This project implements side channel analysis attack for the XTEA algorithm.
It is an entry for the NewAE 2018 contest.

https://en.wikipedia.org/wiki/XTEA
Because is a fairly small symmetric block cipher implementation it is a good candidate for boot-loaders and other embedded projects. With a 128bit key offers a good level of security. Question is how secure is when running on a 32bit microcontroller? Side channel attacks are like magic. First you don't believe your eyes when you recover something from an 8 bit processor. Then when you can convince people that is possible, arises the question of the 32bit architecture. Should be harder, if not impossible.
Harder?, yes, impossible No.
So lets build everything from ground up, and see how secure we are if we use XTEA in something.

The hardware:
For the tests i used a Mikroelektronika MIN-32
https://www.mikroe.com/mini-pic32mx
The board features a PIC32MX534F064H Microchip microcontroller. The board was programmed whit PICKIT3, erasing the Mikroelektronika bootloader.
Target software was developed in MPLAB X IDE , compiled with XC32 1.40 and legacy pic32 plib libraries (on Microchip`s website it is present in the archives).
Target is clocked from the chipwhisperer. Clock is routed on the target trough the PLL to further complicate things.

The target implements a simple XTEA decryption, using the Simpleserial protocol, baudrate 19200.
Trigger is wired from an IO toggle(RE6).
UART is connected to RD2 RD3 (UART1)
Power consumption is measured on the VCORE pin. Capacitor E3 is removed and connected trough a 1 OHM resistor. The voltage drop is amplified with the differential probe. To the capacitor is applied a 1.96v external power supply to overpower the internal regulator. The exact voltage depends on the chip.

A couple of words about the clock management. To replicate a more realistic scenario in the target the clock is routed trough the PLL and doubled. This not only introduces a clock doubling but also a significant phase shift. To overcome the effect we use an external clock divider before the target, and clock phase can be adjusted by routing trough logic gates. This could be a simple FPGA project, but building an FPGA project can be tedious. So I implemented it using the microchip express dev board in the PIC-s CLC-s. Clock enters on RA0, it is divided by the first CLC exiting on RC3. Also it is routed trough the other CLC-s to RC4 RC5 and RC6 each with a bit of delay. This is all peripherals. So the core is doing nothing. The project is ClockDivider.X

The algorithm is fairly simple, a couple of shits, additions and XORs.

```
for()
{
        v1 -= (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum>>11) & 3]);
        sum -= delta;
        v0 -= (((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum + key[sum & 3]);
}
```

We could attack the algorithm after the first XOR HW((((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum>>11) & 3]))
but because of compiler optimizations the best place is after it is subtracted from v1 and v0 because the value is stored.

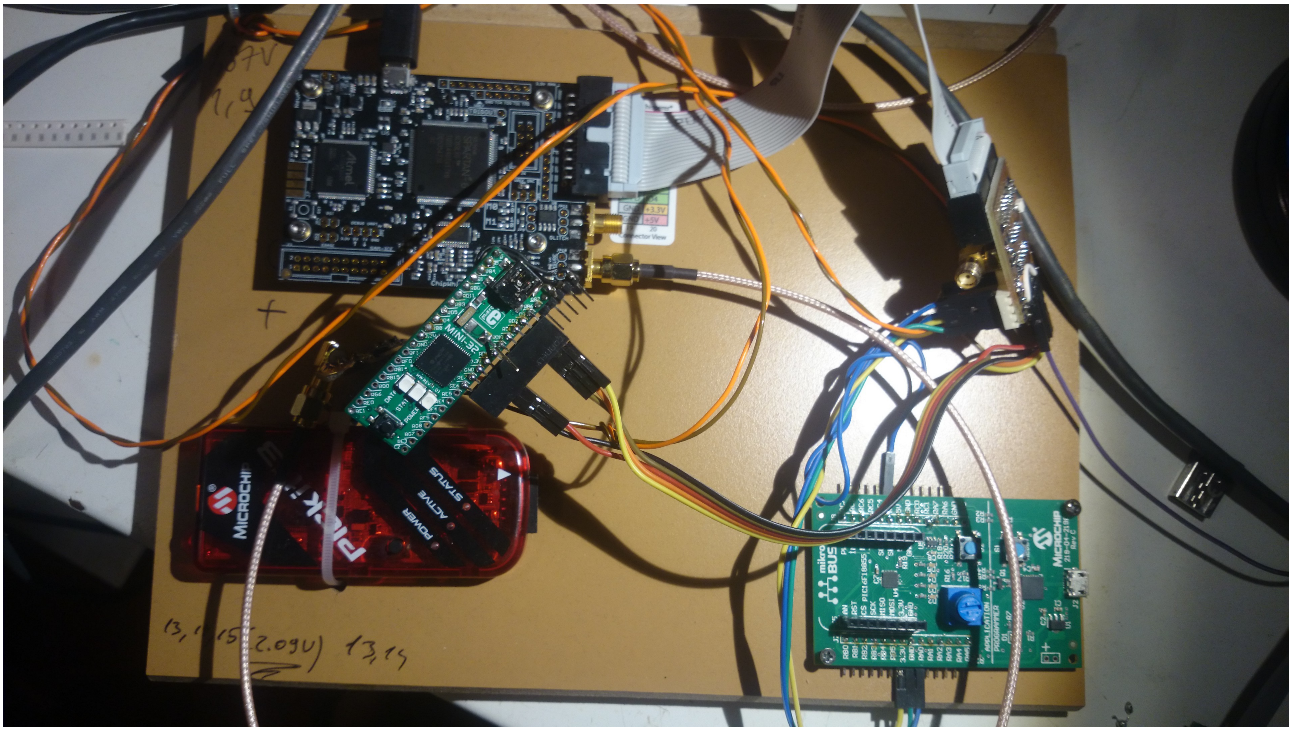
We only fuzz v0, v1 is always 0.

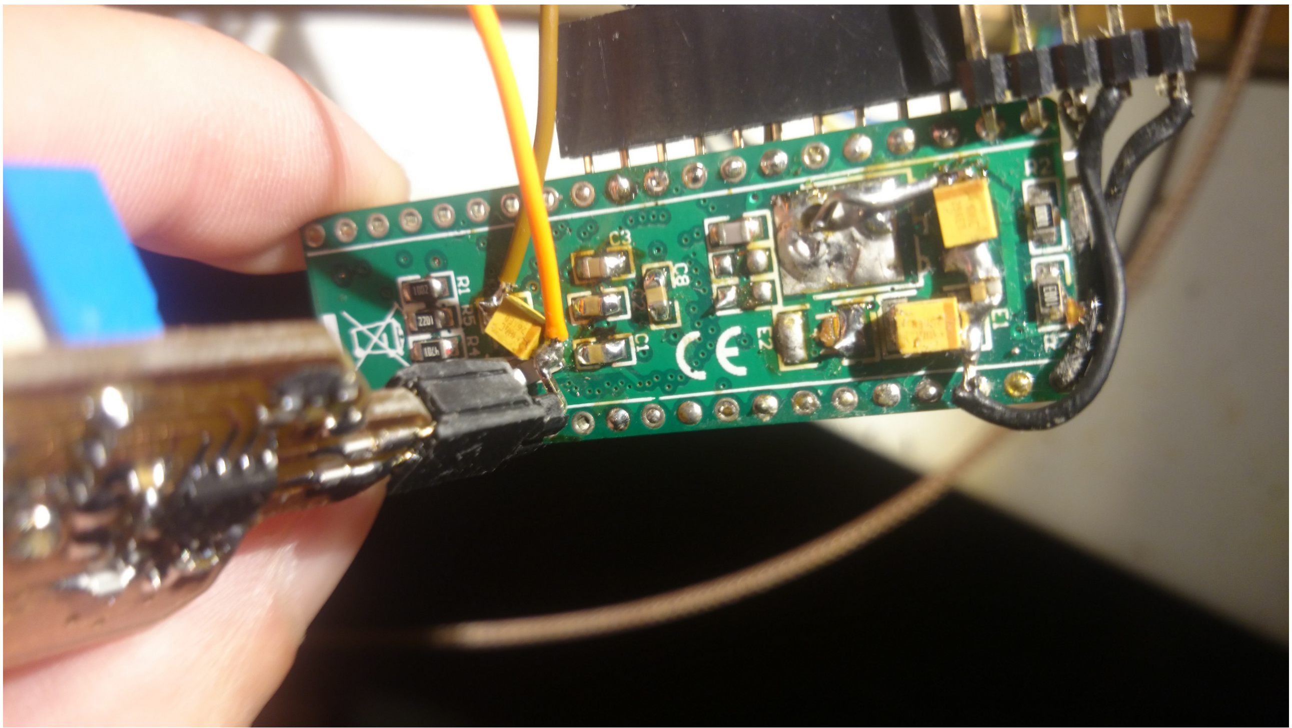
Because we are on a 32 bit micro, the calculated Hamming weight needs be for the whole 32 bits.
We have to attack the keys in the following order: 2,3,0,1

First we start from each key being 0xFFFFFFFF
Then after the attack we update this guess with the result. Usually after 2-3 iterations we arrive to the correct subkey.
To speed up the things we can restrict the point range, this also helps reducing the guessing noise.
To select the best range refer to Output vs. Point range diagram.

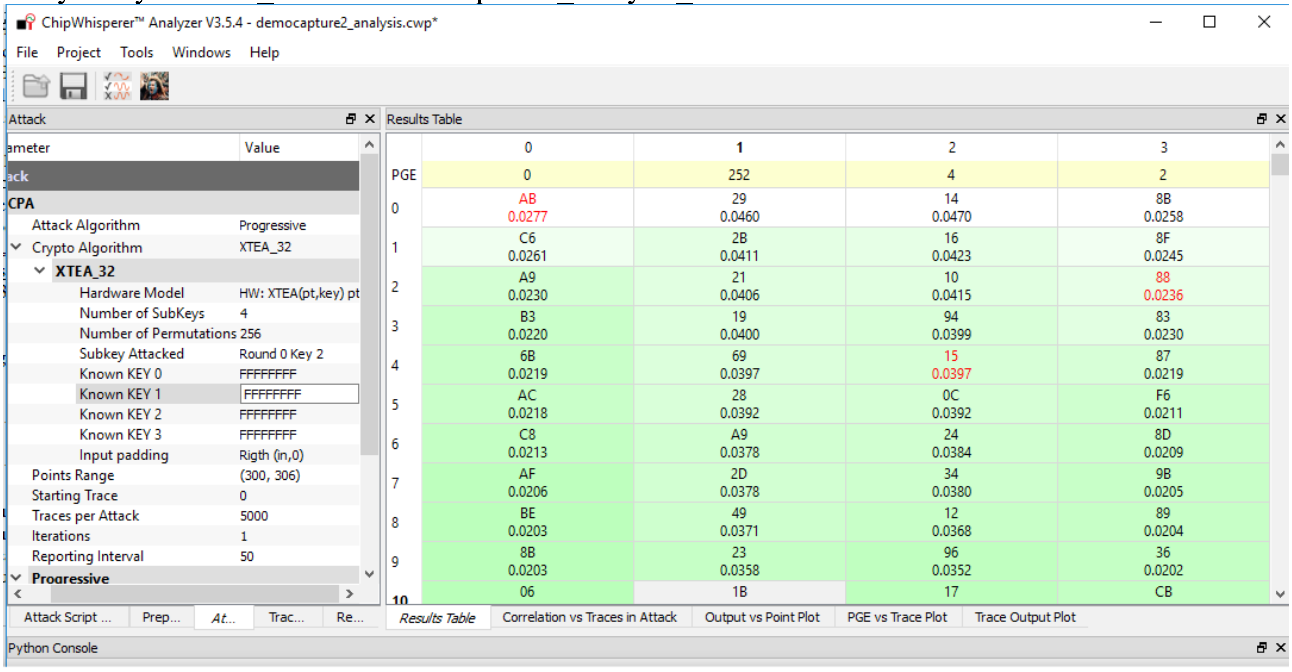
Python implementation of XTEA library inspired by
https://github.com/OpenXenManager/openxenmanager/blob/master/src/OXM/xtea.py

Conclusion. It a fairly slow attack, results heavily depend on noise and settings. But demonstrates that is not impossible.





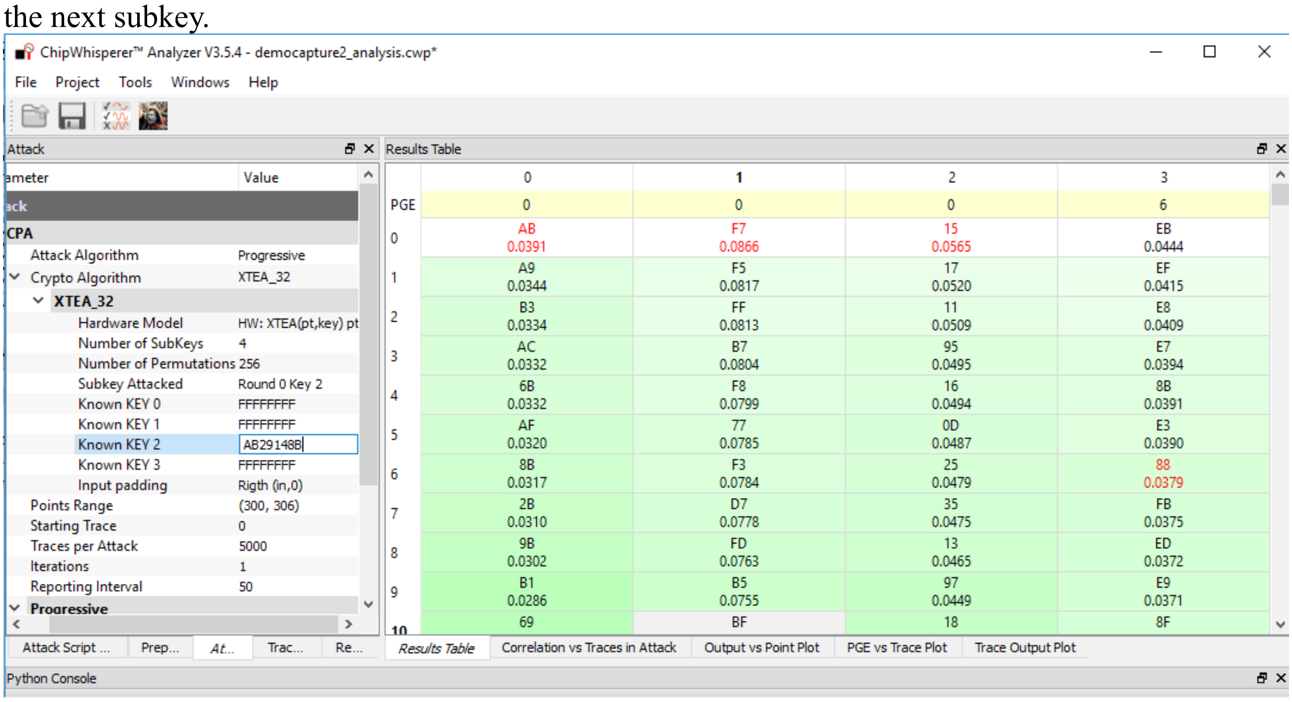
Example attack. Use the XTEA.py and XTEALIB.py from plugin folder. Simpleserial needs a slight modification to allow 4byte inputs. The captured data for this attack can be found in. This data is fairly noisy. XTEA_DEMO\democapture2_analysis_data



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 0 Key 2
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	FFFFFFFF
Known KEY 3	FFFFFFFF
Input padding	Rigth (in,0)
Points Range	(300, 306)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	252	4	2
0	AB 0.0277	29 0.0460	14 0.0470	8B 0.0258
1	C6 0.0261	2B 0.0411	16 0.0423	8F 0.0245
2	A9 0.0230	21 0.0406	10 0.0415	88 0.0236
3	B3 0.0220	19 0.0400	94 0.0399	83 0.0230
4	6B 0.0219	69 0.0397	15 0.0397	87 0.0219
5	AC 0.0218	28 0.0392	0C 0.0392	F6 0.0211
6	C8 0.0213	A9 0.0378	24 0.0384	8D 0.0209
7	AF 0.0206	2D 0.0378	34 0.0380	9B 0.0205
8	BE 0.0203	49 0.0371	12 0.0368	89 0.0204
9	8B 0.0203	23 0.0358	96 0.0352	36 0.0202
10	06	1B	17	CB

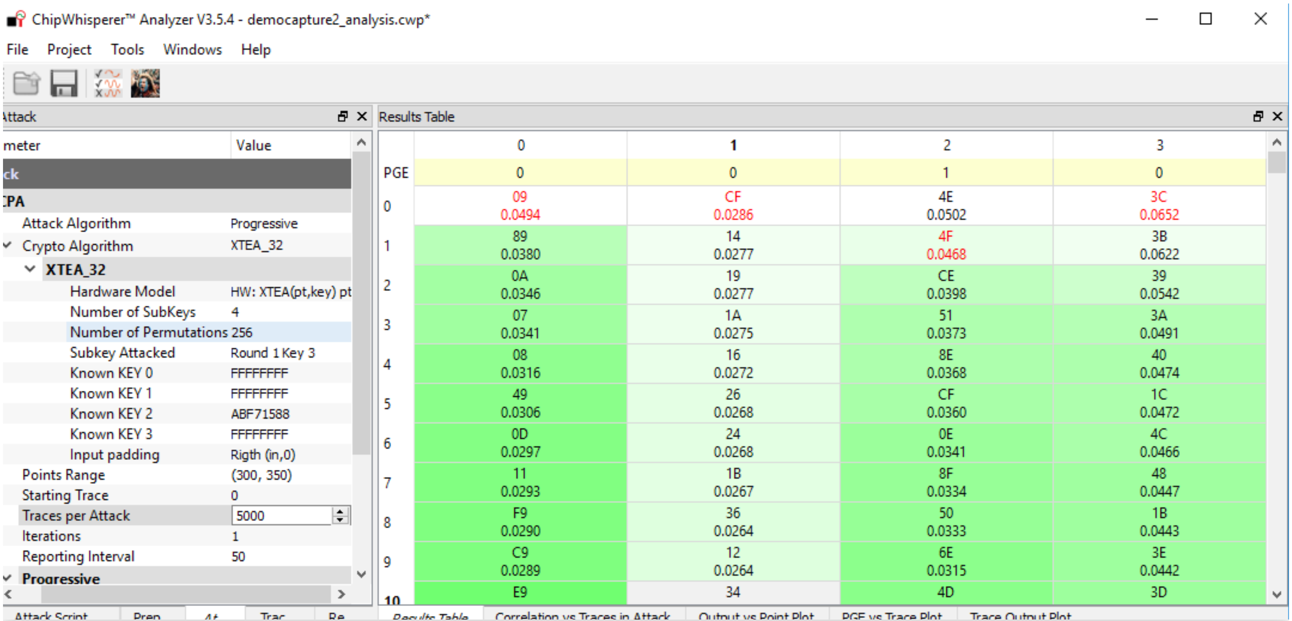
After the first attack we are still far from the truth. So we enter the guess AB29148B to the KnowKey 2 field and restart the attack. We repeat this 2-3 times then proceed to the next subkey.



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 0 Key 2
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	AB29148B
Known KEY 3	FFFFFFFF
Input padding	Rigth (in,0)
Points Range	(300, 306)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

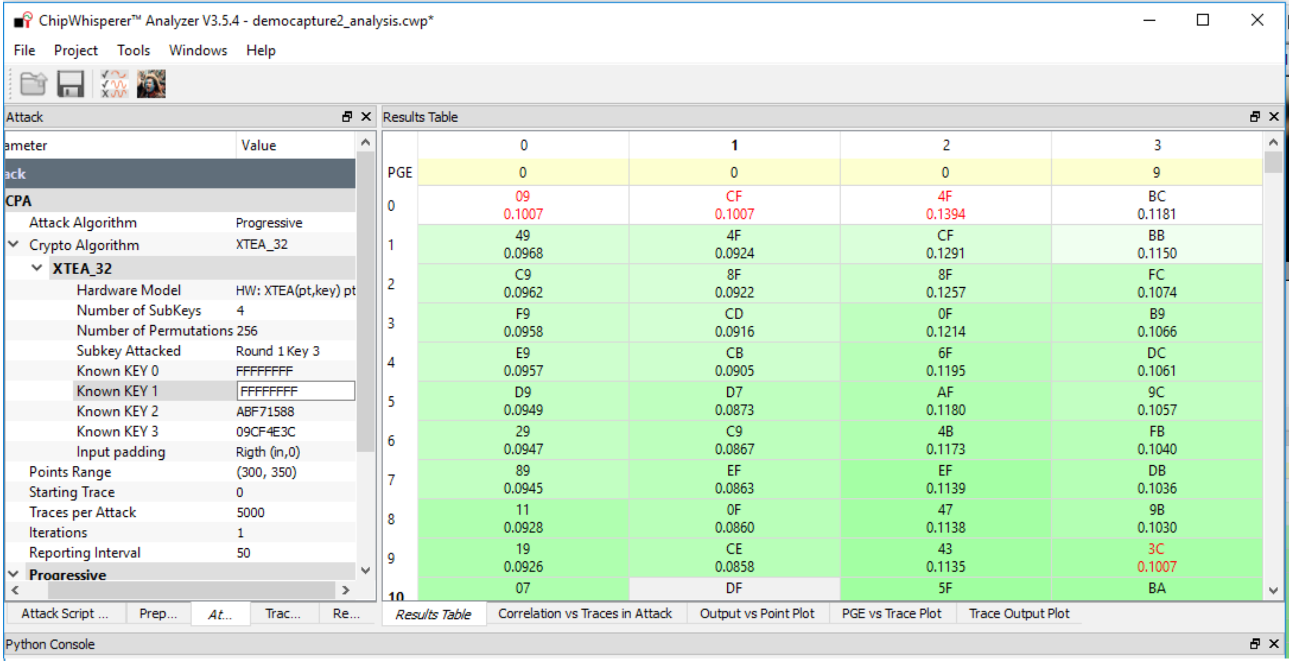
	0	1	2	3
PGE	0	0	0	6
0	AB 0.0391	F7 0.0866	15 0.0565	EB 0.0444
1	A9 0.0344	F5 0.0817	17 0.0520	EF 0.0415
2	B3 0.0334	FF 0.0813	11 0.0509	E8 0.0409
3	AC 0.0332	B7 0.0804	95 0.0495	E7 0.0394
4	6B 0.0332	F8 0.0799	16 0.0494	8B 0.0391
5	AF 0.0320	77 0.0785	0D 0.0487	E3 0.0390
6	8B 0.0317	F3 0.0784	25 0.0479	88 0.0379
7	2B 0.0310	D7 0.0778	35 0.0475	FB 0.0375
8	9B 0.0302	FD 0.0763	13 0.0465	ED 0.0372
9	B1 0.0286	B5 0.0755	97 0.0449	E9 0.0371
10	69	BF	18	8F

After the second round we are better off, but the last byte is still bad. But we are close. Lets cheat a bit and enter the correct key for the guess, and try the next key 3.We expand a bit the points range because the next operation happens later in time.



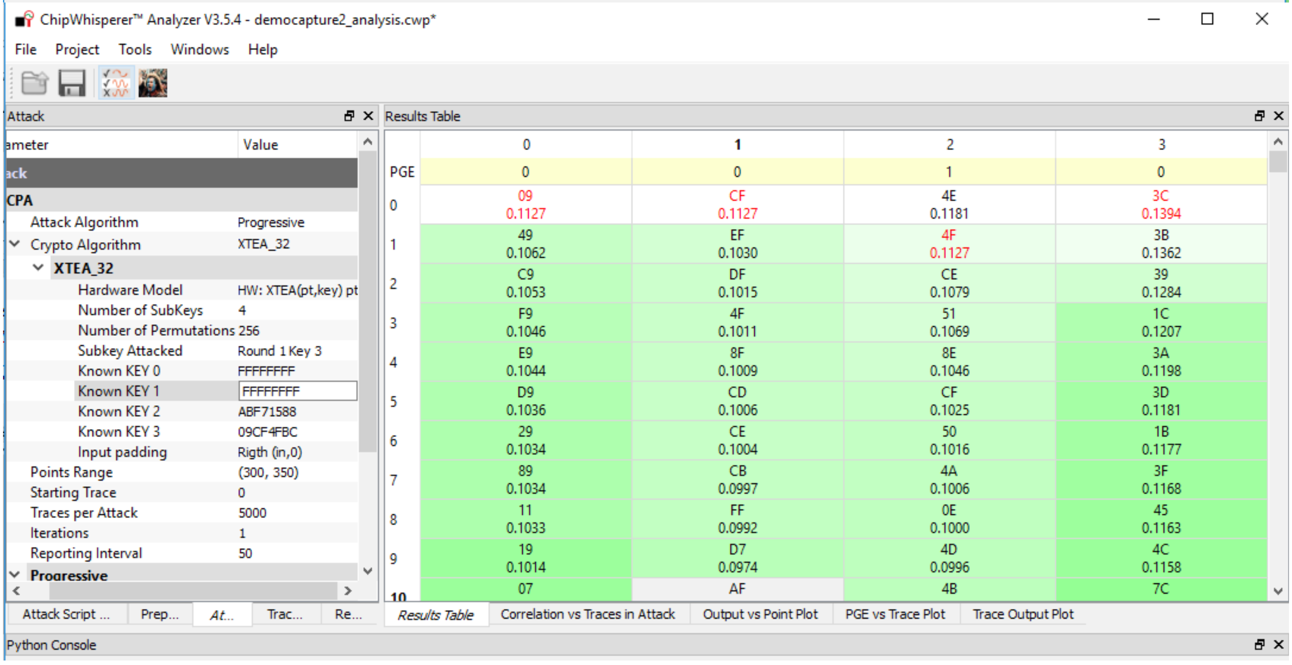
meter	Value
ck	
PA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 1 Key 3
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	FFFFFFFF
Input padding	Rigth (in,0)
Points Range	(300, 350)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	0	1	0
0	09 0.0494	CF 0.0286	4E 0.0502	3C 0.0652
1	89 0.0380	14 0.0277	4F 0.0468	3B 0.0622
2	0A 0.0346	19 0.0277	CE 0.0398	39 0.0542
3	07 0.0341	1A 0.0275	51 0.0373	3A 0.0491
4	08 0.0316	16 0.0272	8E 0.0368	40 0.0474
5	49 0.0306	26 0.0268	CF 0.0360	1C 0.0472
6	0D 0.0297	24 0.0268	0E 0.0341	4C 0.0466
7	11 0.0293	1B 0.0267	8F 0.0334	48 0.0447
8	F9 0.0290	36 0.0264	50 0.0333	1B 0.0443
9	C9 0.0289	12 0.0264	6E 0.0315	3E 0.0442
10	E9	34	4D	3D



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 1 Key 3
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4E3C
Input padding	Rigth (in,0)
Points Range	(300, 350)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

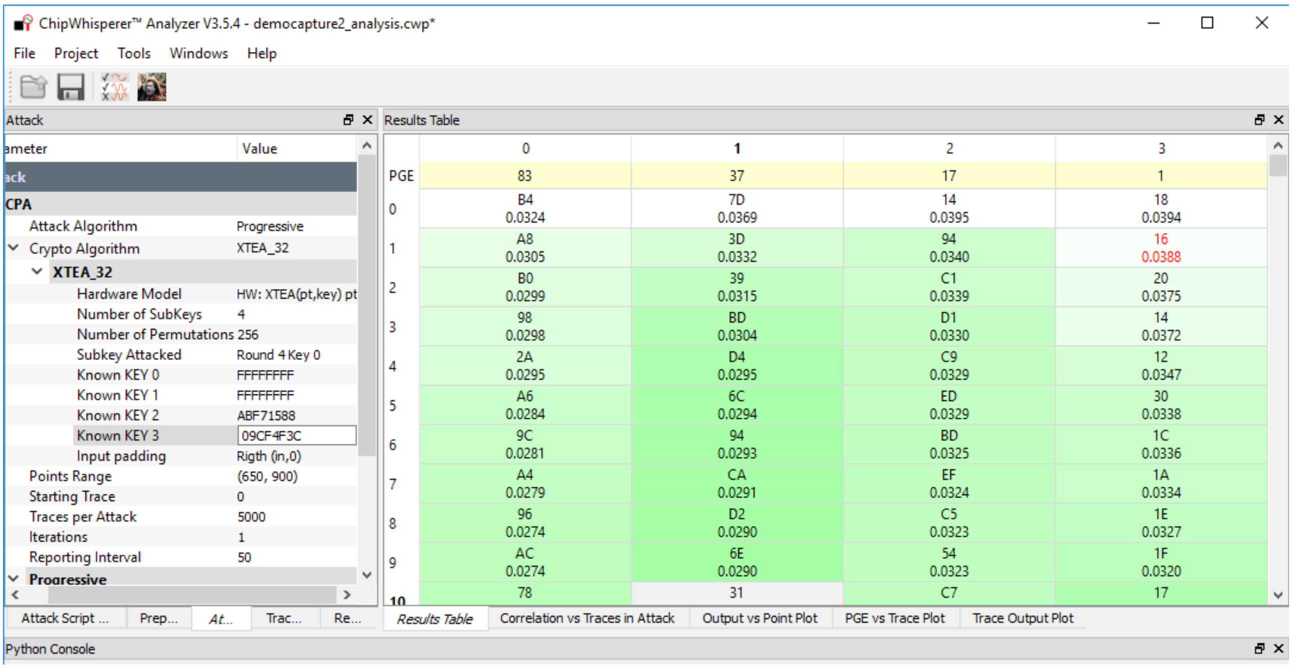
	0	1	2	3
PGE	0	0	0	9
0	09 0.1007	CF 0.1007	4F 0.1394	BC 0.1181
1	49 0.0968	4F 0.0924	CF 0.1291	BB 0.1150
2	C9 0.0962	8F 0.0922	8F 0.1257	FC 0.1074
3	F9 0.0958	CD 0.0916	0F 0.1214	B9 0.1066
4	E9 0.0957	CB 0.0905	6F 0.1195	DC 0.1061
5	D9 0.0949	D7 0.0873	AF 0.1180	9C 0.1057
6	29 0.0947	C9 0.0867	4B 0.1173	FB 0.1040
7	89 0.0945	EF 0.0863	EF 0.1139	DB 0.1036
8	11 0.0928	0F 0.0860	47 0.1138	9B 0.1030
9	19 0.0926	CE 0.0858	43 0.1135	3C 0.1007
10	07	DF	5F	BA



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 1 Key 3
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4FBC
Input padding	Rigth (in,0)
Points Range	(300, 350)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

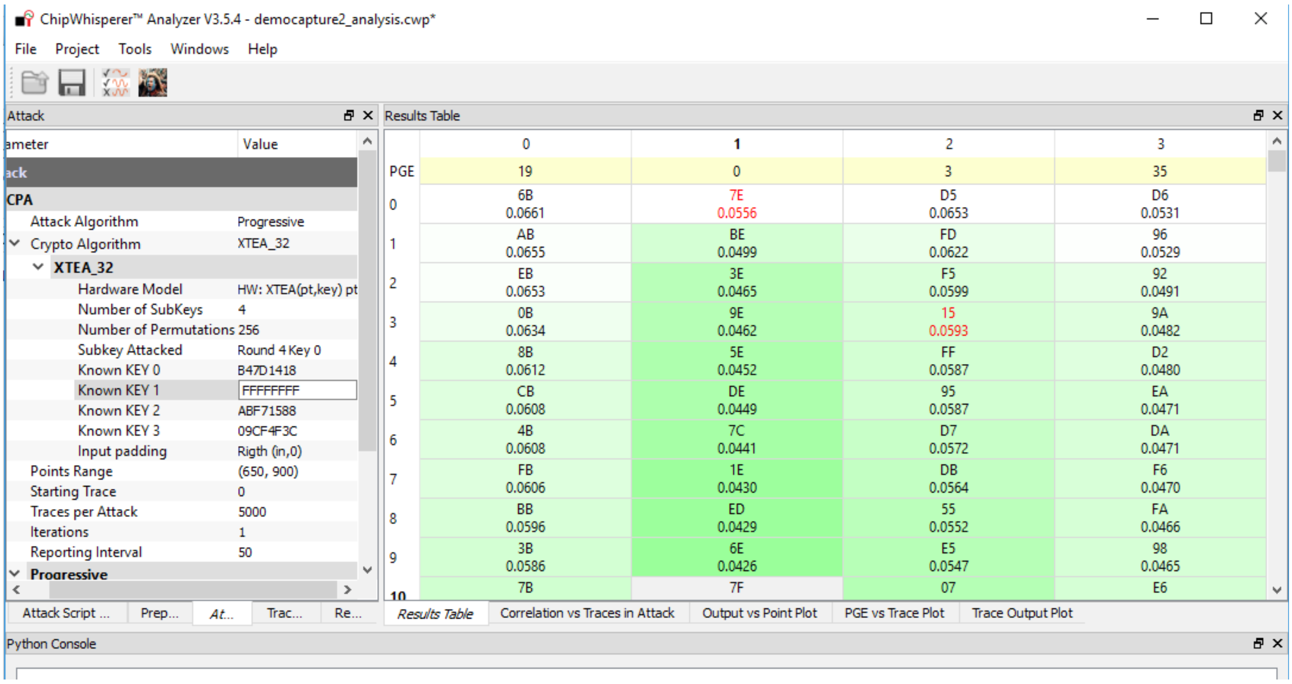
	0	1	2	3
PGE	0	0	1	0
0	09 0.1127	CF 0.1127	4E 0.1181	3C 0.1394
1	49 0.1062	EF 0.1030	4F 0.1127	3B 0.1362
2	C9 0.1053	DF 0.1015	CE 0.1079	39 0.1284
3	F9 0.1046	4F 0.1011	51 0.1069	1C 0.1207
4	E9 0.1044	8F 0.1009	8E 0.1046	3A 0.1198
5	D9 0.1036	CD 0.1006	CF 0.1025	3D 0.1181
6	29 0.1034	CE 0.1004	50 0.1016	1B 0.1177
7	89 0.1034	CB 0.0997	4A 0.1006	3F 0.1168
8	11 0.1033	FF 0.0992	0E 0.1000	45 0.1163
9	19 0.1014	D7 0.0974	4D 0.0996	4C 0.1158
10	07	AF	4B	7C

The same result like after the first iteration. But still we are pretty close. Lets cheat again a bit. And try the remaining keys. If attacking the next key fails. We can go back, and try the next guess.



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(650, 900)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

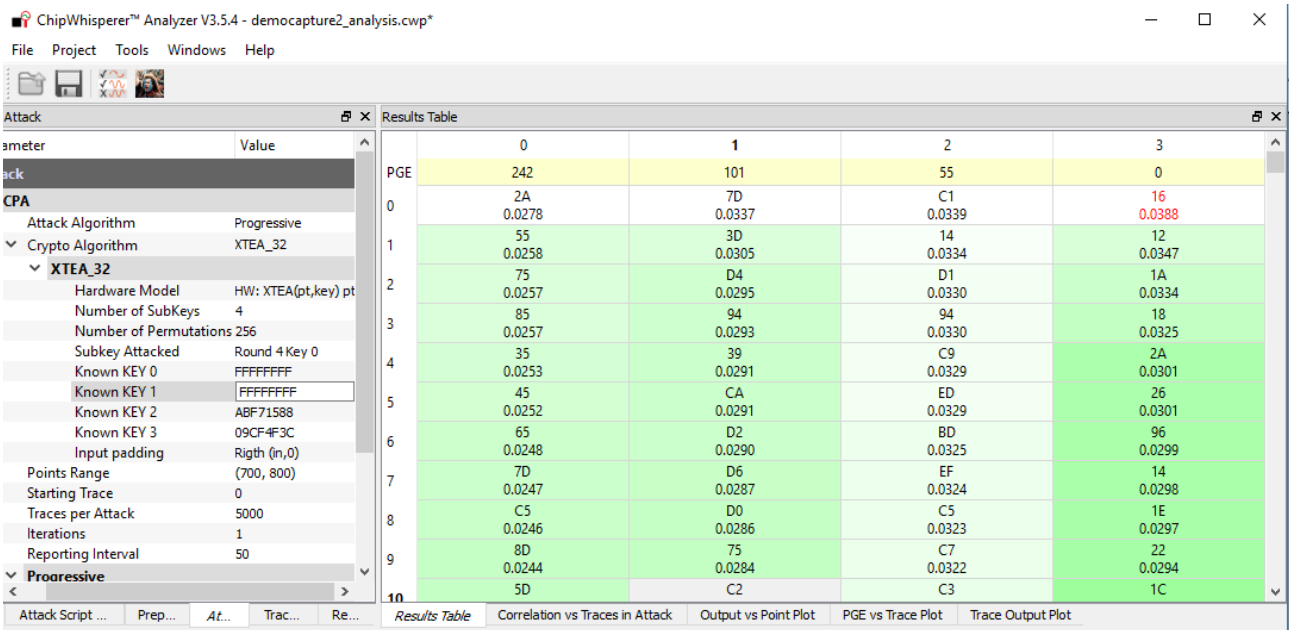
	0	1	2	3
PGE	83	37	17	1
0	B4 0.0324	7D 0.0369	14 0.0395	18 0.0394
1	A8 0.0305	3D 0.0332	94 0.0340	16 0.0388
2	B0 0.0299	39 0.0315	C1 0.0339	20 0.0375
3	98 0.0298	BD 0.0304	D1 0.0330	14 0.0372
4	2A 0.0295	D4 0.0295	C9 0.0329	12 0.0347
5	A6 0.0284	6C 0.0294	ED 0.0329	30 0.0338
6	9C 0.0281	94 0.0293	BD 0.0325	1C 0.0336
7	A4 0.0279	CA 0.0291	EF 0.0324	1A 0.0334
8	96 0.0274	D2 0.0290	C5 0.0323	1E 0.0327
9	AC 0.0274	6E 0.0290	54 0.0323	1F 0.0320
10	78	31	C7	17



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	B47D1418
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(650, 900)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	19	0	3	35
0	6B 0.0661	7E 0.0556	D5 0.0653	D6 0.0531
1	AB 0.0655	BE 0.0499	FD 0.0622	96 0.0529
2	EB 0.0653	3E 0.0465	F5 0.0599	92 0.0491
3	0B 0.0634	9E 0.0462	15 0.0593	9A 0.0482
4	8B 0.0612	5E 0.0452	FF 0.0587	D2 0.0480
5	CB 0.0608	DE 0.0449	95 0.0587	EA 0.0471
6	4B 0.0608	7C 0.0441	D7 0.0572	DA 0.0471
7	FB 0.0606	1E 0.0430	DB 0.0564	F6 0.0470
8	BB 0.0596	ED 0.0429	55 0.0552	FA 0.0466
9	3B 0.0586	6E 0.0426	E5 0.0547	98 0.0465
10	7B	7F	07	E6

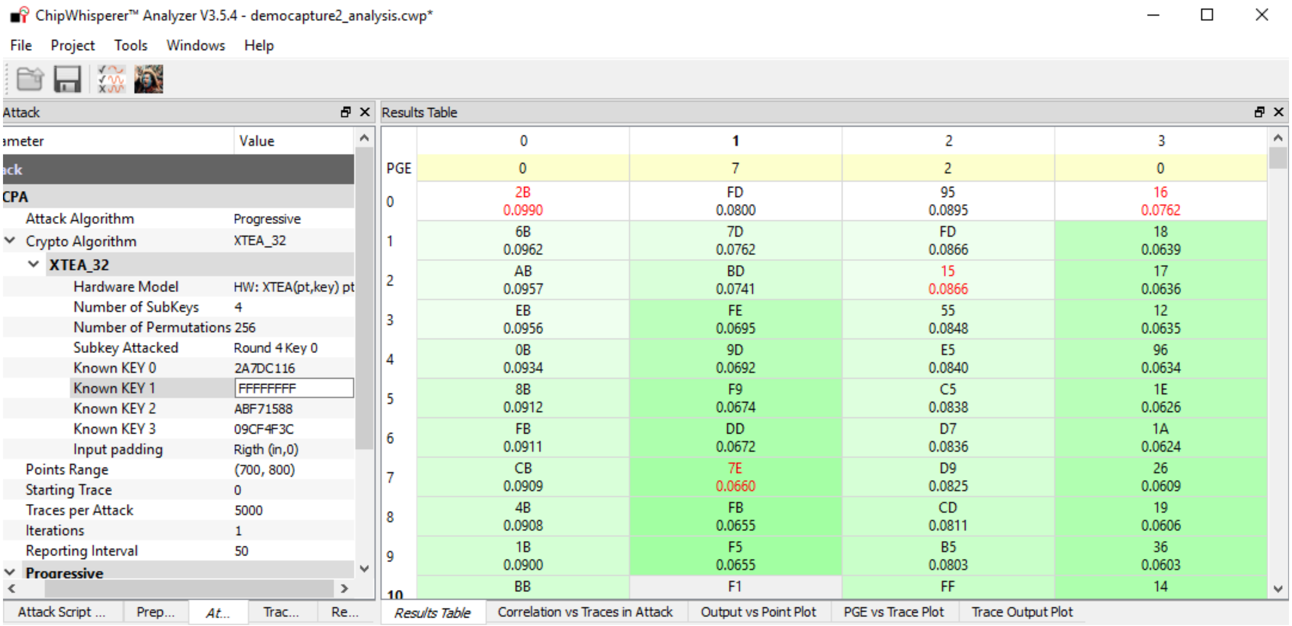
We are getting pretty much nothing . This means our range is too wide. We have to narrow down on POI-s better. Changing ranges and running again from 0xFFFFFFFF



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	FFFFFFFF
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 800)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	242	101	55	0
0	2A 0.0278	7D 0.0337	C1 0.0339	16 0.0388
1	55 0.0258	3D 0.0305	14 0.0334	12 0.0347
2	75 0.0257	D4 0.0295	D1 0.0330	1A 0.0334
3	85 0.0257	94 0.0293	94 0.0330	18 0.0325
4	35 0.0253	39 0.0291	C9 0.0329	2A 0.0301
5	45 0.0252	CA 0.0291	ED 0.0329	26 0.0301
6	65 0.0248	D2 0.0290	BD 0.0325	96 0.0299
7	7D 0.0247	D6 0.0287	EF 0.0324	14 0.0298
8	C5 0.0246	D0 0.0286	C5 0.0323	1E 0.0297
9	8D 0.0244	75 0.0284	C7 0.0322	22 0.0294
10	5D	C2	C3	1C

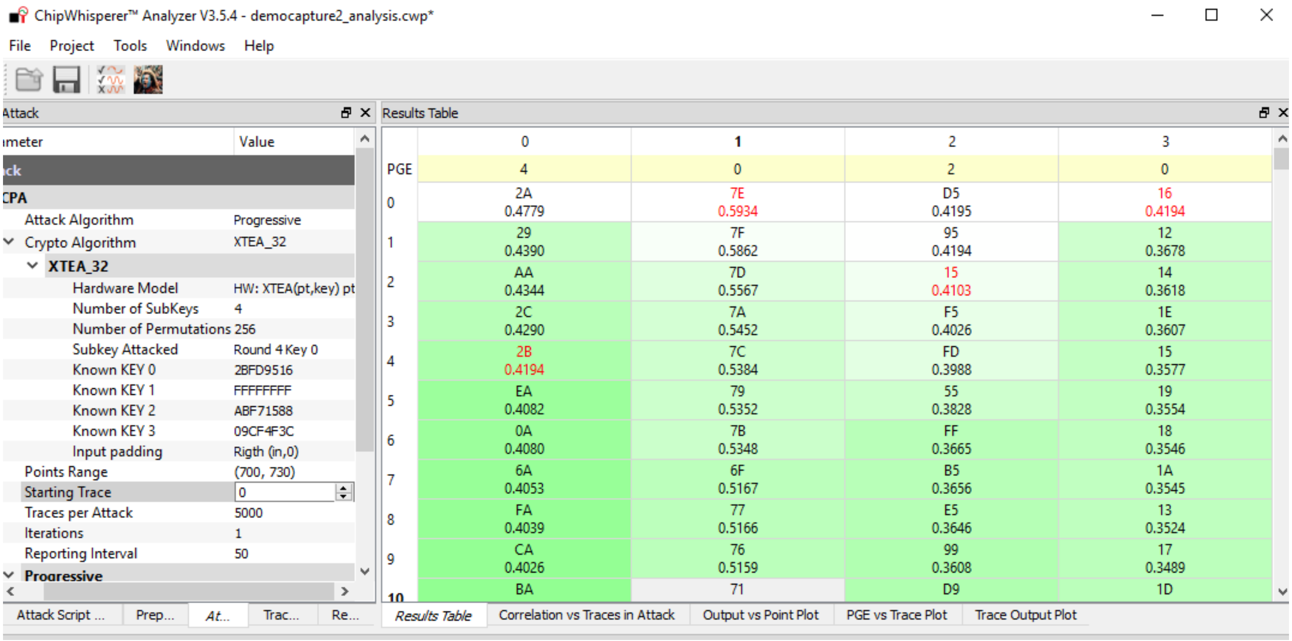
Ok,



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	2A7DC116
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 800)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	7	2	0
0	2B 0.0990	FD 0.0800	95 0.0895	16 0.0762
1	6B 0.0962	7D 0.0762	FD 0.0866	18 0.0639
2	AB 0.0957	BD 0.0741	15 0.0866	17 0.0636
3	EB 0.0956	FE 0.0695	55 0.0848	12 0.0635
4	0B 0.0934	9D 0.0692	E5 0.0840	96 0.0634
5	8B 0.0912	F9 0.0674	C5 0.0838	1E 0.0626
6	FB 0.0911	DD 0.0672	D7 0.0836	1A 0.0624
7	CB 0.0909	7E 0.0660	D9 0.0825	26 0.0609
8	4B 0.0908	FB 0.0655	CD 0.0811	19 0.0606
9	1B 0.0900	F5 0.0655	B5 0.0803	36 0.0603
10	BB	F1	FF	14

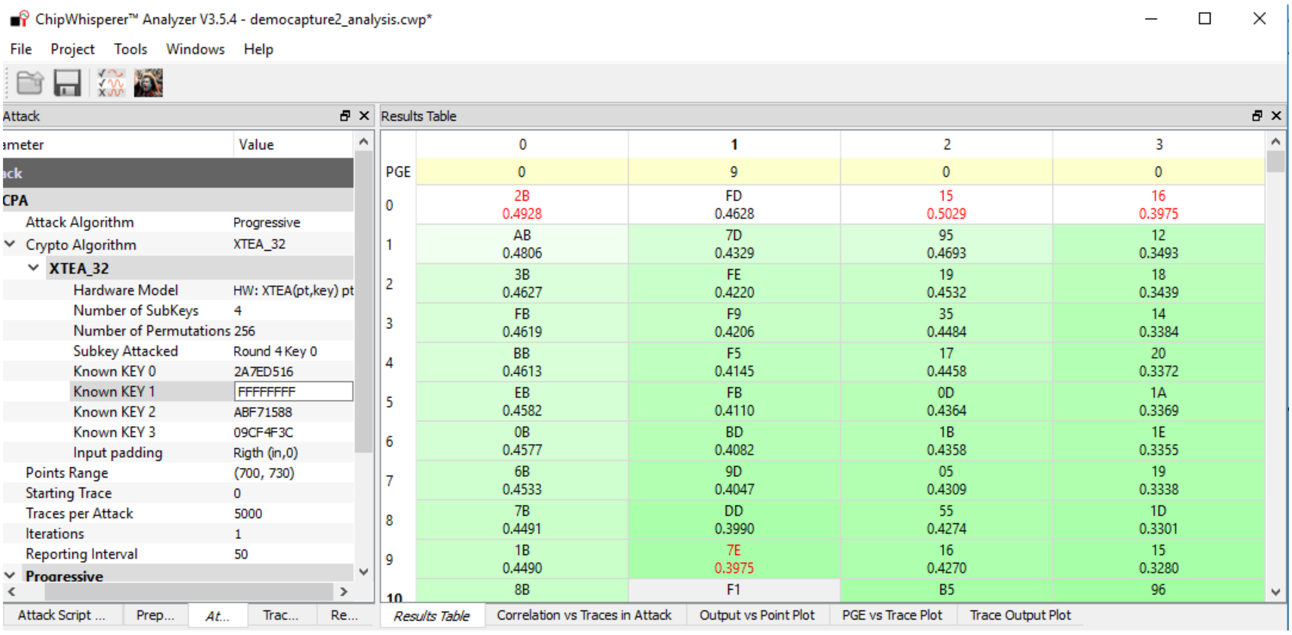
Better



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	2BFD9516
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 730)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	4	0	2	0
0	2A 0.4779	7E 0.5934	D5 0.4195	16 0.4194
1	29 0.4390	7F 0.5862	95 0.4194	12 0.3678
2	AA 0.4344	7D 0.5567	15 0.4103	14 0.3618
3	2C 0.4290	7A 0.5452	F5 0.4026	1E 0.3607
4	2B 0.4194	7C 0.5384	FD 0.3988	15 0.3577
5	EA 0.4082	79 0.5352	55 0.3828	19 0.3554
6	0A 0.4080	7B 0.5348	FF 0.3665	18 0.3546
7	6A 0.4053	6F 0.5167	B5 0.3656	1A 0.3545
8	FA 0.4039	77 0.5166	E5 0.3646	13 0.3524
9	CA 0.4026	76 0.5159	99 0.3608	17 0.3489
10	BA	71	D9	1D

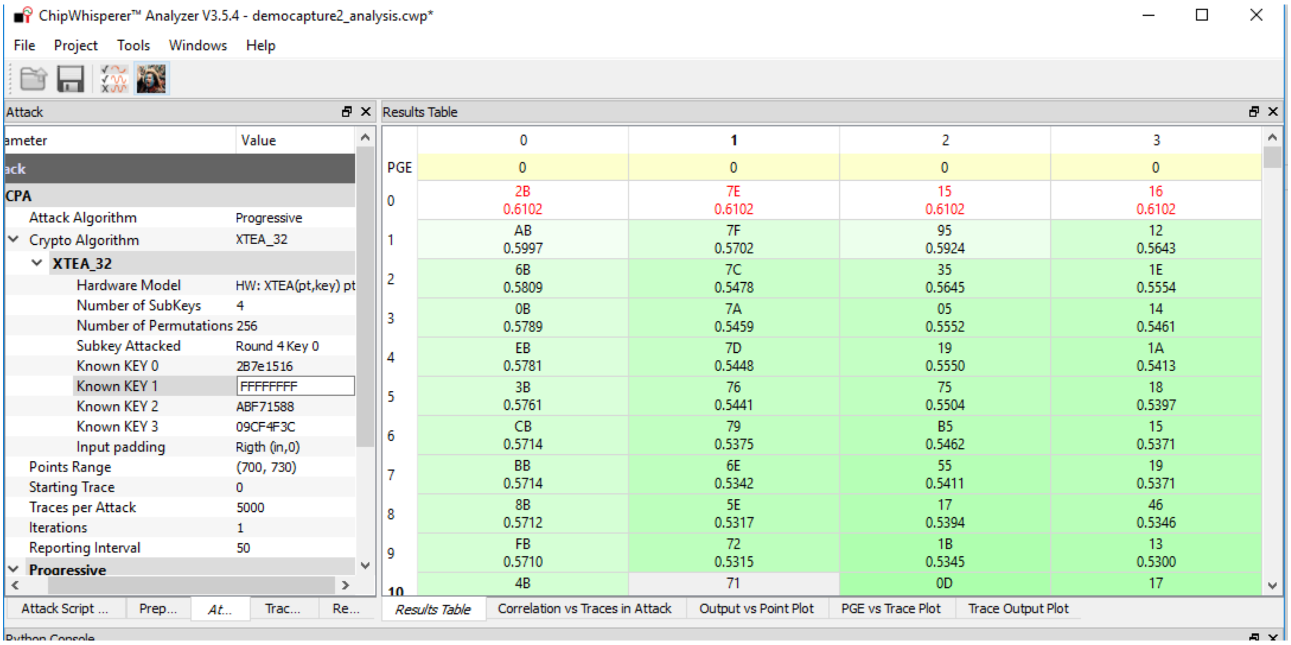
Oh



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	2A7ED516
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 730)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	9	0	0
0	2B 0.4928	FD 0.4628	15 0.5029	16 0.3975
1	AB 0.4806	7D 0.4329	95 0.4693	12 0.3493
2	3B 0.4627	FE 0.4220	19 0.4532	18 0.3439
3	FB 0.4619	F9 0.4206	35 0.4484	14 0.3384
4	BB 0.4613	F5 0.4145	17 0.4458	20 0.3372
5	EB 0.4582	FB 0.4110	0D 0.4364	1A 0.3369
6	0B 0.4577	BD 0.4082	1B 0.4358	1E 0.3355
7	6B 0.4533	9D 0.4047	05 0.4309	19 0.3338
8	7B 0.4491	DD 0.3990	55 0.4274	1D 0.3301
9	1B 0.4490	7E 0.3975	16 0.4270	15 0.3280
10	8B	F1	B5	96

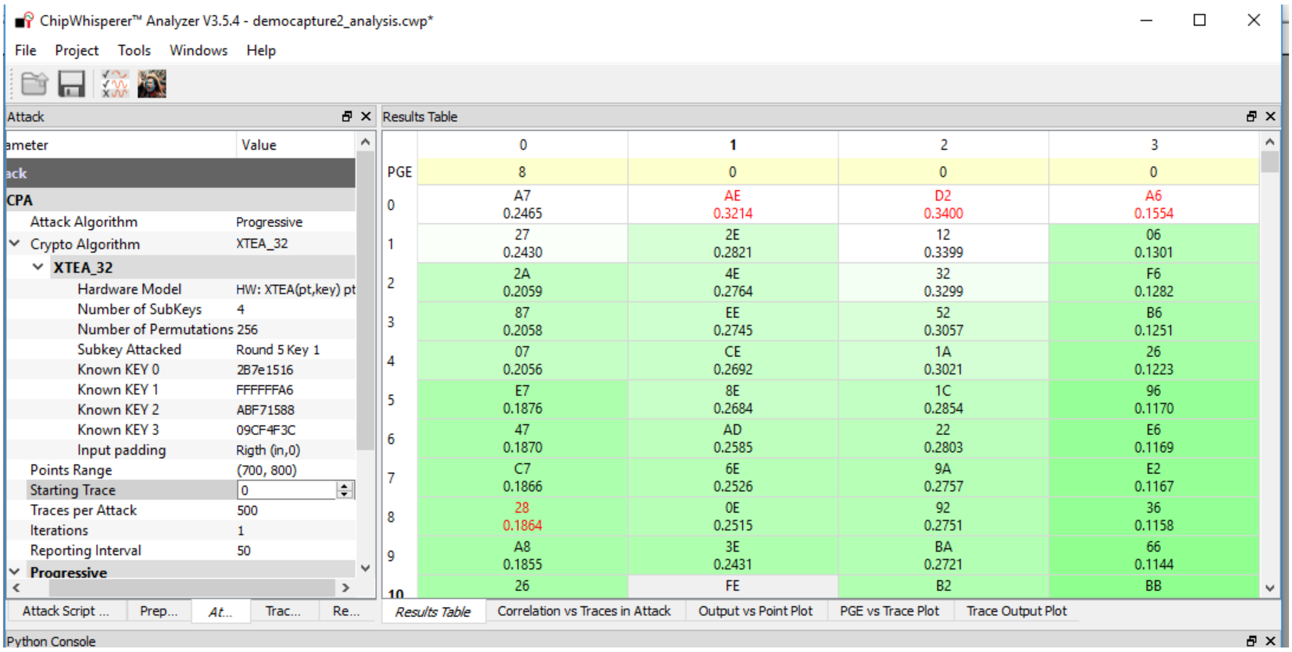
Perfect



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 4 Key 0
Known KEY 0	2B7e1516
Known KEY 1	FFFFFFFF
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 730)
Starting Trace	0
Traces per Attack	5000
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	0	0	0
0	2B 0.6102	7E 0.6102	15 0.6102	16 0.6102
1	AB 0.5997	7F 0.5702	95 0.5924	12 0.5643
2	6B 0.5809	7C 0.5478	35 0.5645	1E 0.5554
3	0B 0.5789	7A 0.5459	05 0.5552	14 0.5461
4	EB 0.5781	7D 0.5448	19 0.5550	1A 0.5413
5	3B 0.5761	76 0.5441	75 0.5504	18 0.5397
6	CB 0.5714	79 0.5375	B5 0.5462	15 0.5371
7	BB 0.5714	6E 0.5342	55 0.5411	19 0.5371
8	8B 0.5712	5E 0.5317	17 0.5394	46 0.5346
9	FB 0.5710	72 0.5315	1B 0.5345	13 0.5300
10	4B	71	0D	17

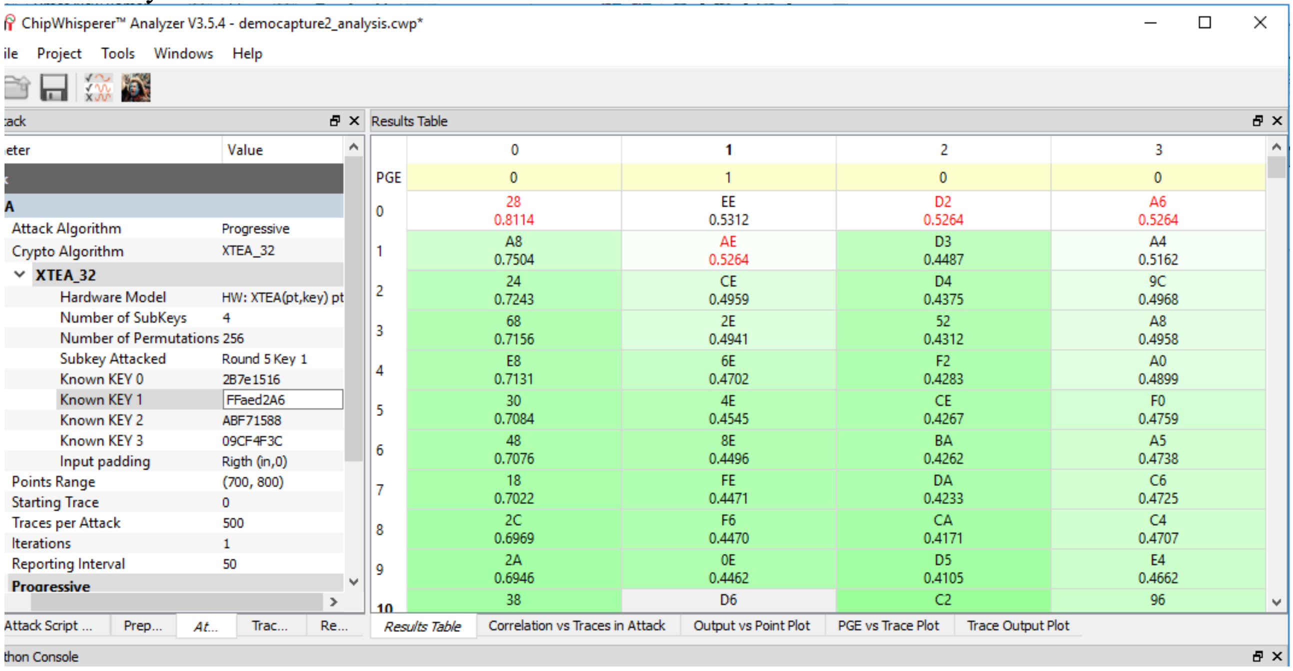
Lets try the last key to.



ameter	Value
ack	
CPA	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 5 Key 1
Known KEY 0	2B7e1516
Known KEY 1	FFFFFFA6
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 800)
Starting Trace	0
Traces per Attack	500
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	8	0	0	0
0	A7 0.2465	AE 0.3214	D2 0.3400	A6 0.1554
1	27 0.2430	2E 0.2821	12 0.3399	06 0.1301
2	2A 0.2059	4E 0.2764	32 0.3299	F6 0.1282
3	87 0.2058	EE 0.2745	52 0.3057	B6 0.1251
4	07 0.2056	CE 0.2692	1A 0.3021	26 0.1223
5	E7 0.1876	8E 0.2684	1C 0.2854	96 0.1170
6	47 0.1870	AD 0.2585	22 0.2803	E6 0.1169
7	C7 0.1866	6E 0.2526	9A 0.2757	E2 0.1167
8	28 0.1864	0E 0.2515	92 0.2751	36 0.1158
9	A8 0.1855	3E 0.2431	BA 0.2721	66 0.1144
10	26	FE	B2	BB

The last key is also recoverable.

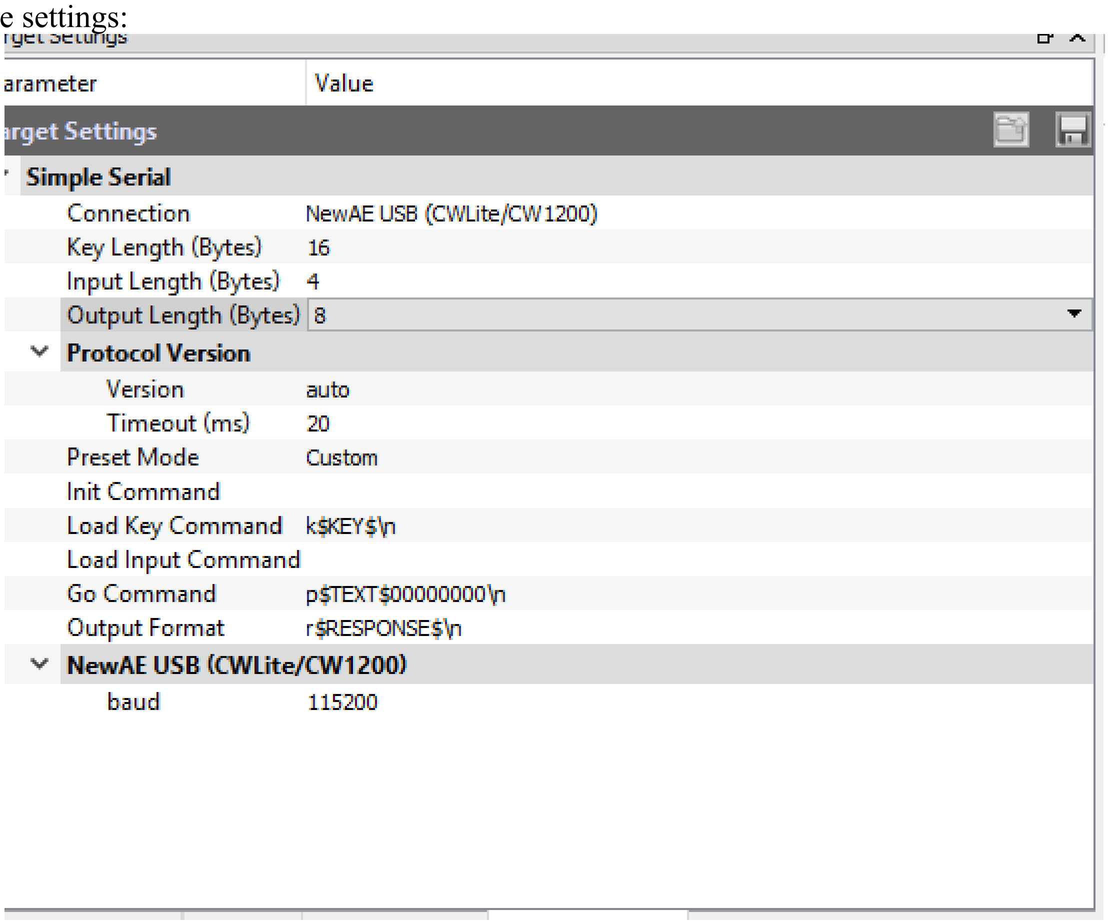


eter	Value
A	
Attack Algorithm	Progressive
Crypto Algorithm	XTEA_32
XTEA_32	
Hardware Model	HW: XTEA(pt,key) pt
Number of SubKeys	4
Number of Permutations	256
Subkey Attacked	Round 5 Key 1
Known KEY 0	2B7e1516
Known KEY 1	FFaed2A6
Known KEY 2	ABF71588
Known KEY 3	09CF4F3C
Input padding	Rigth (in,0)
Points Range	(700, 800)
Starting Trace	0
Traces per Attack	500
Iterations	1
Reporting Interval	50
Progressive	

	0	1	2	3
PGE	0	1	0	0
0	28 0.8114	EE 0.5312	D2 0.5264	A6 0.5264
1	A8 0.7504	AE 0.5264	D3 0.4487	A4 0.5162
2	24 0.7243	CE 0.4959	D4 0.4375	9C 0.4968
3	68 0.7156	2E 0.4941	52 0.4312	A8 0.4958
4	E8 0.7131	6E 0.4702	F2 0.4283	A0 0.4899
5	30 0.7084	4E 0.4545	CE 0.4267	F0 0.4759
6	48 0.7076	8E 0.4496	BA 0.4262	A5 0.4738
7	18 0.7022	FE 0.4471	DA 0.4233	C6 0.4725
8	2C 0.6969	F6 0.4470	CA 0.4171	C4 0.4707
9	2A 0.6946	0E 0.4462	D5 0.4105	E4 0.4662
10	38	D6	C2	96

This data is not the best example, but demonstrates that is feasible to attack a 32bit system running XTEA.

Capture settings:



arameter	Value
arget Settings	
Simple Serial	
Connection	NewAE USB (CWLite/CW1200)
Key Length (Bytes)	16
Input Length (Bytes)	4
Output Length (Bytes)	8
Protocol Version	
Version	auto
Timeout (ms)	20
Preset Mode	Custom
Init Command	
Load Key Command	kKEY\n
Load Input Command	
Go Command	p$TEXT$00000000\n
Output Format	r$RESPONSE$\n
NewAE USB (CWLite/CW1200)	
baud	115200