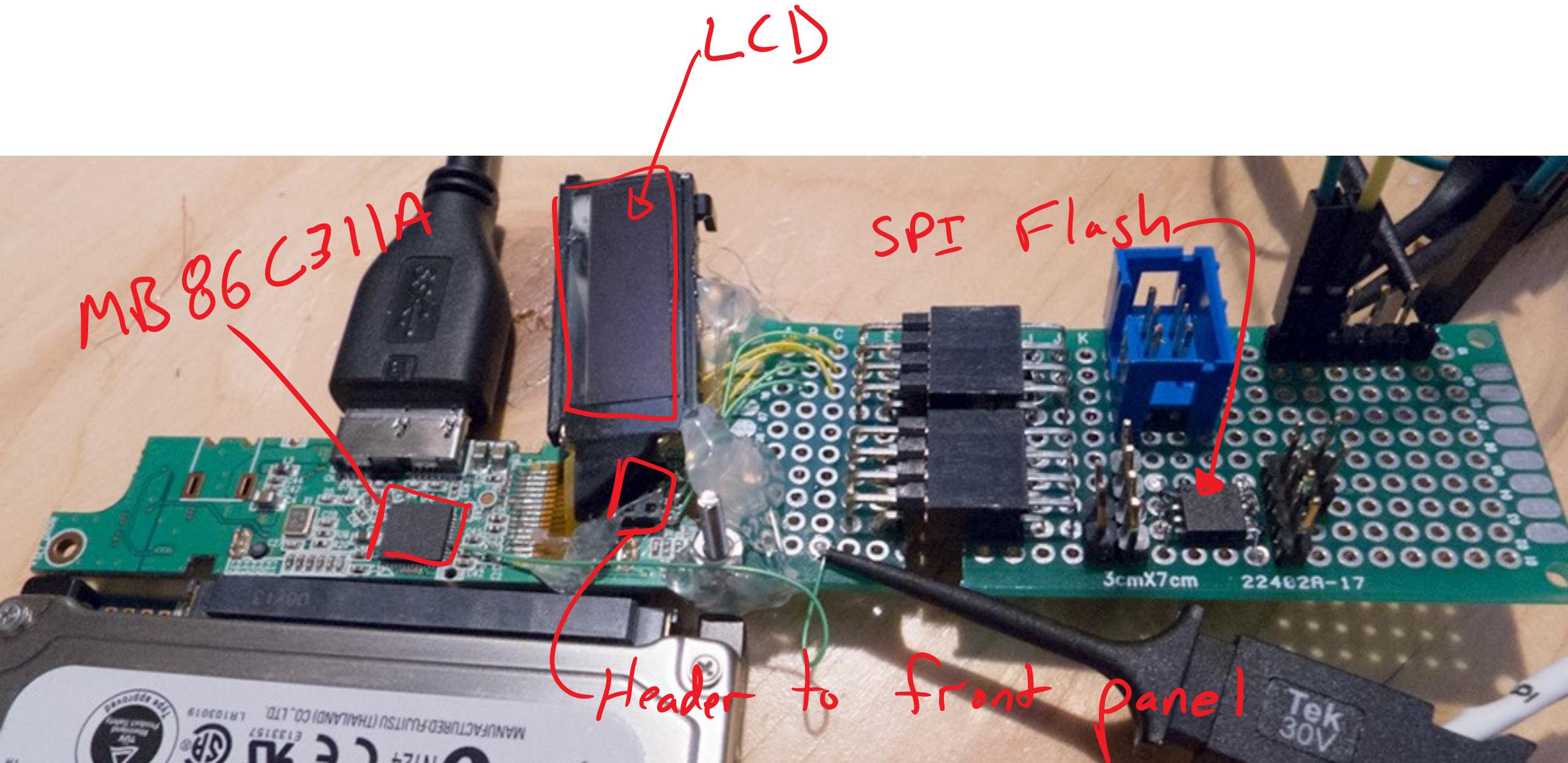
Lots of details in paper:

https://www.sstic.org/media/SSTIC2015/SSTIC-actes/hardware_re_for_software_reversers/SSTIC2015-Article-hardware_re_for_software_reversers-czarny_rigo.pdf

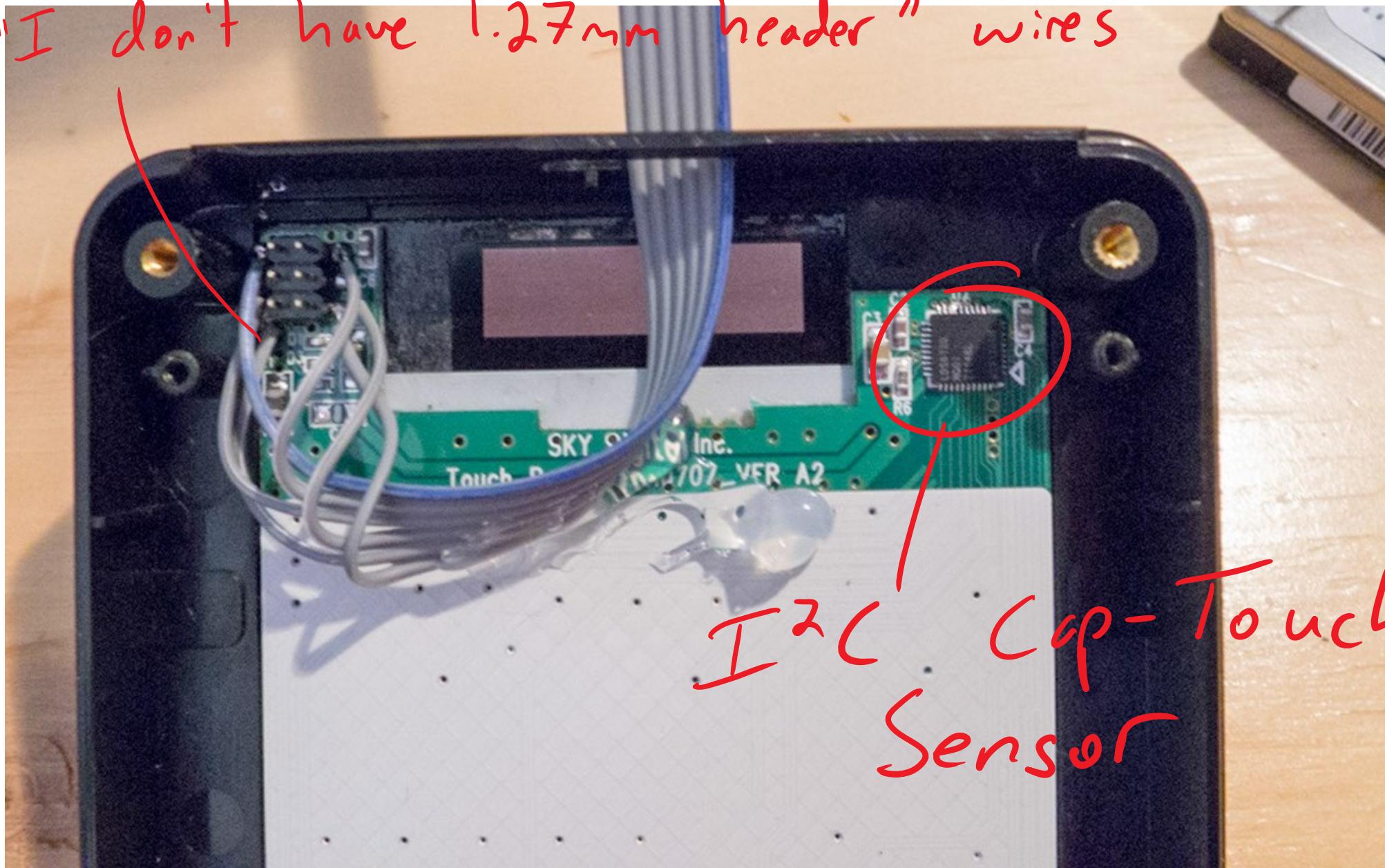
Me →
Czarny & Rigo's Paper →



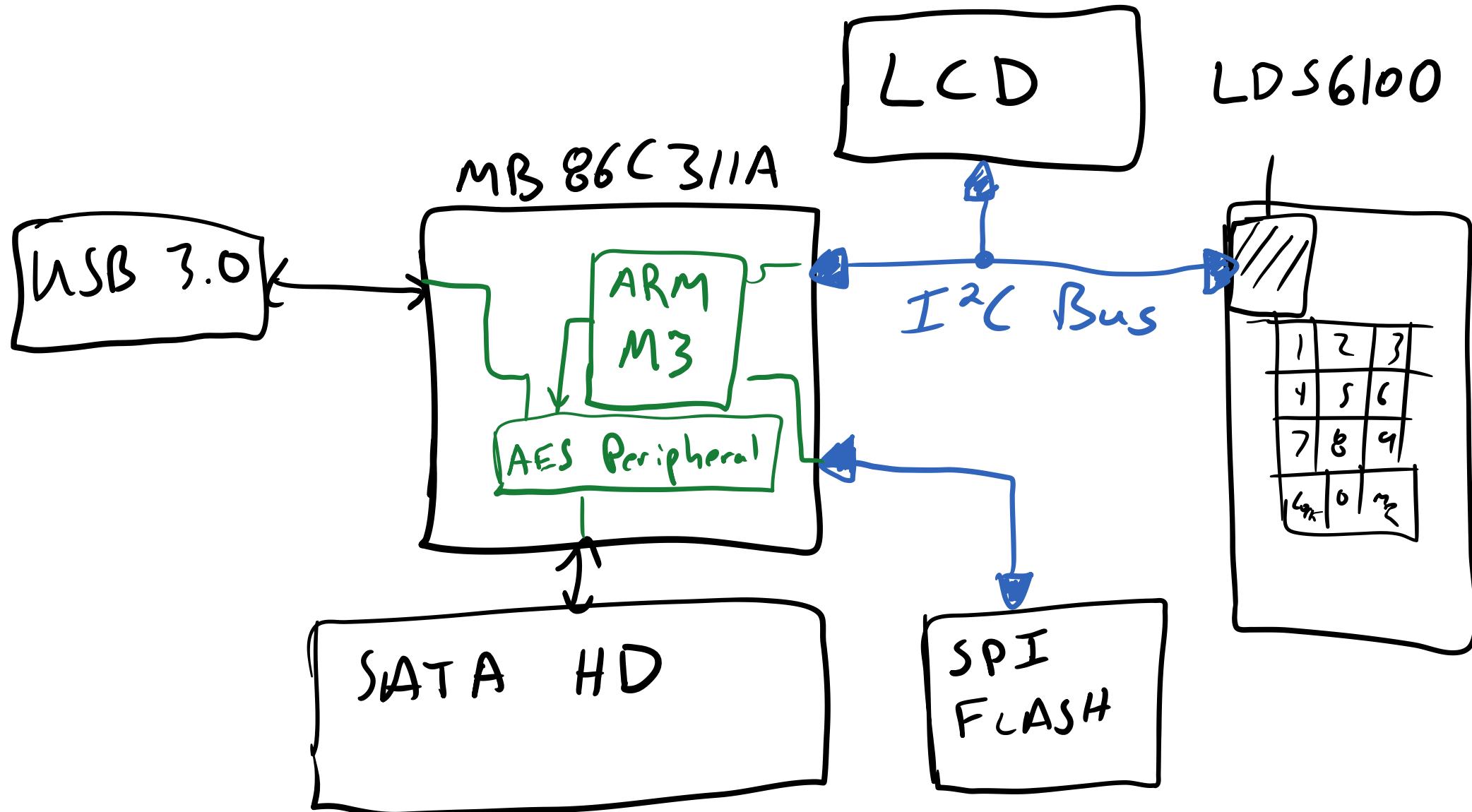
BRUTE
FORCING



"I don't have 1.27mm header" wires

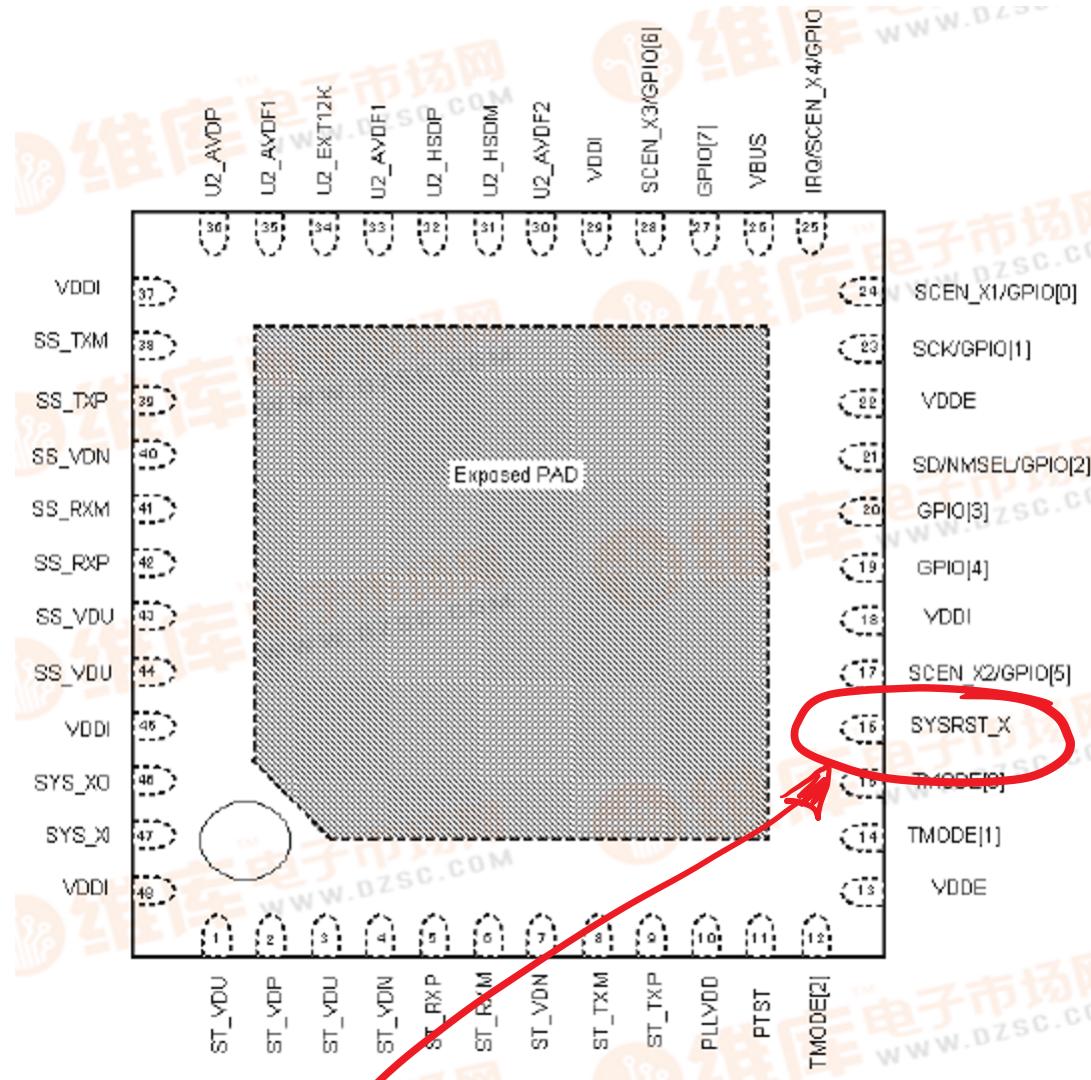


BLOCK DIAGRAM

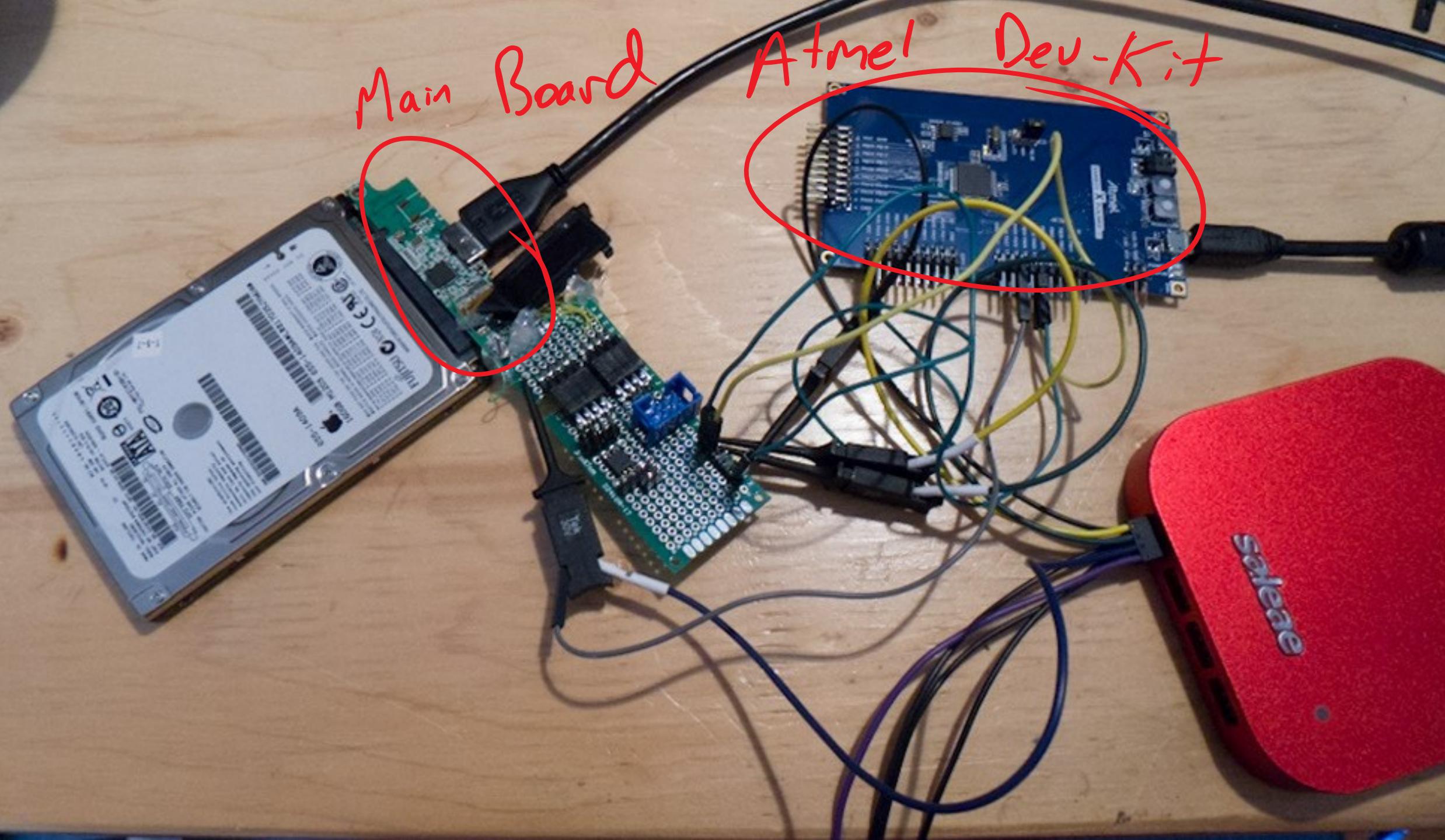


3. Turning on/off the power supply

item	Regulator	Pin
Turning on/ off the power supply	3.3V Power supply	Digital power supply for external IO
		VDDE
		SATA 3.3V analog power supply
Turning on/off the power supply	1.2V Power supply	USB2.0 3.3V analog power supply
		U2_AVDF1, U2_AVDB
		Analog power supply for PLL
		PLLVDD
		Digital power supply for internal core
		VDDI
		SATA 1.2V analog power supply
		ST_VD, ST_VDU
		USB3.0 1.2V analog power supply
		SS_VDN, SS_VDU
		U2_AVDF2, U2_AVDP

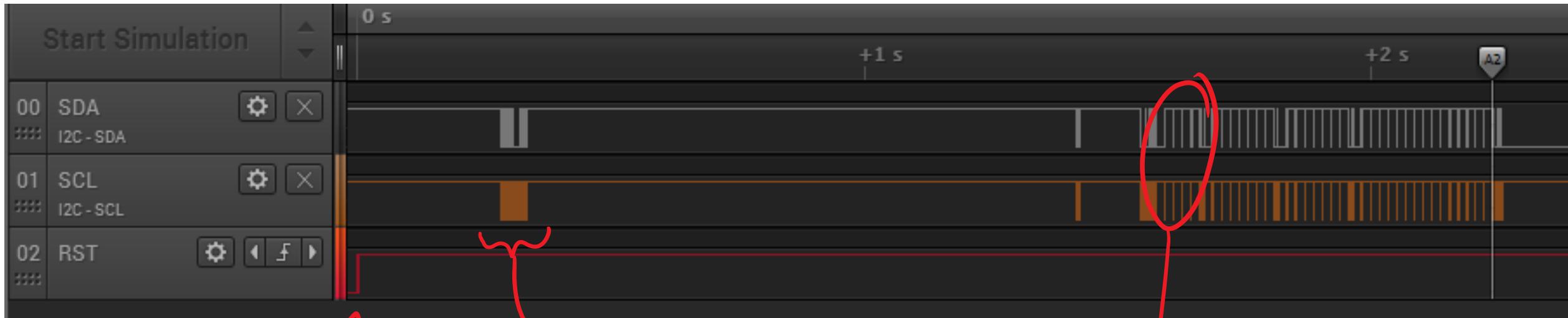


Can we bypass delay?



1. Wait for I²C poll
2. Feed in button presses.
3. Check response.

<https://github.com/colinoflynn/hddkeyboard-spoof-demo/>



Reset released

Initialization of LCD

Polling for buttons

Handwritten annotations in red explain the sequence: "Reset released" points to the RST signal, "Initialization of LCD" points to the I2C bus activity, and "Polling for buttons" points to the high-frequency digital signal on the A2 line.

FINDINGS

1. Time-out not stored in NVM.
↳ Can reset chip to bypass waits.
2. "Reasonable" entry speeds enforced
↳ $\sim 0.5\text{s}$ for 4 digits
3. Boot involves about 1.5s delay.

RESULTS

- 4 digit pin takes 2.23 s

PIN	LENGTH	GUESS TIME (WORST CASE)
4		6.2 hrs
5		2.6 days
6		26 days
7		260 days



You purchased this item on Dec 23 2015.

[View this order](#)



Satechi LockDown USB 3.0 Super-Speed 256-bit Encrypted Portable External 2.5" SATA Hard Drive Enclosure

by Satechi

13 customer reviews

Currently unavailable.

We don't know when or if this item will be back in stock.

- Quality OLED screen enables easy password input, menu navigation, HDD info and more
- Incorporates capacitance touch panel numeric keypad - Unlock the drive with your own unique 4 to 8 digit password
- USB 3.0 Super-Speed (5Gbps) driver also supports USB 2.0, ARM based 32bit Controller
- Measures (W) 3.1 x (H) 5 x (D) 0.5 inches / 3.25 ounces (w/o HDD)



**EARN A \$5 CREDIT FOR
EACH FRIEND WHO JOINS** [» Refer a friend](#)



CHECKING

CHIPS

OK! How SECURE ARE THESE?

Previous work by Czarny & Rigo:

8 Conclusion

Starting with no information, we managed, in full black box, to have a good understanding of the way this encrypted drive enclosure works.

While we know the crypto design is a fail, because all the encryption related data is stored on the drive itself, with no enclosure dependent secret, we were unable to actually exploit it.

SWAP IC FOR VIRGIN

→ Device worked.

↳ No fuse bits
or other secret
specific to
Manufacture.



Compare Bins

Two versions
of program
for Zalman
drive.

(This is from
(Czarny & Rigo)

zalman\fw\UE400_firmware_1-37<FAT>.bin	
0000	0000: 32 FF 1F 81 8E F2 DE E2 34 76 A0 2B 77 CC 03 E3 2 .üä=ö 4vá+w!l..ö
0000	0010: 92 A9 6E 62 37 E5 8E 48 EA 5D 58 92 8D 5E A5 E6 f@nb?öAH Ü1Xùi^Nµ
0000	0020: 84 2E 01 00 42 00 00 00 AA C8 01 A7 67 D6 C1 18 ä...B... -ll..ogíl.
0000	0030: B0 4D 92 1B 28 0C 38 8F AB D1 0E 18 68 5C 21 D1 JMÉ.Ö.88 %D..h^!D
0000	0040: EC F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 g.Ímñö. .è 2.n!8
0000	0050: 2A C1 36 9E 5A 1C 6B BF 78 F2 EC BC 7B 5F A1 6C *16xZ.kj x=gÙk_il
0000	0060: 2C A4 5A B1 6F 1B 80 E2 53 7E A4 FC FA 67 00 18 nZ)o.çö S~ñ³.g..
0000	0070: 50 63 63 D0 83 D1 E3 9A F5 D6 16 88 C2 19 67 F1 PccðåðöÜ Sí.êT.g±
0000	0080: A8 77 7F A4 C1 26 3D A9 4C 6C 0B 76 1E 3E 18 BA öwðñ=ö=u=@ L1.v.>.
0000	0090: 67 F2 42 55 FC C0 91 A8 10 83 E1 7B DF E6 26 E0 g=BU^Læc .âB ^c µ&ö
0000	00A0: 33 44 4B 90 50 A3 55 32 7C 39 12 0A 89 19 DF E0 3DKÉPúU2 19..ë..ö
0000	00B0: P2 00 30 07 CB AC EC EA B1 E9 DA 9C C6 02 0E 55 =.0.ñzgö ÚrEä..U
0000	00C0: 14 CC 19 19 6D 31 85 41 A7 3F 92 15 9F F2 CA 77 ,j..n1aA e?f=f=üv
0000	00D0: 90 D0 BF 77 63 E8 0A 85 88 14 2E 49 3E 22 F5 05 ÉdJwcP.à ê..I>"S.
0000	00E0: 96 B0 C1 3A 93 23 4C 51 7C 7A BB CD G3 19 10 7F üL:ö#LQ izñ= ..ö
0000	00F0: B2 8F 34 59 B7 0E B4 F2 75 43 10 D5 5B 22 7D 86 g4Yå..l= uC.í["]g
0000	0100: 0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 .öD.C7ñD .r^öýls7
0000	0110: 83 90 A9 EF 89 A1 2B 12 BB 52 38 C2 0B 66 8F DC âé@'ëí+. nR8T.f8
0000	0120: C5 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 <GieùO± :.c.äP.ö
0000	0130: D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF f.uó.ä2á .=FZ.Dé
0000	0140: E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 öðæäëä³øç .i^Vty'
0000	0150: 96 2D D2 5C 5C F4 4C E8 24 83 93 CB 12 B1 18 04 ü-E\\MLP \$âðñ.
0000	0160: 94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 öç.DI HT6 v@JĐ]LÝö
0000	0170: FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F öùë!fëä ÜiL'äðùë
0000	0180: DE F1 0E CB 2F C9 55 28 D7 23 7E 1F 98 10 00 4D i±.ñðñU ^c i#~.ü..M
0000	0190: 53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 Sìx.P2ln éäß.+ä"ñ
0000	01A0: 8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B è#yùqif.. .E.wYüe
0000	01B0: 21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 73 99 8E 70 !T.I!hm. Kúwiöäp

zalman\fw\UE400_firmware_1-37<NTFS>.bin	
0000	0000: 01 ED 10 47 A0 70 D3 BE A4 B0 6B DE 49 0E 09 67 .ü.GápÉ¥ nñkíI..g
0000	0010: E1 87 DB B4 37 87 4B 5A 4B 6D 28 F0 9E 88 21 CD 0çH?çKZ Km(-xé!=
0000	0020: 94 2E 01 00 02 00 00 00 AA C8 01 A7 67 D6 C1 18 ö...B... -ll..ogíl.
0000	0030: CC 4D 92 1B 54 0C 38 8F D7 D1 0E 18 14 5C 21 D1 JMÉ.Ö.88 iD..n!8
0000	0040: 90 F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 g.Ímñö. .è 2.n!8
0000	0050: 2A C1 36 9E 26 1C 6B BF 04 F2 EC BC 7B 5F A1 6C *16xZ.kj x=gÙk_il
0000	0060: 50 A4 5A B1 13 1B 80 E2 4F 7E A4 FC F6 67 00 18 PñZ)o.çö Ö~ñ³.g..
0000	0070: 4C 63 D3 D0 83 D1 E3 9A F9 D6 16 88 36 1A 67 F1 LccðåðöÜ "i.ä6.g±
0000	0080: BC 77 7F A4 3D 25 3D A9 B0 6P 0B 76 EA 3D 18 BA üwðñ=ö=u=@ o.vü=.
0000	0090: 6B F2 42 55 E8 C0 91 A8 6C 83 E1 7B A3 E6 26 E0 k=BU^Læc lâB ^c µ&ö
0000	00A0: 27 44 4B 90 2C A3 55 32 00 39 12 0A F5 19 DF E0 'DKÉ.äU2 9..S..ö
0000	00B0: 8E 00 30 07 A7 AC EC EA A5 E9 DA 9C BA 02 0E 55 à.0.ñzgö ÙúrE ..U
0000	00C0: 00 CC 19 19 71 31 85 41 B3 3F 92 15 9F F2 CA 77 ,j..n1aA e?f=f=üv
0000	00D0: EC D0 BF 77 6F E8 0A 85 88 14 2E 49 3E 22 F5 05 <GieùO± :.c.äP.ö
0000	00E0: 96 B0 C1 3A 93 23 4C 51 7C 7A BB CD G3 19 10 7F üL:ö#LQ izñ= ..ö
0000	00F0: B2 8F 34 59 B7 0E B4 F2 75 43 10 D5 5B 22 7D 86 g4Yå..l= uC.í["]g
0000	0100: 0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 .öD.C7ñD .r^öýls7
0000	0110: 83 90 A9 EF 89 A1 2B 12 BB 52 38 C2 67 66 8F DC âé@'ëí+. nR8T.yf8
0000	0120: 29 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 >GieùO± :.c.äP.ö
0000	0130: D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF f.uó.ä2á .=FZ.Dé
0000	0140: E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 öðæäëä³øç .i^Vty'
0000	0150: 96 2D D2 5C 5C F4 4C E8 24 83 93 CB 12 B1 18 04 ü-E\\MLP \$âðñ.
0000	0160: 94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 öç.DI HT6 v@JĐ]LÝö
0000	0170: FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F öùë!fëä ÜiL'äðùë
0000	0180: DE F1 0E CB 2F C9 55 28 D7 23 7E 1F 98 10 00 4D i±.ñðñU ^c i#~.ü..M
0000	0190: 53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 Sìx.P2ln éäß.+ä"ñ
0000	01A0: 8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B è#yùqif.. .E.wYüe
0000	01B0: 21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 73 99 8E 70 !T.I!hm. Kúwiöäp

STREAM CIPHER

Keystream : E7 1A F1 37

⊕ ⊕ ⊕ ⊕

Plain text : 2C 1F 09 1A ...

Cipher text : CB 05 F8 2D

Compare Bins

F:b Length

Flag?

Code

zalman\fw\UE400_firmware_1-37<FAT>.bin	
0000 0000:	32 FF 1F 81 8E F2 DE E2 34 76 A0 2B 77 CC 03 E3 2 .üä=ö 4vá+wl.ö
0000 0010:	92 02 6E 02 27 FF 0E 10 EA 5D 58 92 8D 5E A5 E6 ü@nb?öAH ÜIKÜì^NM
0000 0020:	84 2E 01 00 42 00 00 00 AA C8 01 A7 67 D6 C1 18 ä..B.. -L..ogí.
0000 0030:	0E 4D 92 1B 26 0C 38 0F AB D1 0E 18 68 5C 21 D1 äME. <.88 %D..h^!D
0000 0040:	EC F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 E6 21 38 äo.Ímñ0. .è 2.n!8
0000 0050:	2A C1 36 9F 5A 1C 6B BF 78 F2 EC BC 7B 5F A1 6C *-6xZ.kj x=gÜ_k_il
0000 0060:	2C A4 5A B1 6F 1B 80 E2 53 7E A4 FC FA 67 00 18 ñZ o.çö S~ñ^g..
0000 0070:	50 63 63 D0 83 D1 E3 9A F5 D6 16 88 C2 19 67 F1 PccðåðöÜ Sí.êT.g+
0000 0080:	A8 27 7F A4 21 26 3D A9 40 6C 0B 76 1E 3E 18 BA öwðñ^u=@ L1.v.>
0000 0090:	67 F2 42 55 FC C0 91 A8 10 83 E1 2B DF E6 26 E0 g=BU^Læc .âB ^c µ&ö
0000 00A0:	33 44 4B 90 50 A3 55 32 7C 39 12 0A 89 19 DF E0 3DKéPáU2 19..ë..ö
0000 00B0:	F2 00 30 07 CB AC EC EA B1 E9 DA 9C C6 02 0E 55 =.0.ñzgû ÚrEä..U
0000 00C0:	14 CC 19 19 6D 31 85 41 A7 3E 92 15 9F P2 CA 71 j .m1aA o?f.f=ü
0000 00D0:	90 D0 BF 77 63 E8 00 85 88 14 2E 49 3E 22 F5 06 ÉdJwcP.à ê..I>"S.
0000 00E0:	96 B0 C1 3A 93 23 4C 51 7C 2A BB CD C7 19 10 7F üL:ô#LQ izñ= ..ö
0000 00F0:	B2 9F 34 59 B7 0F B4 F2 75 43 10 D5 5B 22 7D 86 ä4Yå.. = uC.í["]>
0000 0100:	0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 .ôD.C7ñD .r^býls7
0000 0110:	93 90 A9 EF 89 A1 2B 12 BB 52 38 02 0B 66 8F DC äé@.éí+. nR8T.f8
0000 0120:	C5 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 >KGieùO± :.c.äP.ö
0000 0130:	D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF f.uó.â2á .=FZ.Dé
0000 0140:	E4 D0 84 85 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 öðæäëä^æc .í+Ýty'
0000 0150:	96 2D D2 5C 5C F4 4C E8 24 82 93 CB 12 B1 18 04 ü-E\\MLp \$âðñ.
0000 0160:	94 BD 16 44 49 C3 54 36 76 16 4A D1 5D 4C BE E0 öç.DI HT6 v@JÐ]LÝö
0000 0170:	FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F üé!Eä!f8 ÜiL'âðùë
0000 0180:	DE F1 0E CB 2F C9 55 28 D7 23 7E 1F 98 10 00 4D i±.ñðñU<ü> î#~.y..M
0000 0190:	53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 Sïx.P2ln éäß.+ä"ñ
0000 01A0:	8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B è#yùqif.. E.wYüø
0000 01B0:	21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 73 99 8E 70 !T.I!hm. Kúwiöäp

zalman\fw\UE400_firmware_1-37<NTFS>.bin	
0000 0000:	01 ED 10 47 A0 70 D3 BE A4 B0 6B DE 49 0E 09 67 .ü.GápÉ¥ ñkíI..g
0000 0010:	E1 87 DB B4 37 87 4B 5A 4B 6D 28 F0 9E 88 21 CD üçH?çKZ Km<-xé!=
0000 0020:	94 2E 01 00 02 00 00 00 AA C8 01 A7 67 D6 C1 18 ö.. -L..ogí.
0000 0030:	CC 4D 92 1B 54 0C 38 8F D7 D1 0E 18 14 5C 21 D1 äME. <.88 îD..n!8
0000 0040:	90 F8 0B D7 6D CB 4F 13 05 8A C3 32 F7 6E 21 38 äo.Ímñ0. .è 2.n!8
0000 0050:	2A C1 36 9E 26 1C 6B BF 04 F2 EC BC 7B 5F A1 6C *-6xZ.kj x=gÜ_k_il
0000 0060:	50 A4 5A B1 13 1B 80 E2 4F 7E A4 FC F6 67 00 18 PñZ o.çö Ö~ñ^g..
0000 0070:	4C 63 63 D0 83 D1 E3 9A F9 D6 16 88 36 1A 67 F1 LccðåðöÜ "í.â6.g+
0000 0080:	BC 77 7F A4 3D 25 3D A9 B0 6F 0B 76 EA 3D 18 BA üwðñ=u=@ äo.vü=.
0000 0090:	6B F2 42 55 E8 C0 91 A8 6C 83 E1 7B A3 E6 26 E0 k=BU^Læc lâB ^c ú&ö
0000 00A0:	27 44 4B 90 2C A3 55 32 00 39 12 0A F5 19 DF E0 ,DKé,áU2 9..S..ö
0000 00B0:	8E 00 30 07 A7 AC EC EA A5 E9 DA 9C BA 02 0E 55 ä.0.ñzgû ÑúrE .U
0000 00C0:	00 CC 19 19 71 31 85 41 B3 3F 92 15 9F F2 CA 77 j .m1aA ?f.f=ü
0000 00D0:	EC D0 BF 77 6F E8 0A 85 88 14 2E 49 3E 22 F5 05 ÉdJwcP.à ê..I>"S.
0000 00E0:	96 B0 C1 3A 93 23 4C 51 7C 2A BB CD C3 19 10 7F üL:ô#LQ izñ= ..ö
0000 00F0:	B2 8F 34 59 B7 0F B4 F2 75 43 10 D5 5B 22 7D 86 ä4Yå.. = uC.í["]>
0000 0100:	0E 93 D1 03 43 37 BB D1 1C C9 DF 95 EC 7C 73 37 .ôD.C7ñD .r^býls7
0000 0110:	83 90 A9 EF 89 A1 2B 12 BB 52 38 C2 67 66 8F DC äé@.éí+. nR8T.yf8
0000 0120:	29 3C 47 D6 9B 97 4F F1 3A 01 87 DC C6 50 18 95 >KGieùO± :.c.äP.ö
0000 0130:	D7 0E 75 E0 17 83 32 A0 19 3D 46 5A DC 44 88 DF f.uó.â2á .=FZ.Dé
0000 0140:	E4 D0 84 89 86 FC 9B BD FA D7 F1 BE C5 79 EF C4 öðæäëä^æc .í+Ýty'
0000 0150:	96 2D D2 5C 5C F4 4C E8 24 82 93 CB 12 B1 18 04 üç.DI HT6 v@JÐ]LÝö
0000 0160:	94 BD 16 44 49 C3 54 36 76 A6 4A D1 5D 4C BE E0 üé!Eä!f8 ÜiL'âðùë
0000 0170:	FF 60 7D 96 D3 DD 9C C7 9A 69 C0 60 C7 7F EB 8F i±.ñðñU<ü> î#~.y..M
0000 0180:	DE F1 0E CB 2F C9 55 28 D7 23 7E 1F 98 10 00 4D Sïx.P2ln éäß.+ä"ñ
0000 0190:	53 8D CF 14 50 32 6C 6E 82 C6 E1 06 2B C6 22 B4 è#yùqif.. E.wYüø
0000 01A0:	8A 23 ED EB F4 46 0F 15 02 EF 45 0A 77 59 A3 9B !T.I!hm. Kúwiöäp
0000 01B0:	21 54 1F 5B DD 68 6D 07 F3 A3 77 AD 73 99 8E 70 !T.I!hm. Kúwiöäp

No difference in encrypted data

⇒ No diff in source at that byte.

Zalman →

buffalo\na_website\hd-lbu3-wr_rev120\firmware_C311.bin

0000 0000:	BA C8 58 DF F7 C9 2C 65	CA CB 54 24 18 01 90 F7	EX■ Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0010:	1B 3D 94 18 D8 C4 P2 BD	B5 92 0A 3C 6C 28 35 E4	.=6.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0020:	54 FD 00 00 42 00 00 00	3A EE 01 A7 67 D6 C1 18	T.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0030:	78 BC 93 1B E0 FD 39 8F	63 20 0F 18 A0 AD 20 D1	x.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0040:	24 09 0A D7 6D CB 4F 13	05 8A C3 32 F7 6E 21 38	\$.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0050:	2A C1 36 9E 92 ED 6A BF	B0 03 ED BC 7B 5F A1 6C	*.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0060:	E4 55 5B B1 A7 EA 81	E2 87 68 A4 FC 7A 63 00 18	ȐU[.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0070:	84 67 63 D0 83 D1 E3 9A	0B DA 16 88 DA 18 67 F1	ȐägȐ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0080:	88 26 7F A4 D9 72 3D A9	54 6D 0B 76 06 3F 18 BA	Ȑeu.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0090:	43 F3 42 55 80 C1 91 A8	D8 72 E0 7B 17 17 27 E0	C.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00A0:	17 48 4B 90 98 52 54	32 B4 C8 13 0A 41 E8 DE	.HKE.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00B0:	3A F1 31 07 B9 8B EC EA	F9 F6 DA 9C 0E P3 0F 55	:±1.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00C0:	3E C7 19 19 65 28 BB 85	41 A5 38 92 15 9F F2 CA 77	>.-.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00D0:	58 21 BE 77 E5 ED 0A 85	88 14 2E 49 3E 22 F5 05	X?W.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00E0:	96 B0 C1 3A 93 23 4C 51	7C 7A BB CD C3 19 3F 2F	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 00F0:	B2 8F 34 59 B7 0E B4 F2	75 43 10 D5 5B 22 7D 86	ȐB4Y.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0100:	0E 93 D1 03 7A 37 BB D1	1C C9 DF 95 EC 7C 73 37	.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0110:	83 90 A9 EF 89 A1 2B 12	BB 52 38 C2 B7 B6 8E DC	ȐäE@.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0120:	09 EC 46 D6 9B 97 4F F1	3A 01 87 DC C6 50 18 95	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0130:	D7 0E 75 E0 17 83 32 A0	19 3D 46 5A DC 44 88 DF	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0140:	E4 D0 84 89 86 FC 9B BD	FA D7 F1 BE C5 79 EF C4	Ȑðäë.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0150:	96 2D D2 5C 5C F4 4C E8	24 83 93 CB 12 B1 18 04	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0160:	94 BD 16 44 49 C3 54 36	76 A6 4A D1 5D 4C BE E0	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0170:	FF 60 7D 96 D3 DD 9C C7	9A 69 C0 60 C7 7F EB 8F	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0180:	CE E8 2A 50 07 24 2D CF	3D C1 04 A7 C4 6E CB 5D	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 0190:	31 4B A3 14 64 9B 28 B1	P9 E1 91 41 34 50 2D 60	1Ku.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 01A0:	8B FA F2 70 F4 C9 32 17	A5 D6 B2 02 DA 09 2D DB	i.-.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.
0000 01B0:	1F 65 B0 18 D9 F8 P4 BB	87 D3 67 5D 51 AA 09 AE	Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.Ȑ.

Buffalo →
(Other manufacture)

zalman\fw\UE400_firmware_1-37(FAT).bin		
0000 0000:	32 FF 1F 81 8E F2 DE E2	34 76 A0 2B 77 CC 03 E3
0000 0010:	92 A9 6E 62 37 E5 8E 48	EA CD 58 92 0D 5F 05 EC
0000 0020:	84 2F 01 00 42 00 00 00	AA C9 81 A7 67 D6 C1 18
0000 0030:	B0 4D 22 1B 28 DC 38 8F	AB D1 DF 1A 48 50 21 D1
0000 0040:	EC B6 3B D7 6D CB 4F 13	05 8A C3 32 F7 6E 21 38
0000 0050:	2A C1 36 9E 5A 1C 6B BF	70 F2 EC B3 7B 5F 01 6C
0000 0060:	2C 01 5A B1 6F 1B 80 E2	53 7E A4 FC FA 67 00 18
0000 0070:	50 63 63 D0 83 D1 E3 9A	F5 D6 16 88 C2 19 67 F1
0000 0080:	A8 77 7F A4 C1 76 3D A9	4C 6C 0B 76 1E 3E 18 BA
0000 0090:	67 P2 42 55 PC C0 91 A8	10 83 E1 7B DF E6 26 E0
0000 00A0:	33 44 4B 90 50 A3 55 32	7C 39 12 0A 89 19 DF E0
0000 00B0:	F2 00 30 07 CB AC EC EA	B1 E9 DA 9C C6 02 0E 55
0000 00C0:	14 CC 19 19 6D 31 85 41	A7 3F 92 15 9F F2 CA 27
0000 00D0:	90 D0 BF 77 63 E8 0A 85	88 14 2E 49 3E 22 F5 05
0000 00E0:	96 B0 C1 3A 93 23 4C 51	7C 7A BB CD C3 19 7F
0000 00F0:	B2 8F 34 59 B7 0E B4 F2	75 43 10 D5 5B 22 7D 86
0000 0100:	0E 93 D1 03 43 37 BB D1	1C C9 DF 95 EC 7C 73 37
0000 0110:	83 90 A9 EF 89 A1 2B 12	DB 52 38 C2 0B 66 8F DC
0000 0120:	C5 3C 47 D6 9B 97 4F P1	3A 01 87 DC C6 50 18 95
0000 0130:	D7 0E 25 E0 17 83 32 A0	19 3D 46 5A DC 44 88 DF
0000 0140:	E4 D0 84 89 86 FC 9B BD	FA D7 F1 BE C5 79 EF C4
0000 0150:	96 2D D2 5C 5C F4 4C E8	24 83 93 CB 12 B1 18 04
0000 0160:	94 BD 16 44 49 C3 54 36	76 A6 4A D1 5D 4C BE E0
0000 0170:	FF 60 7D 96 D3 DD 9C C7	9A 69 C0 60 C7 7F EB 8F
0000 0180:	DE P1 0E CB 7F C9 55 28	D7 23 7E 1F 98 10 00 4D
0000 0190:	53 8D CF 14 50 32 6C 6E	82 C6 E1 06 2B C6 22 B4
0000 01A0:	8A 23 ED EB F4 46 0F 15	02 EF 45 0A 77 59 A3 9B
0000 01B0:	21 54 1F 5B DD 68 6D 07	F3 A3 77 AD 73 99 8E 70

Blocks 8, 9, 10, // same (Block=32 b.ts)

00 20 08 20	F9 46 08 00	F5 46 08 00	F5 46 08 00
F5 46 08 00	F5 46 08 00	F5 46 08 00	00 00 00 00
00 00 00 00	00 00 00 00	00 00 00 00	F5 46 08 00
F5 46 08 00	00 00 00 00	F5 46 08 00	F5 46 08 00
F5 46 08 00			
F5 46 08 00			
F5 46 08 00			
F5 46 08 00	F5 46 08 00	25 2C 08 00	39 2C 08 00
F5 46 08 00	61 13 08 00	81 13 08 00	A1 13 08 00
F5 46 08 00			
F5 46 08 00	F5 46 08 00	79 0F 08 00	F5 46 08 00
F5 46 08 00			
F5 46 08 00	81 36 08 00	F5 46 08 00	10 B5 05 4C
23 78 33 B9	04 4B 13 B1	04 48 AF F3	00 80 01 23
23 70 10 BD	54 0E 00 20	00 00 00 00	E8 B9 08 00
08 B5 06 4B	1B B1 06 48	06 49 AF F3	00 80 06 48
03 68 13 B1	05 4B 03 B1	98 47 08 BD	00 00 00 00
E8 B9 08 00	58 0E 00 20	E8 B9 08 00	00 00 00 00
10 B4 89 01	43 18 02 24	44 50 4F F0	FF 31 99 62
19 6A 5A 60	5D F8 04 4B	70 47 00 BF	89 01 05 23
43 50 70 47	89 01 02 23	43 50 70 47	00 EB 81 11
CA 61 70 47	00 EB 81 11	4A 62 70 47	00 EB 81 11
08 6A 70 47	70 B5 86 B0	05 46 0E 46	04 23 00 93
DC 48 0E 21	0F 22 02 AB	0B 4C A0 47	02 46 60 B9
04 2B 28 BF	04 26 4E B1	B1 00 00 23	02 AC 1C 59
EC 50 04 33	8B 42 F9 D1	00 E0 10 22	10 46 06 B0
70 BD 00 BF	00 08 0E 40	01 00 00 20	00 23 43 60
03 60 83 60	70 47 00 BF	10 B4 04 68	01 34 80 2C
28 BF 00 24	04 E0 1A B9	83 68 01 33	83 60 06 E0

Figure 2.2. Vector table

Exception number	IRQ number	Offset	Vector
16+n	n	0x0040+4n	IRQn
.	.	.	.
18	2	0x004C	IRQ2
17	1	0x0048	IRQ1
16	0	0x0044	IRQ0
15	-1	0x0040	Systick
14	-2	0x003C	PendSV
13		0x0038	Reserved
12			Reserved for Debug
11	-5	0x002C	SVCall
10			Reserved
9			
8			
7			
6	-10	0x0018	Usage fault
5	-11	0x0014	Bus fault
4	-12	0x0010	Memory management fault
3	-13	0x000C	Hard fault
2	-14	0x0008	NMI
1		0x0004	Reset
		0x0000	Initial SP value

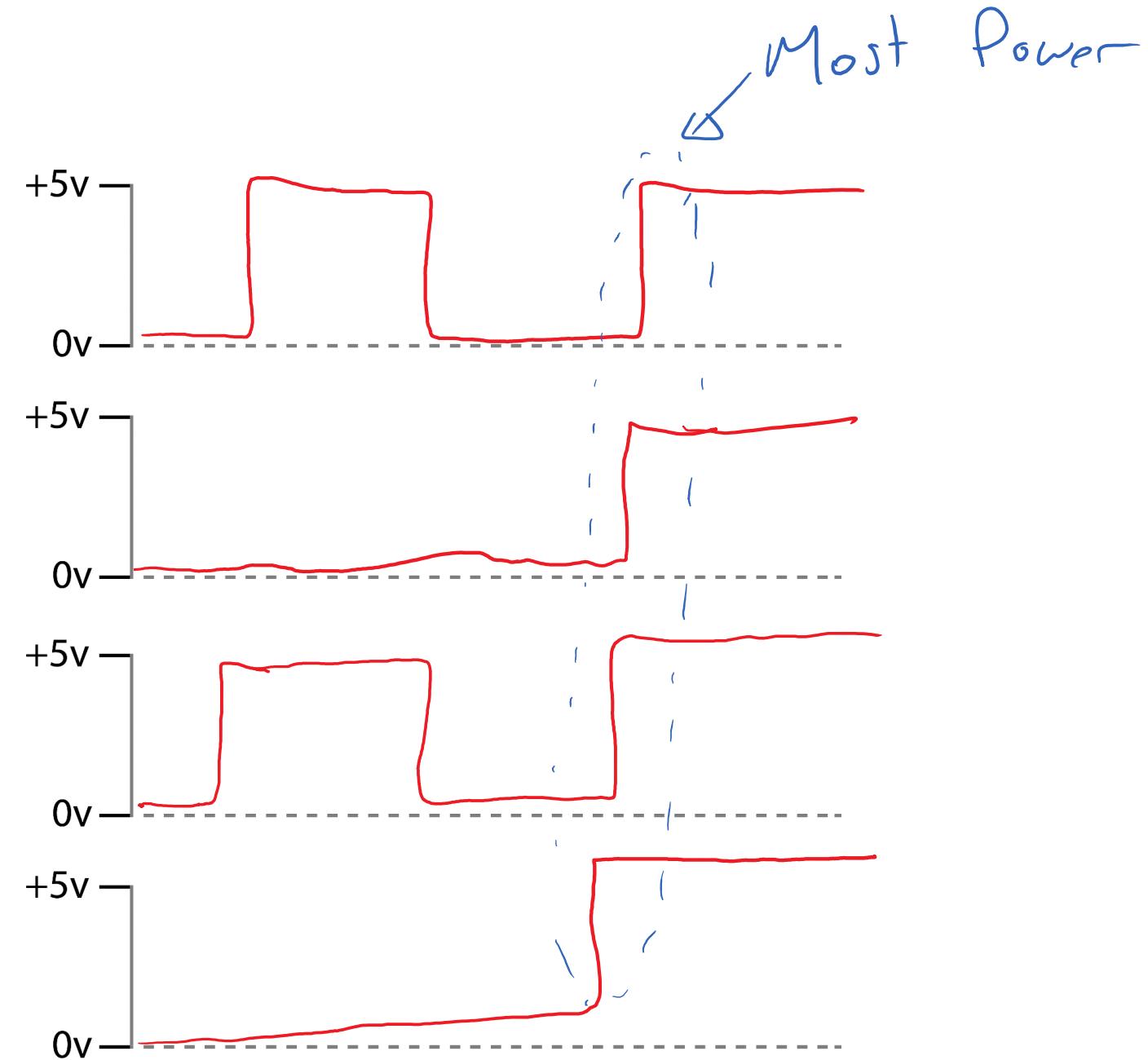
On system reset, the vector table is fixed at address [0x00000000](#). |

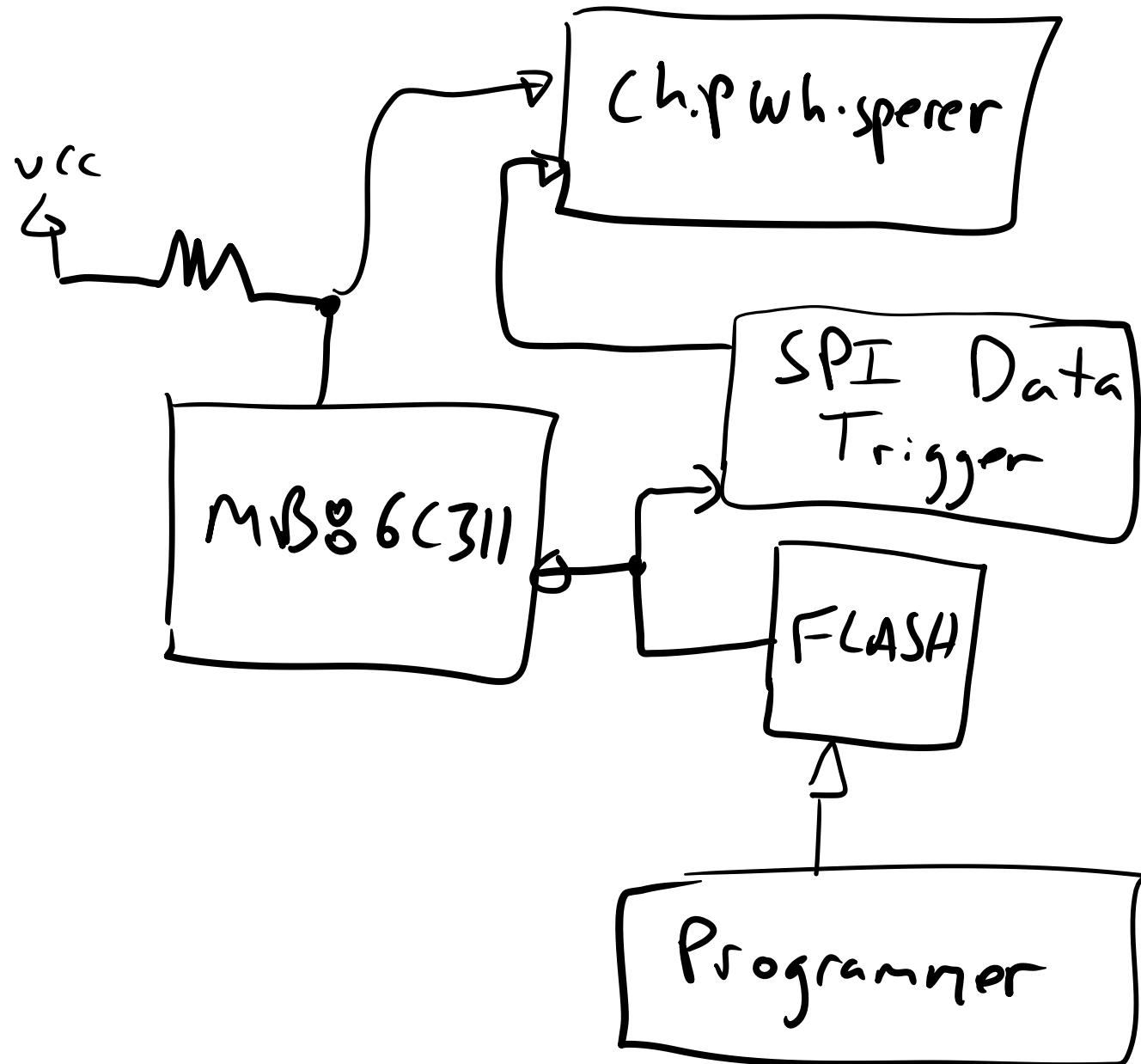
Knowledge?

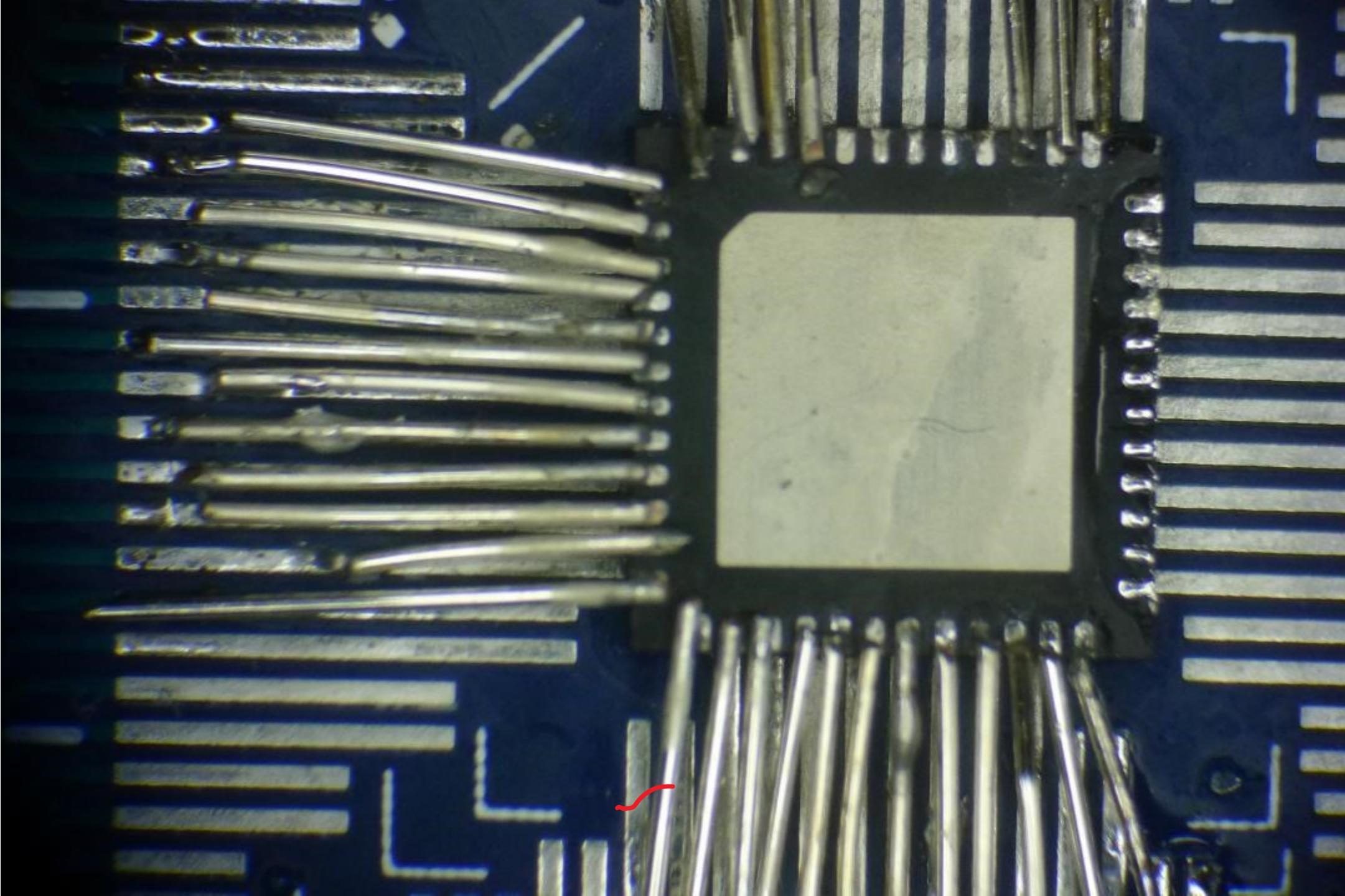
- Direct ARM Cortex M3 code, with stream cipher.
- Break stream cipher, all is lost.

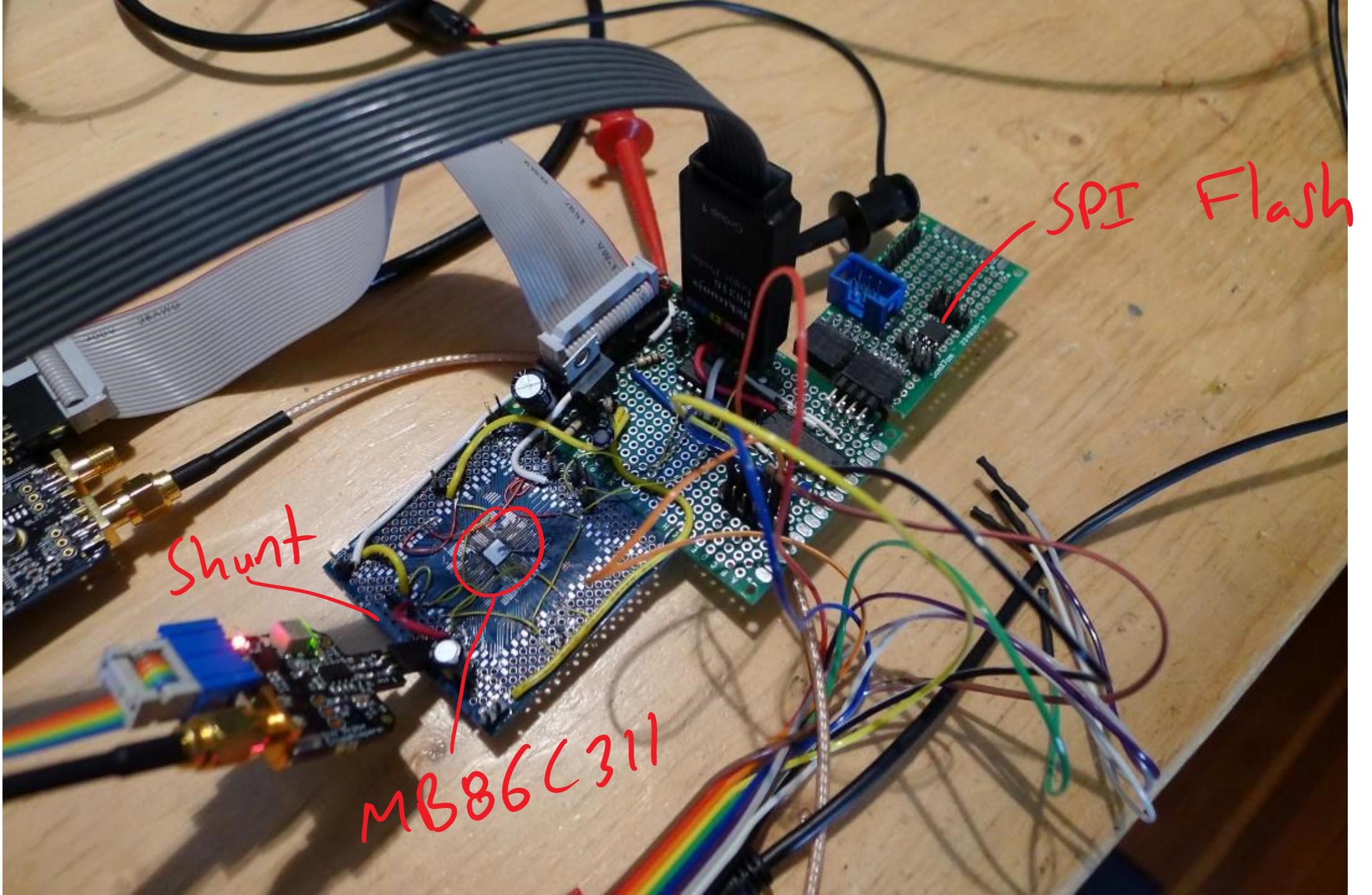
POWER
ANALYSIS?

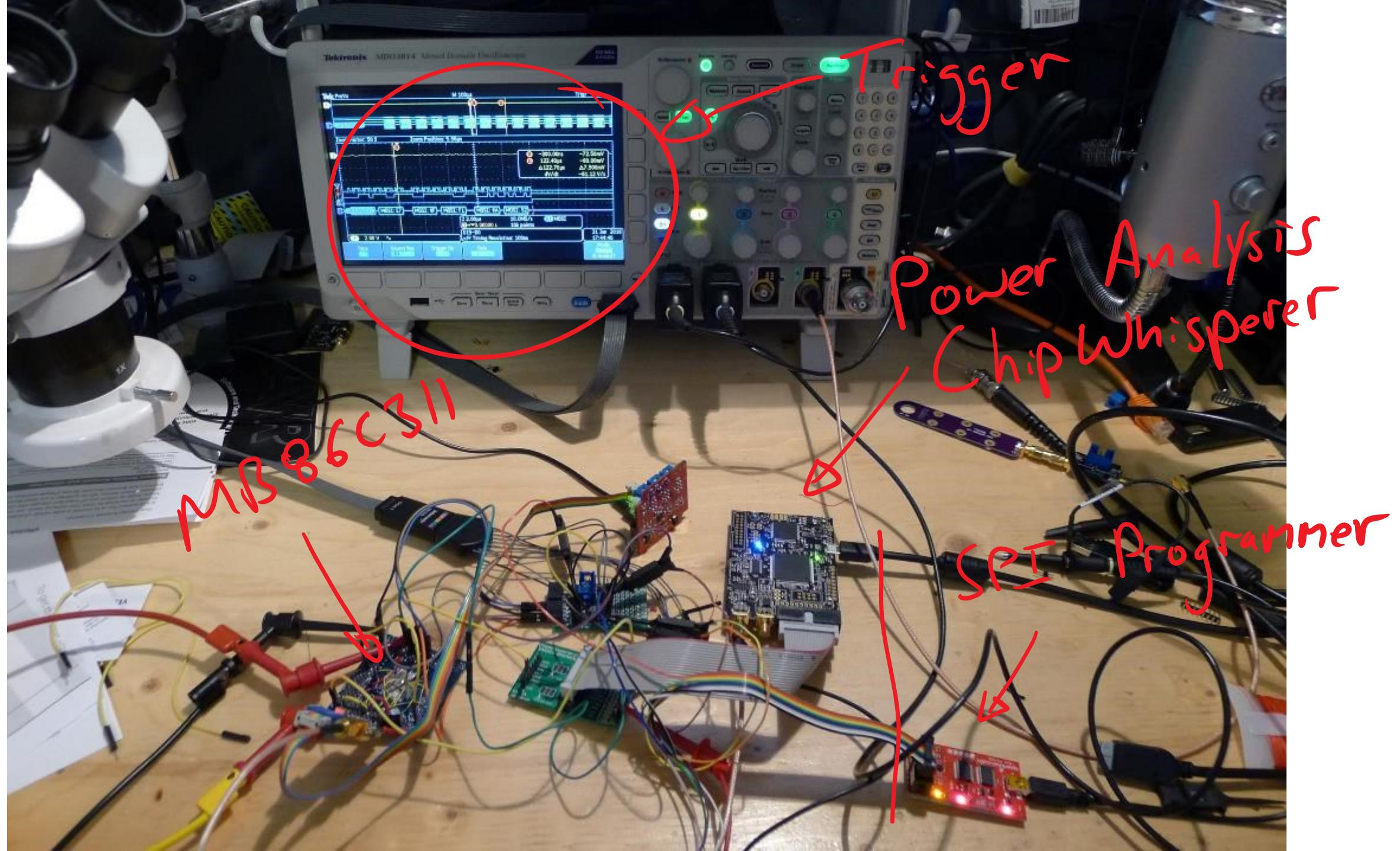
Data Busses...











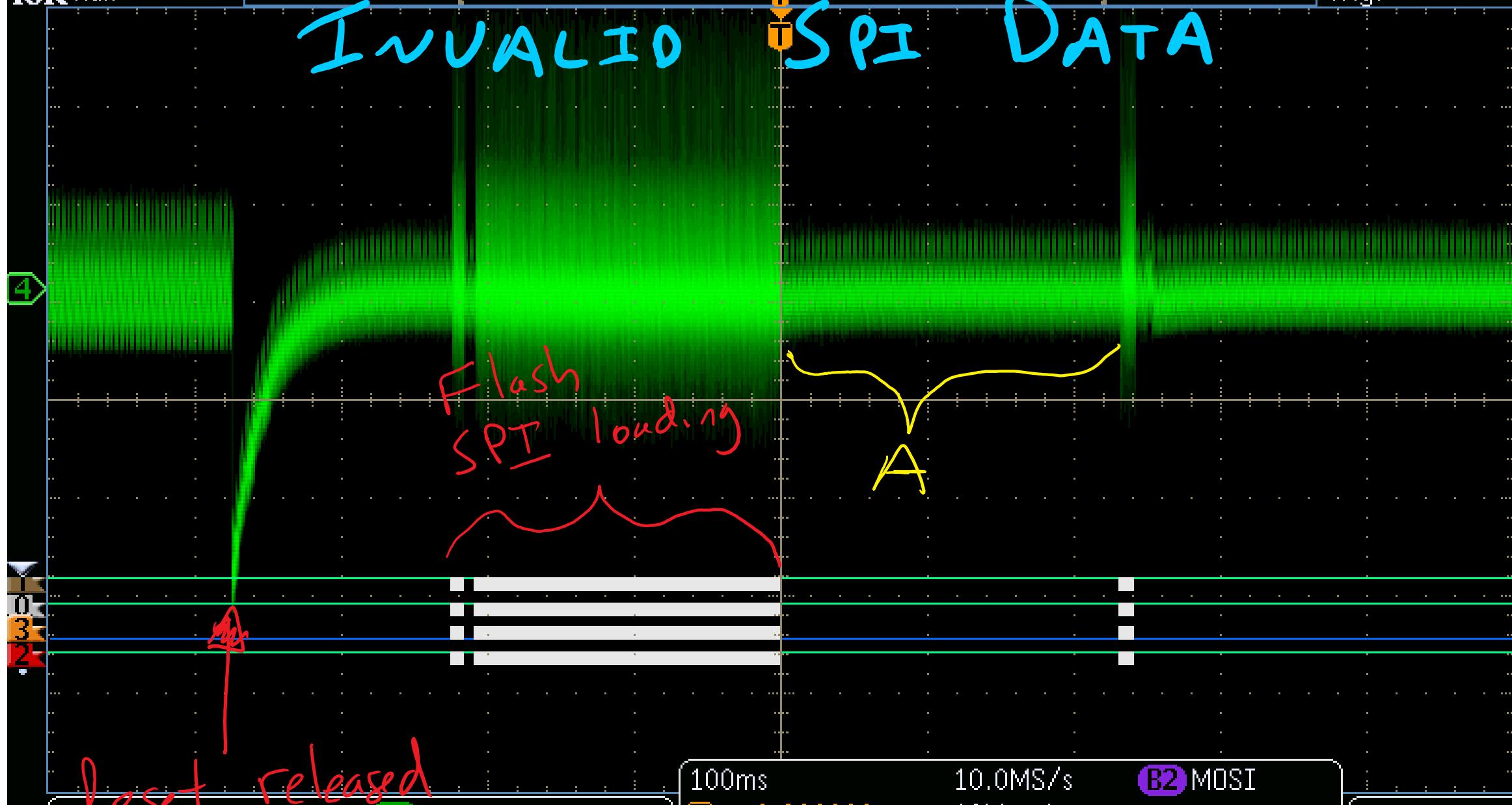
POWER ANALYSIS

1. Program SPI Flash with pattern.
2. Reset MB86711, will reload FLASH.
3. Capture power at different places.

Tek Run

Trig?

INVALID SPI DATA



Reset released

4

200mV

V

100ms
0.000000 s

D15-D0

* Timing Resolution: 100ns

10.0MS/s
10M points

B2 MOSI

21 May 2016
14:40:37

Tek Run

Trig?

VALIDO SPI DATA

4

Y

C

K

L

R

Flash
SPT loading

Reset released

4

200mV

100ms

0.000000 s

10.0MS/s

10M points

B2 MOSI

D15-D0

Timing Resolution: 100ns

21 May 2016

14:44:09

B

C

COMPARISON

Invalid = Changed a few bytes
Valid = Original Image

- ① Both complete operation "A"
- ② Only valid code completes "B"
- ③ Assume "C" is switching to operating code, maybe powering on SATA c-lc?

LEARNINGS

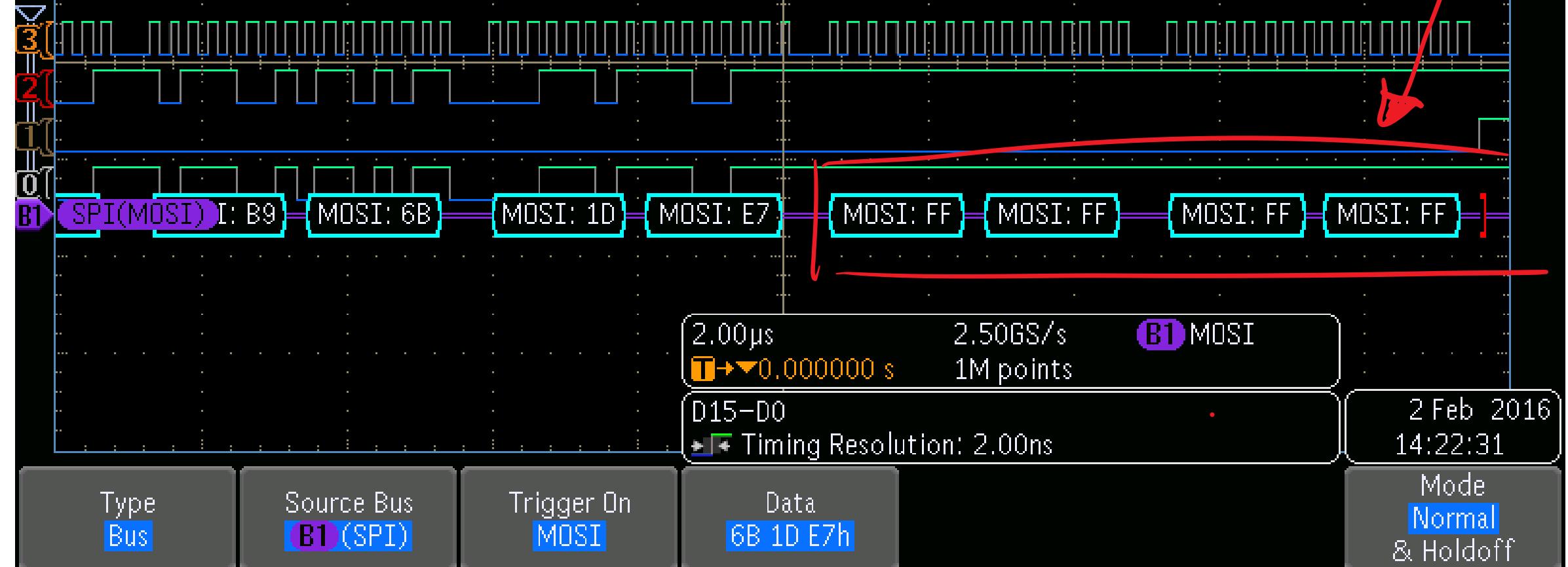
As $\textcircled{A} \rightarrow \textcircled{B}$ when code valid
 $\textcircled{A} \cancel{\rightarrow}$ when code invalid

\textcircled{A} = Validation (Hash?)

Tek Run

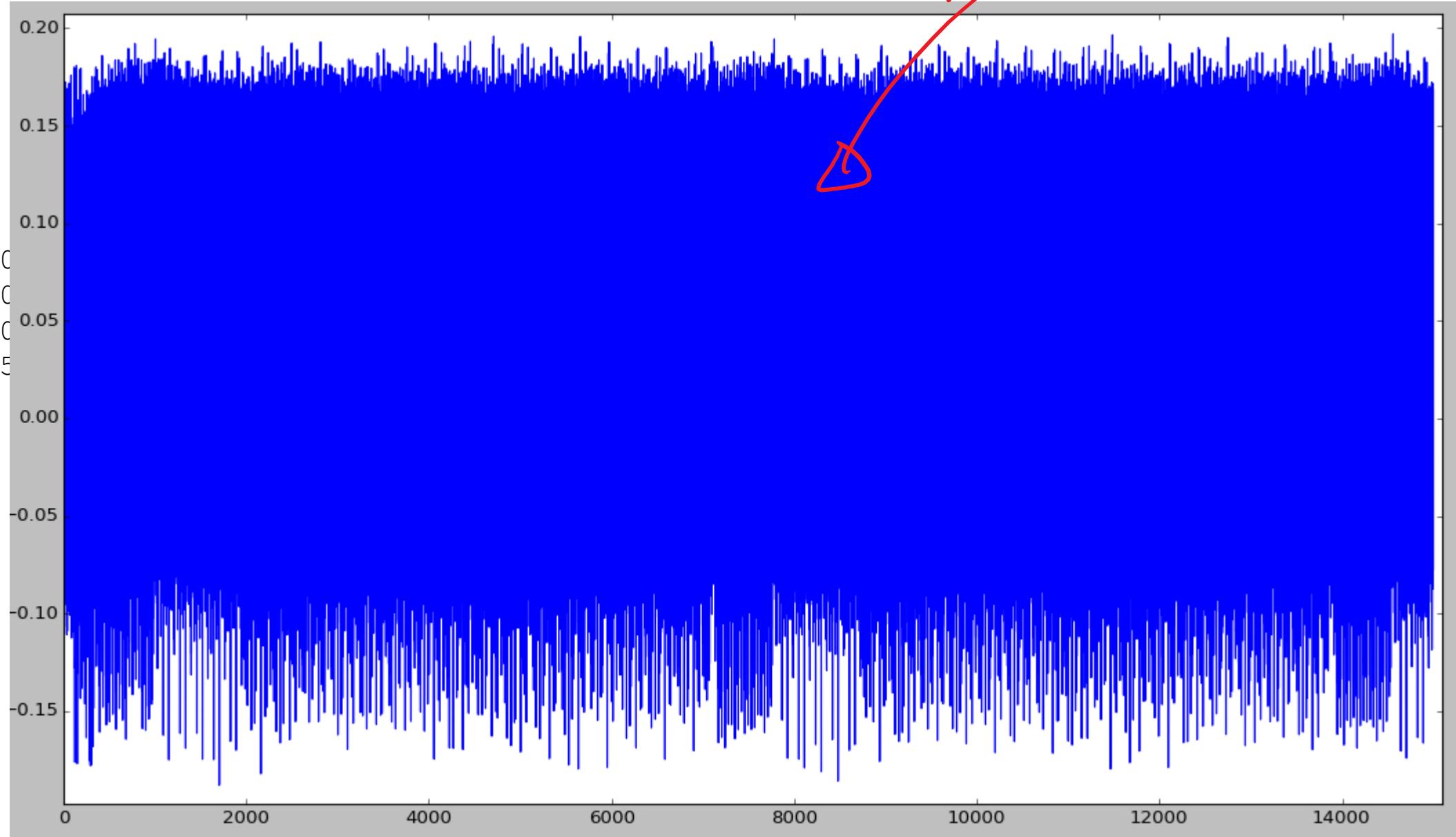
Trig?

Experiment with "Known" section where plaintext = 0's



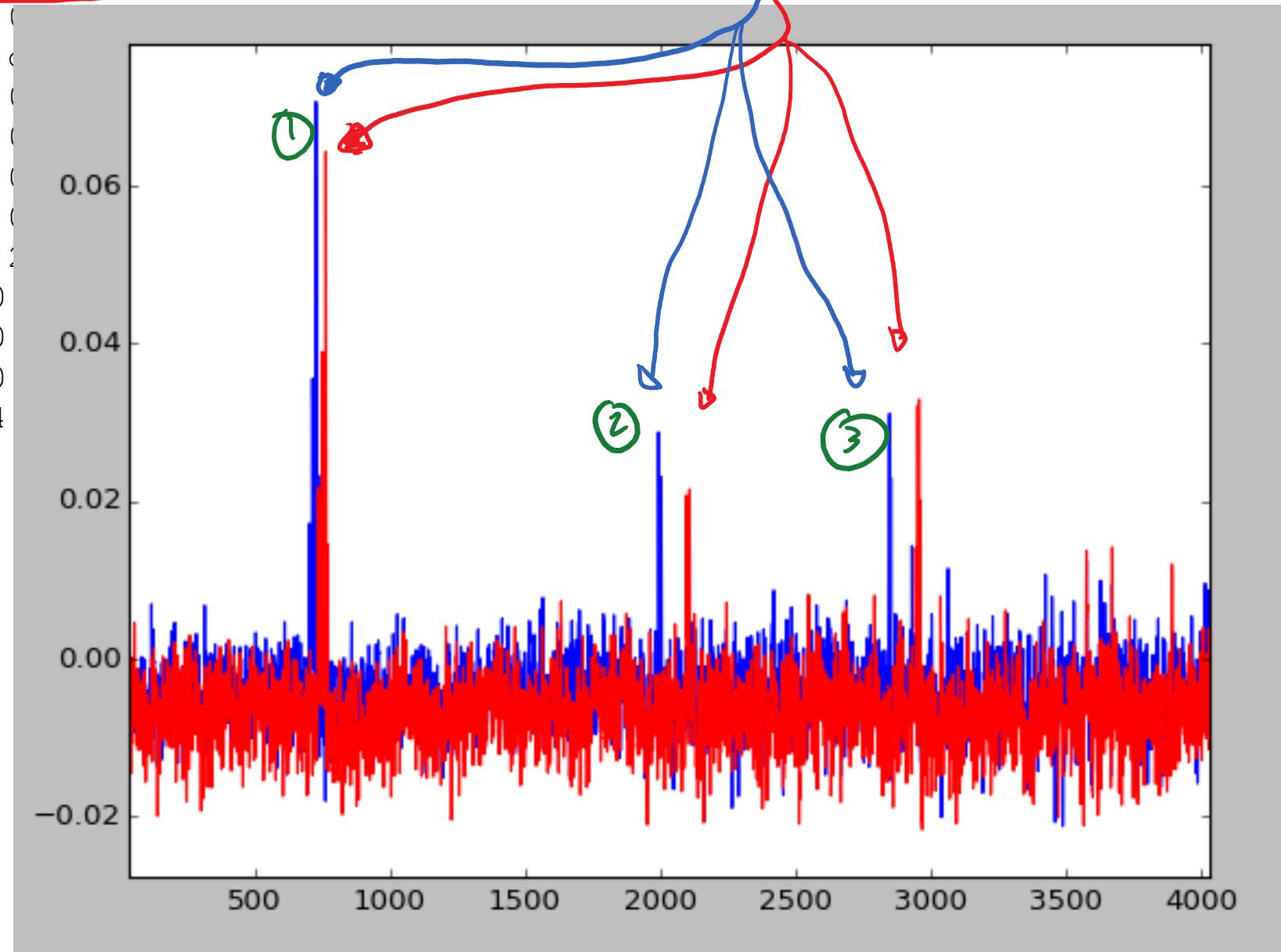
0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00
2: 00 00 00 00 ff ff ff 00 00 00 00 00 00 00 00 00
3: ff 00 00
4: 00 ff 00
5: 00 00 ff
6: 00 00 00
7: 70 0e 75
8: 8f f1 8a
9: 00 00 00
10: 00 00 00
11: 00 00 00
12: 00 00 00
13: a3 3c f5

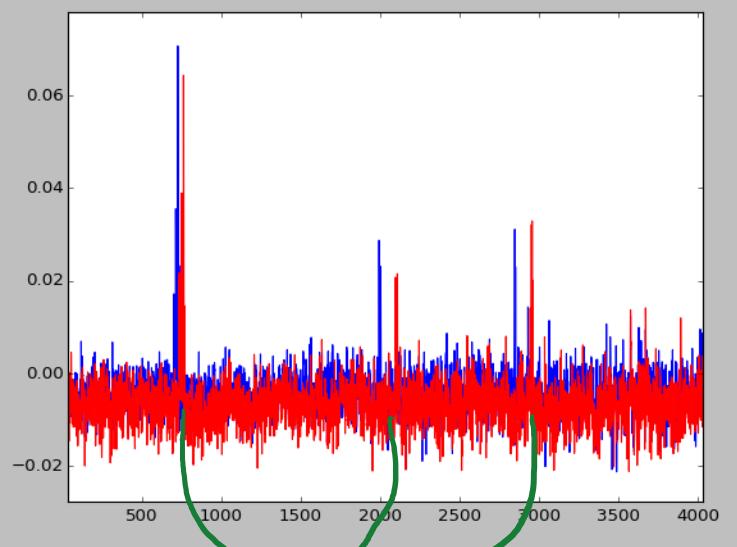
Raw power trace



0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1: ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00
2: 00 00 00 00 ft ff ff ff 00 00 00 00 00 00 00 00 00
3: ff 00 00 00
4: 00 ff 00 00
5: 00 00 ff 00
6: 00 00 00 ff 00
7: 70 0e 75 ad 00
8: 8f f1 8a 52 00
9: 00 00 00 00 20
10: 00 00 00 00
11: 00 00 00 00
12: 00 00 00 00
13: a3 3c f5 54

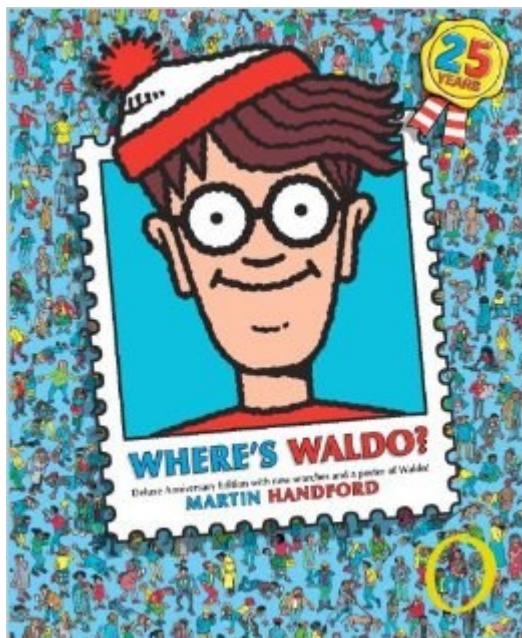
Difference Traces





Multiple Manipulations
↳ Some sort of feedback?

FINDING HASH



```
#Simple python script to try a bunch of hashes
import hashlib
raw_data = open('firmware_C311.bin', 'rb').read()
known_hash = raw_data[0:32]

test_hash = hashlib.algorithms_available

for startoffset in range(0x20, 0x28, 4):
    #Trim bytes off end, seems to be some header at end?
    for endoffset in range(0, -1024, -1):
        firmware = raw_data[startoffset:endoffset]
        for t in test_hash:
            h = hashlib.new(t)
            h.update(firmware)
            dig = h.hexdigest()

            #This example uses known hash, NOT read from start of file
            #If searching in middle, do:
            #if "77badb" in dig:
            if dig.startswith("77badb"):
                print dig
                print "***HASH FOUND***"
                print "start=0x%02x, end=0x%02x, type=%s"%(startoffset, endoffset, t)
```

BUILD SIGNATURES

```
import hashlib

fd = open('lockdown_hdd1.bin', 'rb')
orig_flash = fd.read()
fd.close()

#As an example - write 0xff's in blanks
programmed_file = [0xff]*16

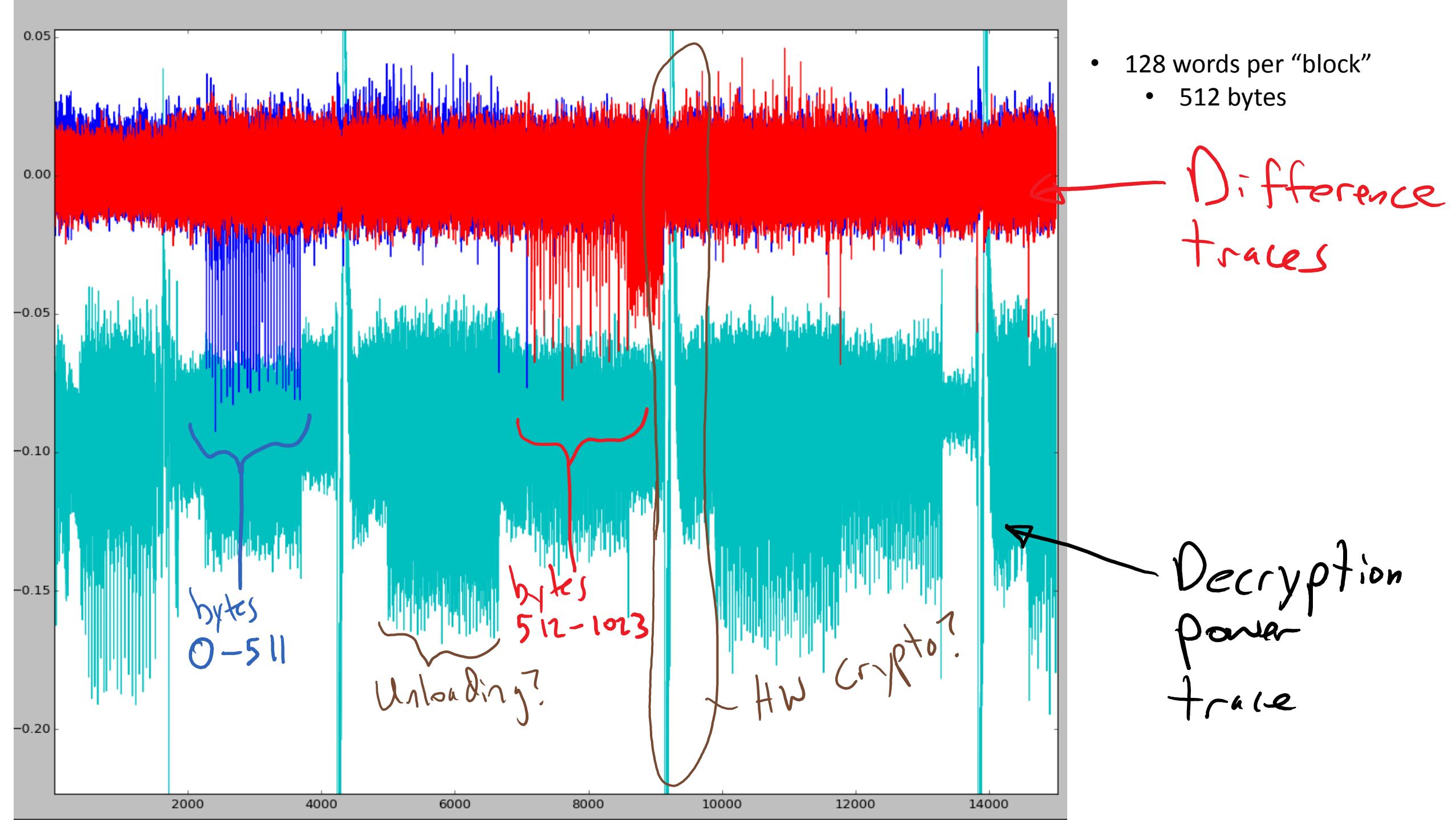
newdata = orig_flash[:]
newdata = [ord(d) for d in newdata]
for i in range(0x2044, 0x2044+16):
    newdata[i] = programmed_file[i-0x2044]

#Calculate new hash
newdata_temp = ''.join([chr(j) for j in newdata])
h = hashlib.new("sha256")
h.update(newdata_temp[0x2020:0x170F8])
shash = h.hexdigest()

#Add hash to file
i=0
for t in range(0, len(shash), 2):
    newdata[0x2000+i] = int(shash[t:(t+2)], 16)
    i += 1

#Save file
newdata = ''.join([chr(j) for j in newdata])

fd = open('lockdown_temp.bin', 'wb')
fd.write(newdata)
fd.close() |
```



FIRMWARE ATTACKS

- 1) Can cause arbitrary code to be decrypted.
- 2) Can move interrupt/reset vectors quasi-blindly.
- 3) If could determine either (a) part of stream cipher or (b) part of code (init routines?) may be able to build short "dumper".

HARD DRIVE SUMMARY

1. No secrets inside silicon
 2. Secure and normal variants of MB86C311 use same FW protection.
- ∴ Any company using these devices could decrypt this FW.

HARD DRIVE SUMMARY

3. Once F.W. is known,
all is lost. Possible to
brute-force password in <1s.
4. Various attack vectors to FW
itself due to flaws.

QUESTIONS?

Colin O'Flynn

@colinoflynn

oflynn.com

newae.com

coflynn@newae.com

Twitter

Website / Blog

Company