Side Channel Analysis

CPA

권용빈

목차

내용 ㅡ
부채널분석

암호가 동작중인 하드웨어에서 부가적으로 발생하는 물리적인 정보를 분석하여 키를 획득하는 방법

이러한 정보는 아예 숨기는 것은 불가능하다.

내용 ㅡ
전력분석

내용 ㅡ
전력분석

내용 ㅡ
SPA

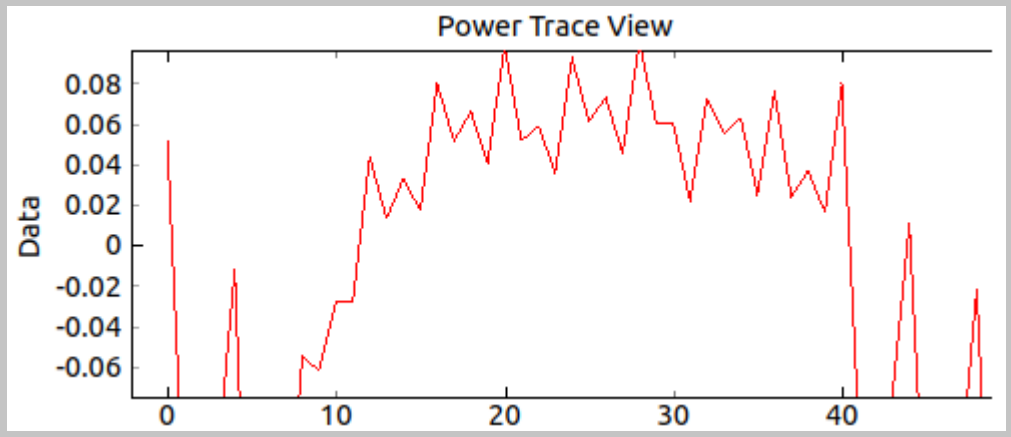
01 파형 수집

02 파형 확인

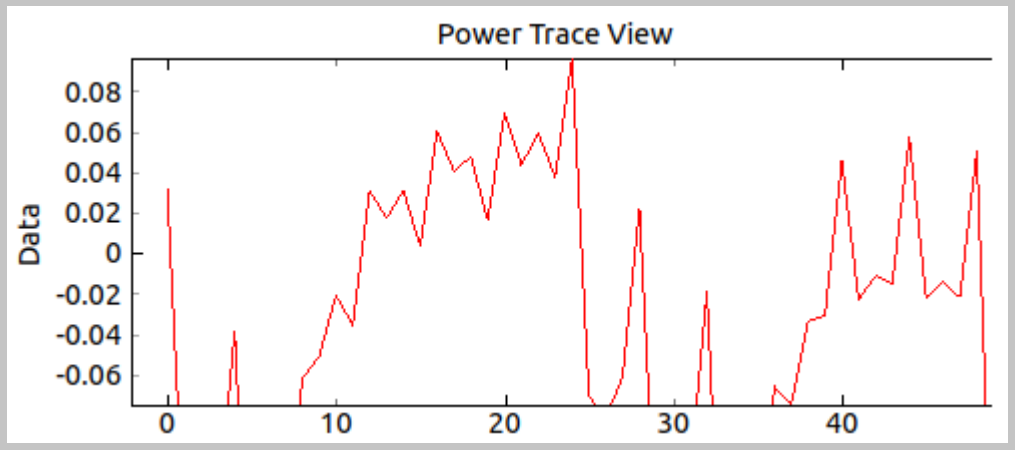
03 정보 획득

MICROCHIP

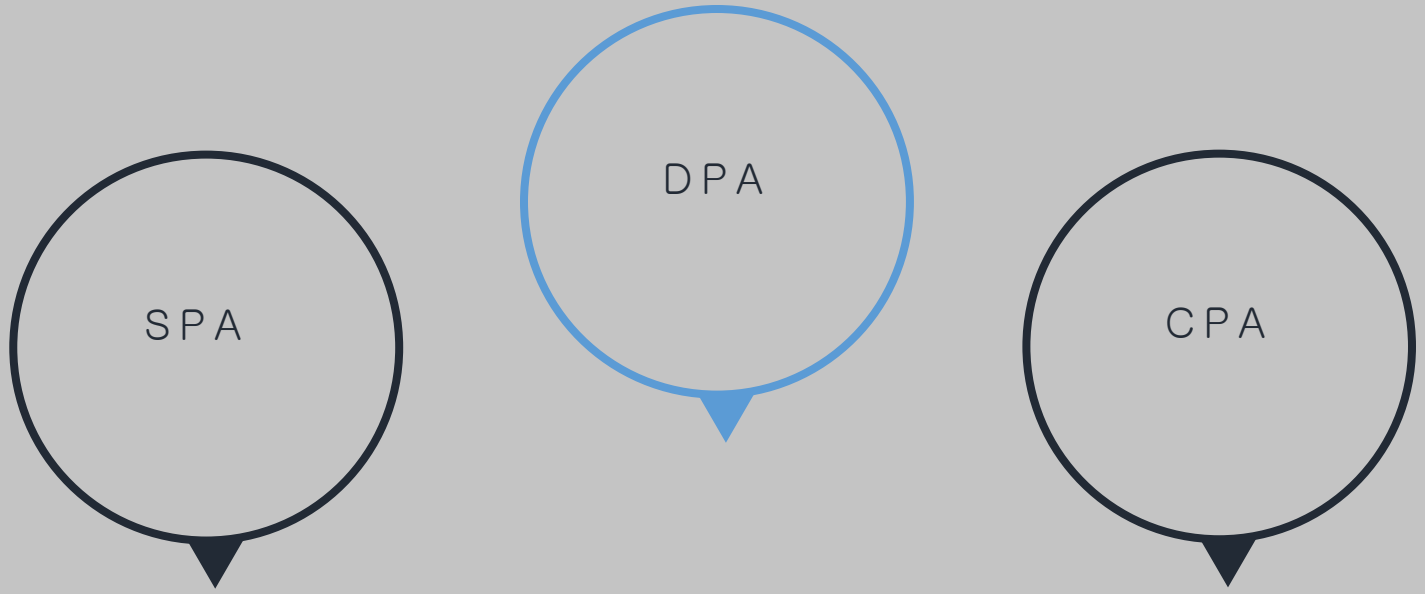
AVR Assembler
Instructions



4번의 NOP 연산



4번의 NOP 연산


SPA
DPA
CPA

전력 분석

$T_{0\ldots N}$

$H_{0\ldots N}\ by\ Hamming\ Weight$

$A_0 < -T\ with\ low\ H$
$A_1 < -T\ with\ high\ H$

$D = E\ (A_0)\ - E(A_1)$

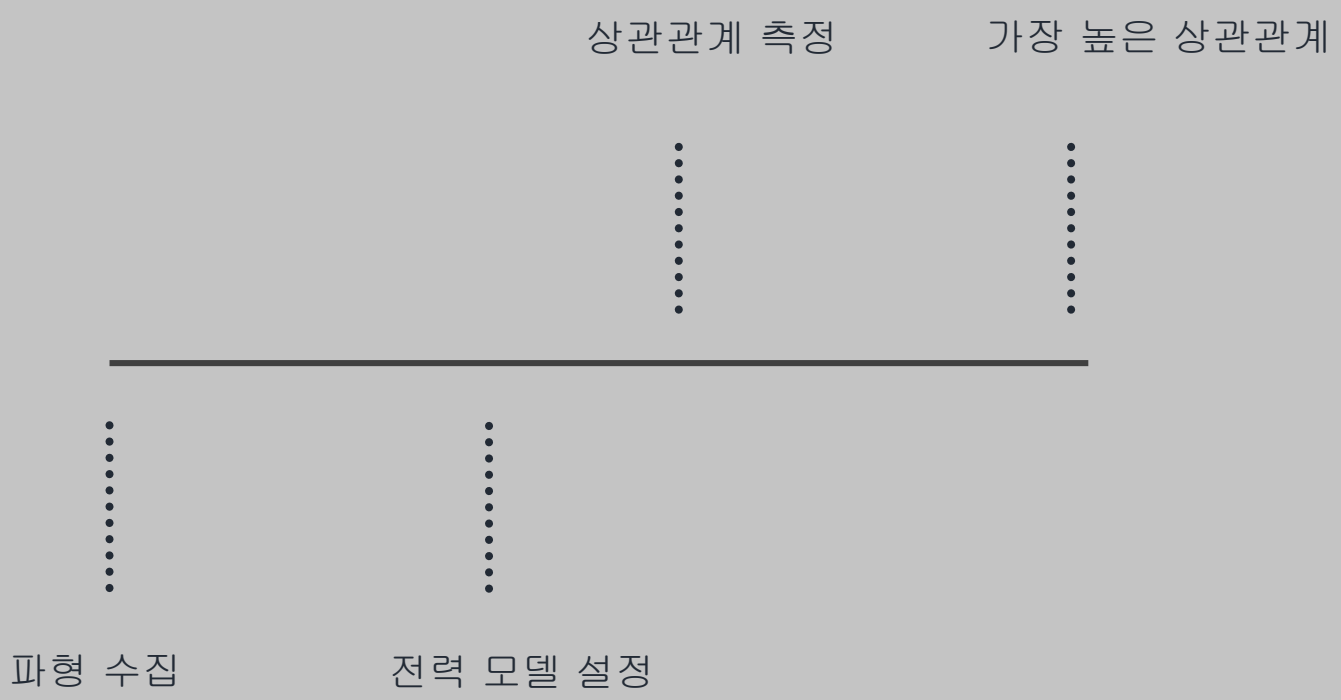
$D \neq 0$ -> Key

DPA

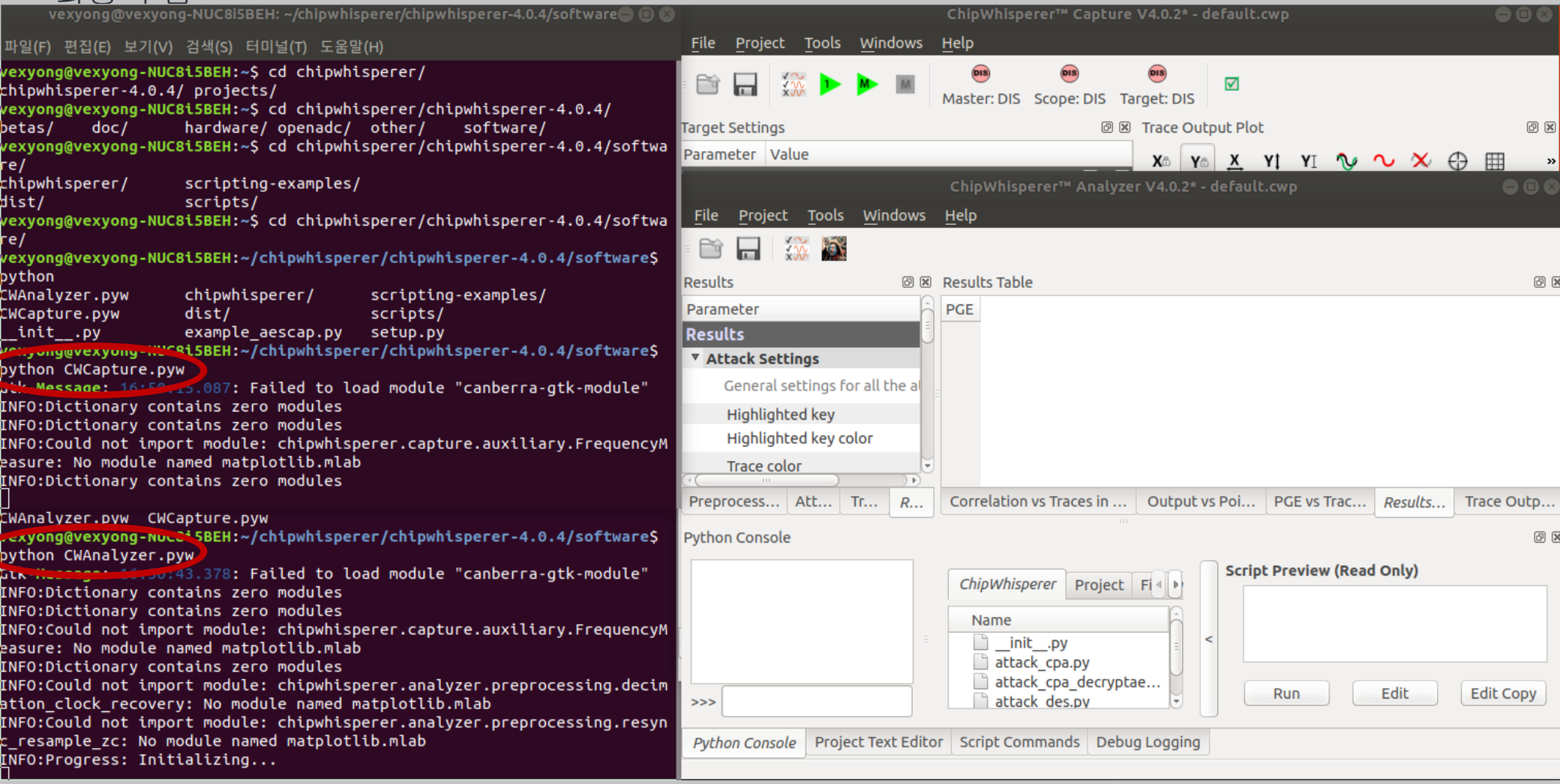
1. 올바른 수행 파형 수집
2. 중간값을 전력 모델로 변환한 값 수집
3. 분류함수를 통해 파형 그룹화
4. 평균값을 차분
5. 차분이 0이 아니라면 키

내용 ㅡ
전력분석

내용 ㅡ
전력분석

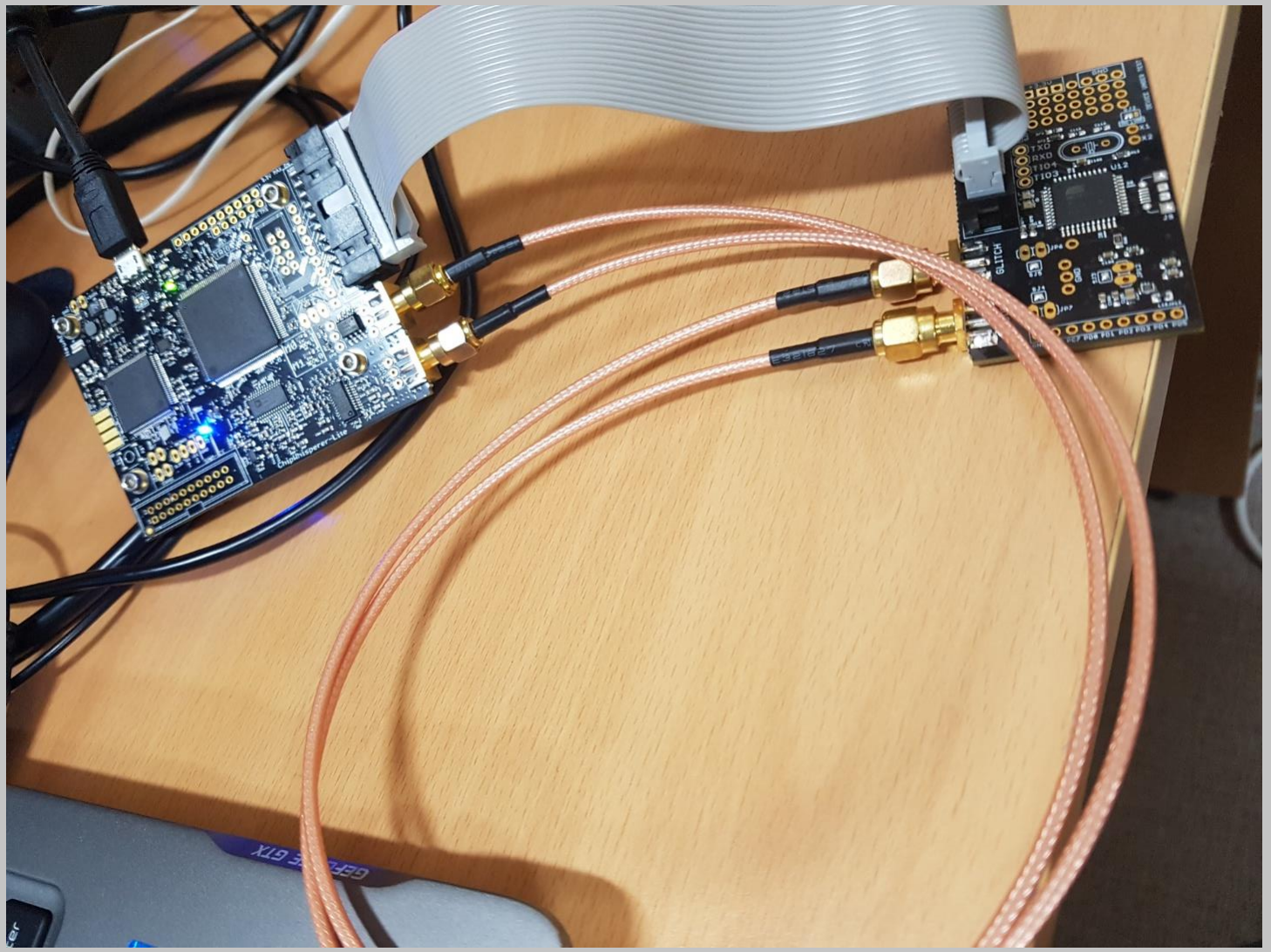


내용 ㅡ
CPA To AES
파형 수집



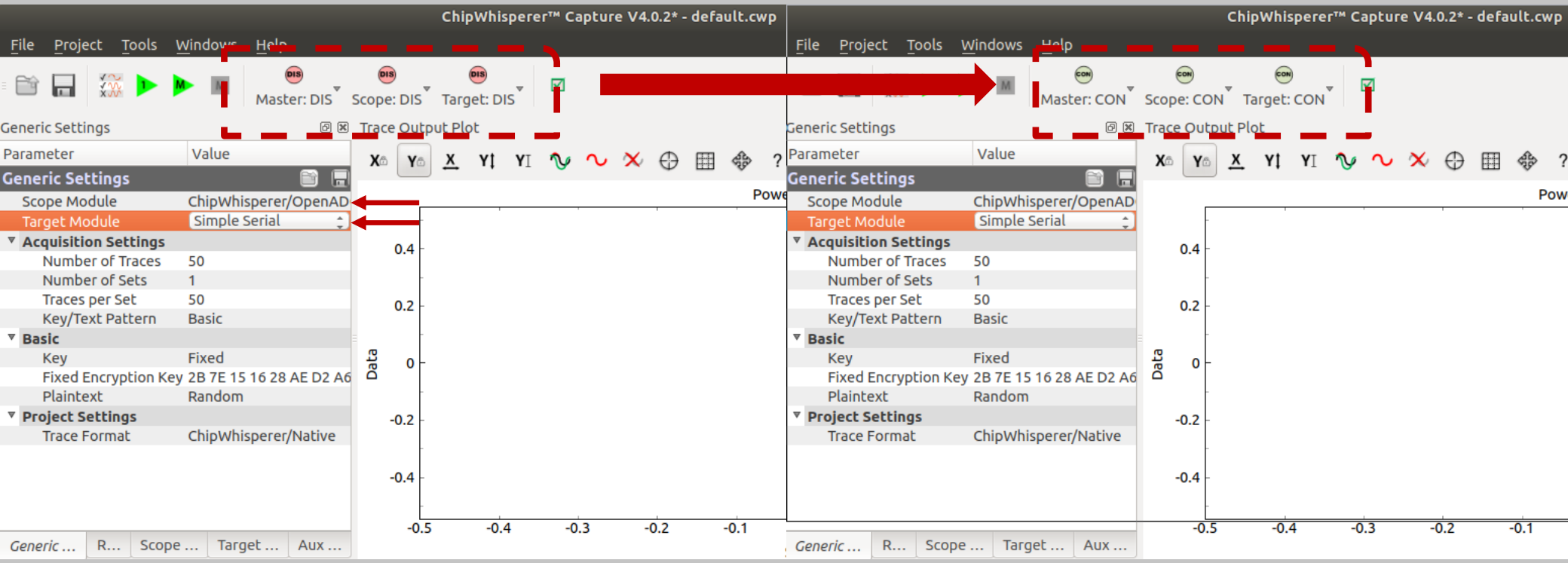
도구 준비 : 파형을 수집하는 CWCapture, 파형을 분석하는 CWAnalyzer

내용 ㅡ
CPA To AES
파형 수집



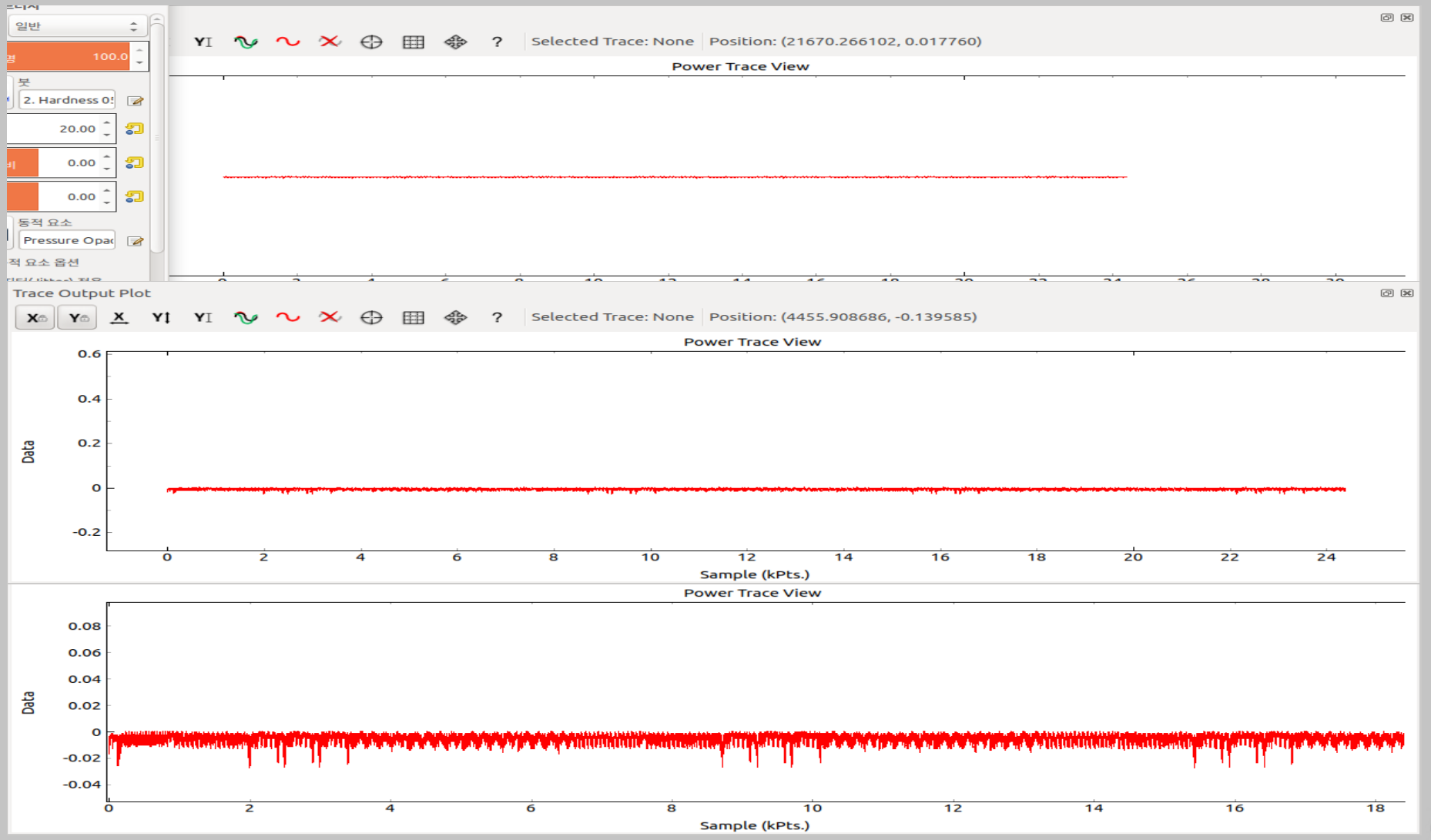
도구 준비 : 파형을 수집하는 OscilloScope, 암호가 구동되는 TargetBoard

내용 ㅡ
CPA To AES
파형 수집



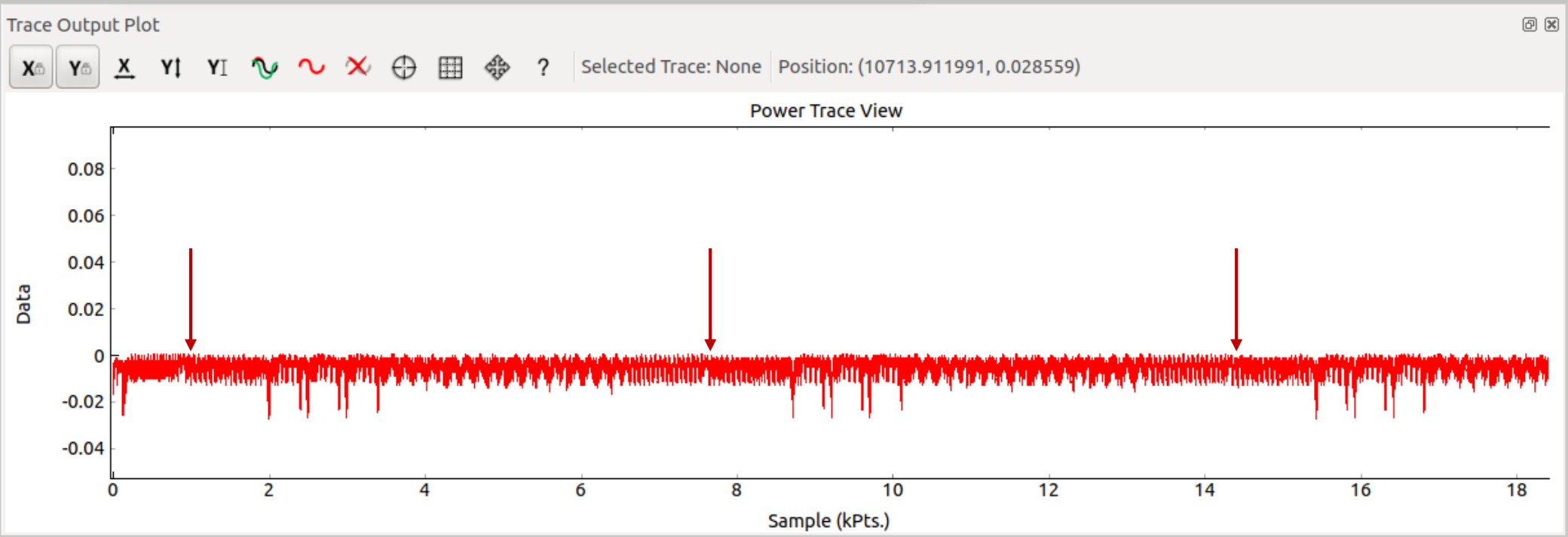
도구 연결 : 소프트웨어 도구들과 하드웨어 도구들을 연결

내용 ㅡ
CPA To AES
파형 수집



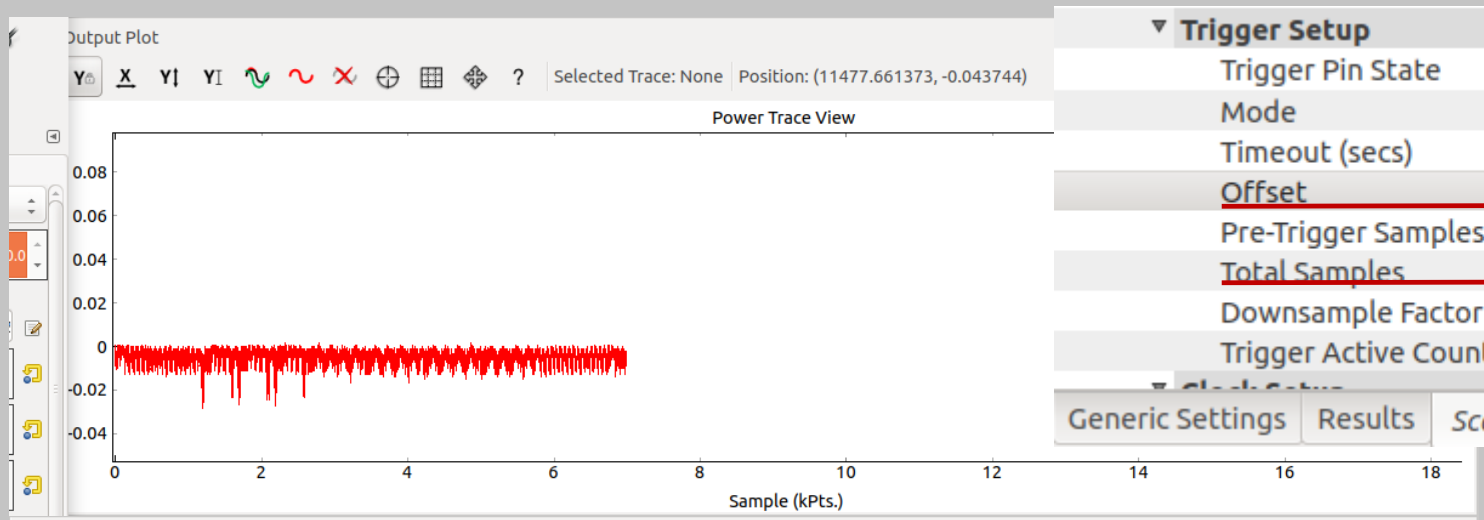
적합한 파형 측정 환경을 찾습니다.

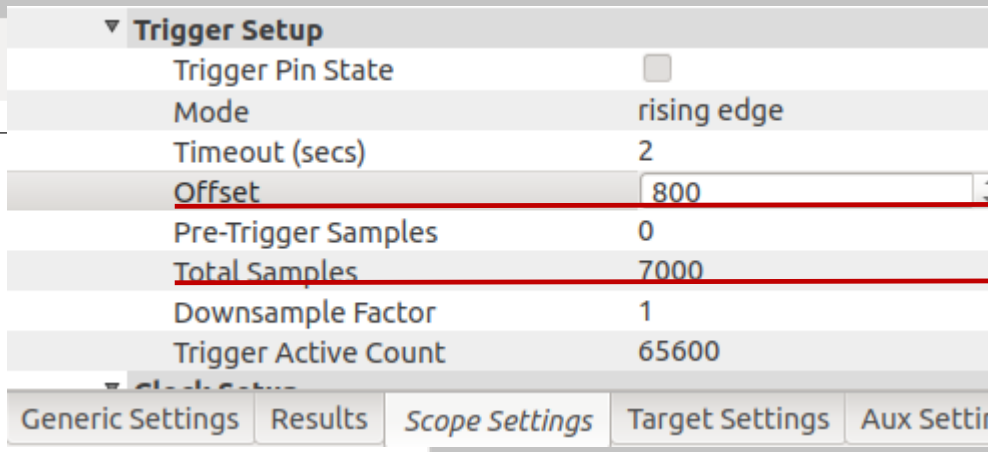
내용 ㅡ
CPA To AES
파형 수집

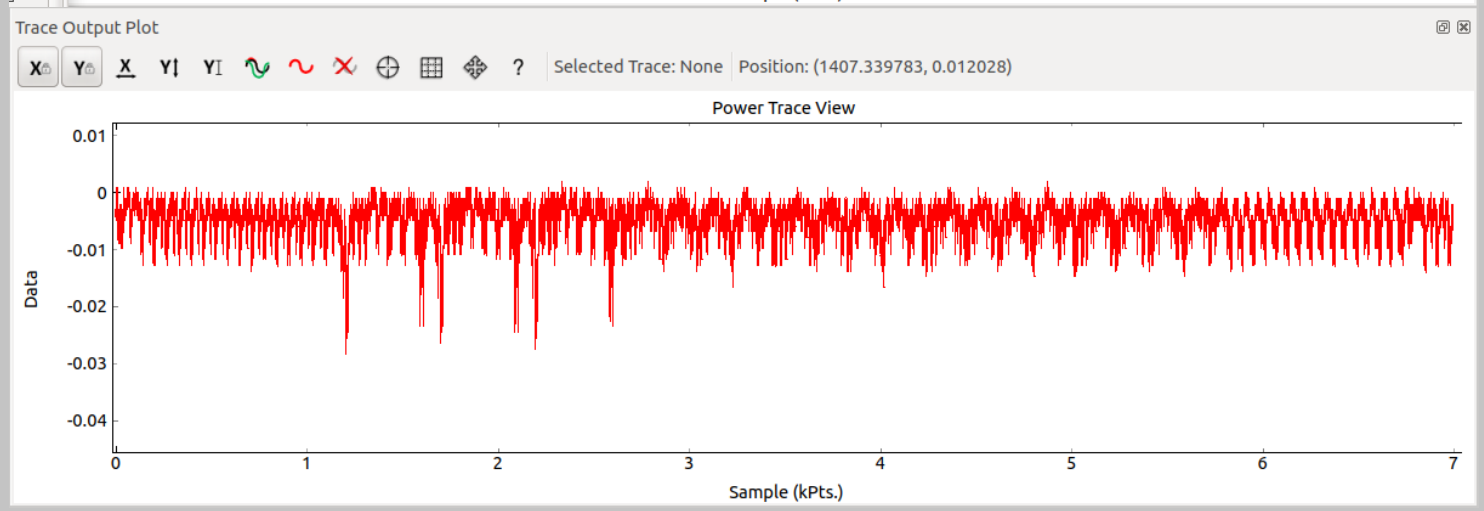


암호알고리즘이 동작하는 부분 찾기 800 ~ 7800

내용 ㅡ
CPA To AES
파형 수집



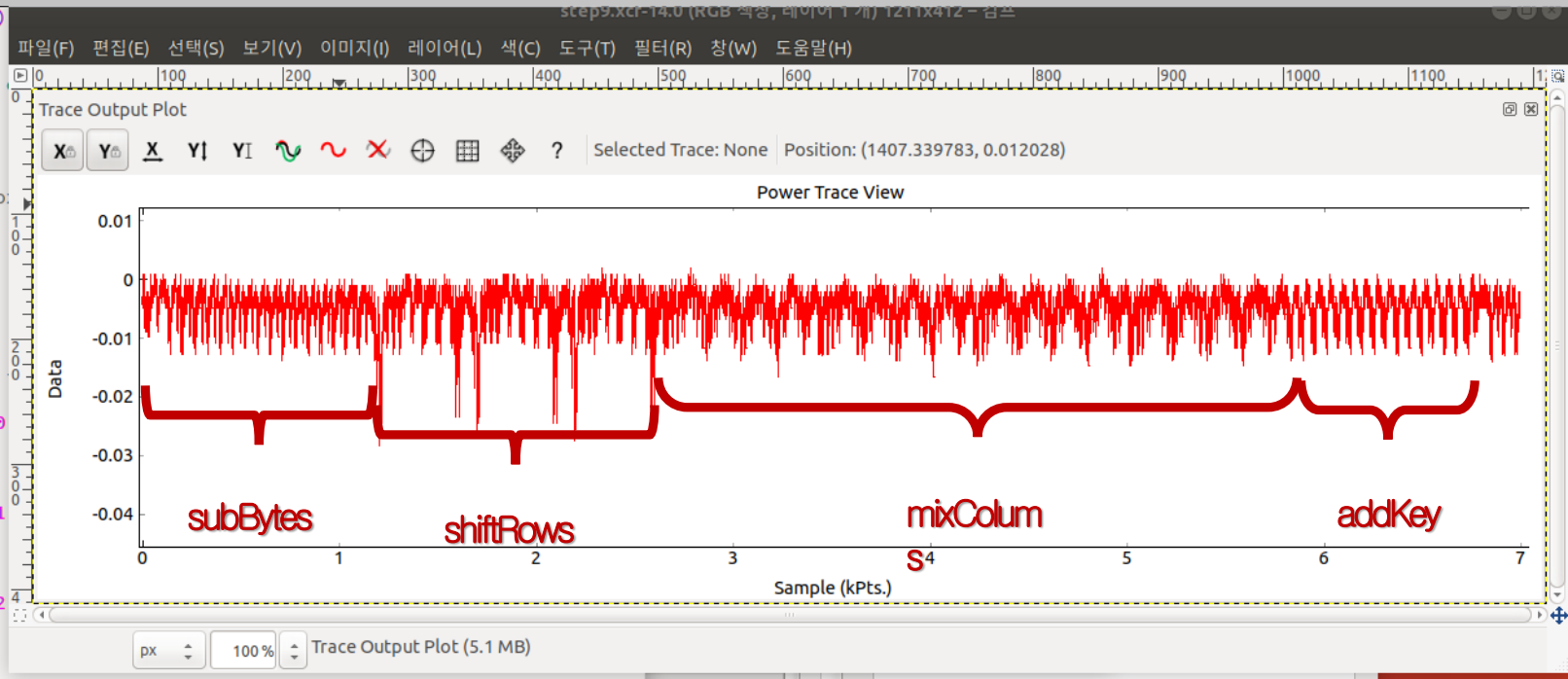




암호알고리즘이 동작하는 부분의 파형 수집
(이제 우리는 암호 알고리즘이 동작하는 지점의 파형을 수집합니다.)

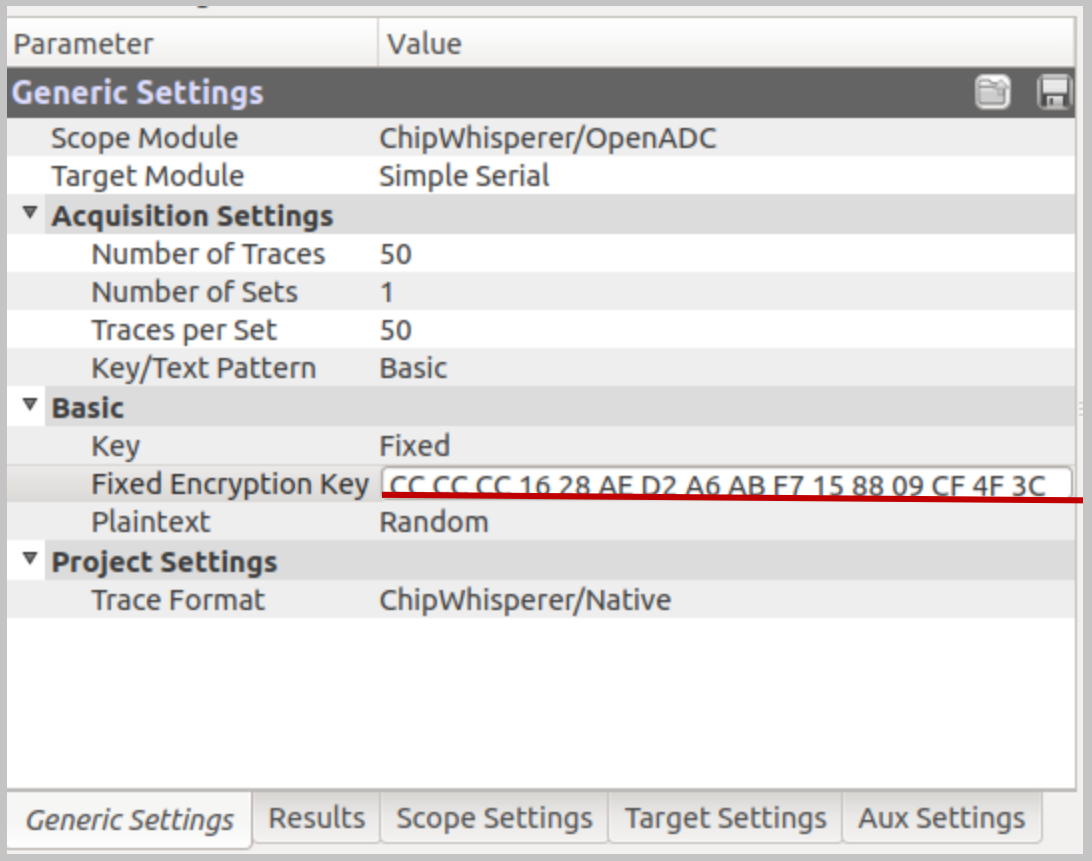
내용 ㅡ
CPA To AES
파형 수집

```
ne GF256MUL_3(a) (gf256mul(3, (a), 0x1b))

c
aes_enc_round(aes_cipher_state_t* state,
  uint8_t tmp[16], t;
  uint8_t i;
  /* subBytes */
  for(i=0; i<16; ++i){
          tmp[i] = pgm_read_byte(aes_sbo
  }
  /* shiftRows */
  aes_shiftcol(tmp+1, 1);
  aes_shiftcol(tmp+2, 2);
  aes_shiftcol(tmp+3, 3);
  /* mixColums */
  for(i=0; i<4; ++i){
          t = tmp[4*i+0] ^ tmp[4*i+1] ^
          state->s[4*i+0] =
                    GF256MUL_2(tmp[4*i+0
                  ^ tmp[4*i+0]
                  ^ t;
          state->s[4*i+1] =
                    GF256MUL_2(tmp[4*i+1
                  ^ tmp[4*i+1]
                  ^ t;
          state->s[4*i+2] =
                    GF256MUL_2(tmp[4*i+2
                  ^ tmp[4*i+2]
                  ^ t;
          state->s[4*i+3] =
                    GF256MUL_2(tmp[4*i+3]^tmp[4*i+0])
                  ^ tmp[4*i+3]
                  ^ t;
  }

  /* addKey */
  for(i=0; i<16; ++i){
          state->s[i] ^= k->ks[i];
  }
```



검사하기 (SPA)

내용 ㅡ
CPA To AES
파형 수집

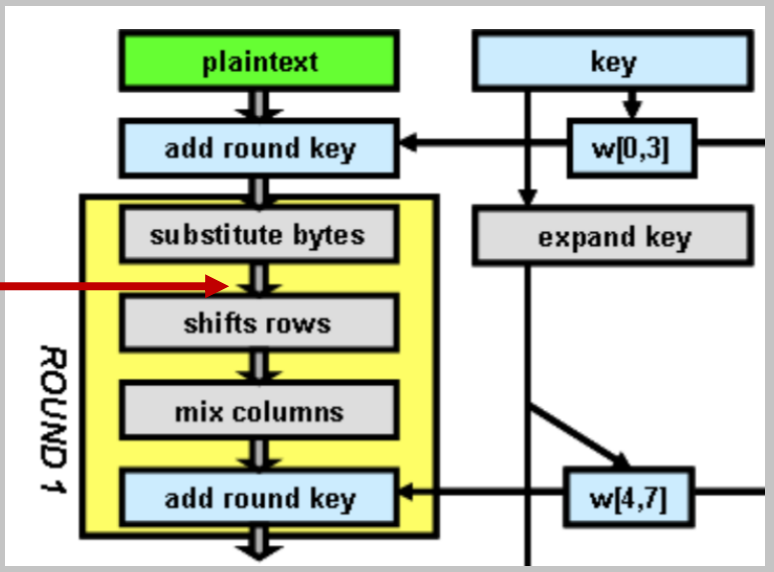


올바른 키를 이용하여 알고리즘을 50회 동작한 파형을 수집한다.

내용 ㅡ
CPA To AES
전력 모델 설정

```
leak_model = AES128_8bit(SBox_output)
```

```
class SBox_output(AESLeakageHelper):
    name = 'HW: AES SBox Output, First Round (Enc)'
    c_model_enum_value = 1
    c_model_enum_name = 'LEAK_HW_SBOXOUT_FIRSTROUND'
    def leakage(self, pt, ct, key, bnum):
        return self.sbox(pt[bnum] ^ key[bnum])
```



목표 : 첫 번째 S-box(substitute bytes) 이후 지점
해당 모델 : sbox(plaintxt XOR key)

내용 ㅡ
CPA To AES
상관관계 측정

$h_{d,i}$ = 모델링된 전력소모
$t_{d,j}$ = 측정한 파형

$r_{i,j}$ =둘 사이의 상관관계
With Pearson

$$\rho_{X,Y} = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y} = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sqrt{E[(X-\mu_X)^2]E[(Y-\mu_Y)^2]}}$$

$$r_{i,j} = \frac{D\sum_{d=1}^{D} h_{d,i}t_{d,j} - \sum_{d=1}^{D} h_{d,i} \sum_{d=1}^{D} t_{d,j}}{\sqrt{\left((\sum_{d=1}^{D} h_{d,i})^2 - D\sum_{d=1}^{D} h_{d,i}^2\right)\left((\sum_{d=1}^{D} t_{d,j})^2 - D\sum_{d=1}^{D} t_{d,j}^2\right)}}$$

```
sumnum = self.totalTraces * self.sumht[key] - self.sumh[key] * self.sumt
```

```
sumden2 = (np.square(self.sumt) - self.totalTraces * self.sumtq)
sumden1 = (np.square(self.sumh[key]) - self.totalTraces * self.sumhq[key])
sumden = sumden1 * sumden2
```

$r_{i,j}$

```
diffs[key] = sumnum / np.sqrt(sumden)
```

내용 ㅡ
CPA To AES
키 획득

50 traces try

Results Table

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	0	0	3	15	0	0	2	0	0	0	0	1	0	0	0
0	CC 0.7787	CC 0.6907	CC 0.6741	74 0.6720	7C 0.6508	AE 0.6779	D2 0.7389	25 0.6333	AB 0.7199	F7 0.7024	15 0.6891	88 0.6877	BD 0.6628	CF 0.7416	4F 0.7282	3C 0.6852
1	CD 0.6774	81 0.6150	F9 0.6253	38 0.6704	23 0.6478	C5 0.6536	D5 0.6529	D6 0.6297	CE 0.6650	BA 0.6669	96 0.6596	AF 0.6600	09 0.6613	F1 0.6418	7C 0.6268	2A 0.6404
2	17 0.6499	3B 0.6116	B8 0.6213	B6 0.6254	30 0.6453	79 0.6345	FA 0.6405	A6 0.6111	EF 0.6317	BD 0.6328	AE 0.6386	83 0.6456	78 0.6207	46 0.6354	B9 0.6206	14 0.6317
3	BB 0.6339	5A 0.6114	D9 0.6164	16 0.6232	1F 0.6138	A3 0.6250	CA 0.6330	F9 0.6081	FD 0.6197	43 0.6285	4F 0.6285	1E 0.6305	ED 0.6120	84 0.6353	4D 0.6204	1B 0.6309
4	32 0.6275	49 0.6112	B7 0.6114	36 0.6186	F3 0.6134	A9 0.6223	0D 0.6292	BF 0.6066	EE 0.6112	D8 0.6190	C3 0.6146	B6 0.6260	43 0.6103	70 0.6349	4E 0.6202	0A 0.6162
5	85 0.6259	22 0.6040	F0 0.6093	68 0.6183	27 0.5990	D0 0.6185	FD 0.6168	73 0.6047	7D 0.6105	57 0.6169	E4 0.6121	24 0.6225	5D 0.6018	8D 0.6289	87 0.6191	07 0.6039
6	2F 0.6250	20 0.6032	E5 0.6077	B0 0.6167	43 0.5916	6E 0.6107	DF 0.6144	92 0.6017	0C 0.6092	D6 0.6121	3D 0.6027	6C 0.6100	E4 0.5974	85 0.6242	B6 0.6120	DC 0.6029
7	A8 0.6213	25 0.5999	C0 0.6021	03 0.6103	25 0.5896	94 0.6102	78 0.6081	7C 0.5963	63 0.6087	46 0.6109	27 0.5992	29 0.6054	2E 0.5935	53 0.6080	CE 0.6113	A7 0.6013
8	06 0.6194	DD 0.5981	77 0.5972	4B 0.6083	2F 0.5868	FE 0.5967	BD 0.5990	57 0.5937	E7 0.6073	BE 0.6084	D9 0.5988	6E 0.6021	68 0.5892	E0 0.6078	B2 0.6024	F3 0.6005
9	35	8F	61	15	AD	29	13	87	E1	B6	13	E4	6A	72	AC	BE

FAILURE

내용 ㅡ
CPA To AES
키 획득

50 more traces try

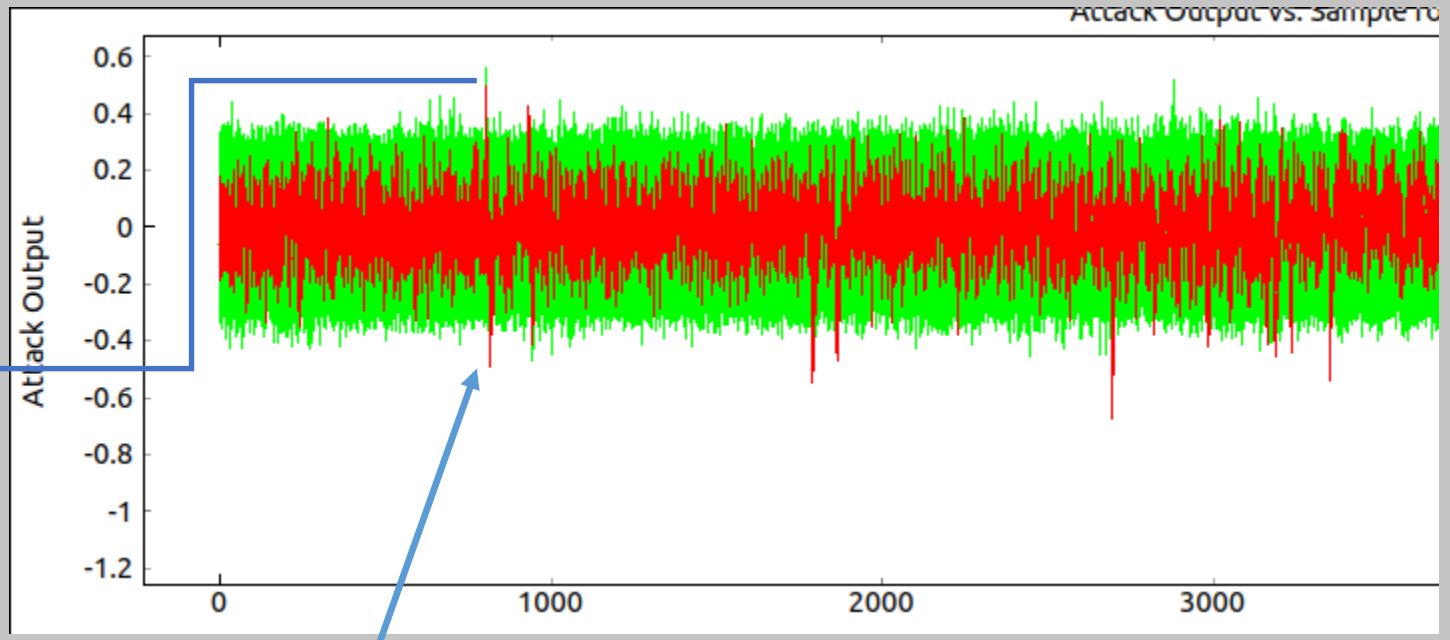
Results Table

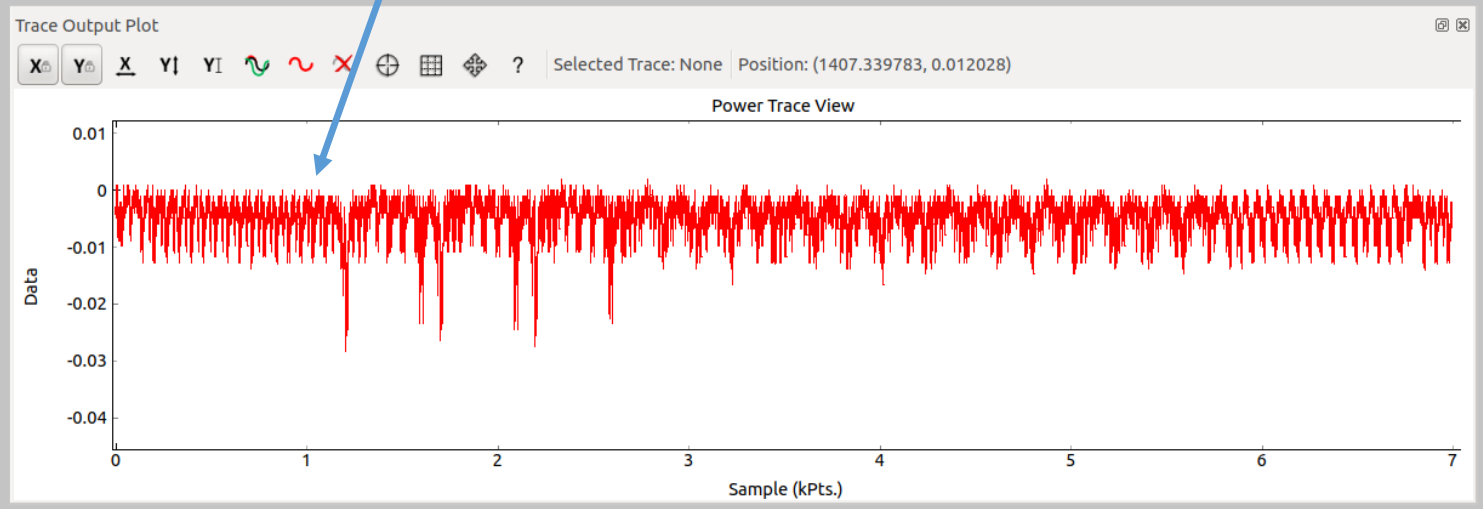
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	CC 0.6967	CC 0.6610	CC 0.6122	16 0.5490	28 0.5622	AE 0.6157	D2 0.6516	A6 0.5687	AB 0.6269	F7 0.6465	15 0.6753	88 0.6484	09 0.6100	CF 0.6803	4F 0.6191	3C 0.6415
1	D5 0.4826	61 0.4683	CD 0.5502	6D 0.4928	86 0.4763	08 0.4834	F2 0.4719	AA 0.4905	83 0.4916	F9 0.4962	14 0.5578	89 0.4939	3E 0.4701	46 0.5081	8C 0.4670	3D 0.4993
2	69 0.4650	08 0.4596	03 0.4496	73 0.4830	9E 0.4762	2F 0.4500	74 0.4577	07 0.4607	95 0.4676	BD 0.4783	96 0.5165	BC 0.4750	FE 0.4615	CE 0.5052	B5 0.4487	28 0.4914
3	5A 0.4598	26 0.4572	7E 0.4496	17 0.4780	26 0.4740	F5 0.4469	D3 0.4541	92 0.4596	57 0.4620	B8 0.4709	6E 0.4673	22 0.4539	76 0.4596	F6 0.4673	19 0.4481	E0 0.4810
4	49 0.4480	5B 0.4543	B2 0.4491	52 0.4775	43 0.4623	70 0.4450	75 0.4480	96 0.4577	08 0.4566	D2 0.4544	69 0.4643	9E 0.4466	08 0.4547	24 0.4651	C3 0.4449	7F 0.4754
5	D1 0.4454	65 0.4537	A5 0.4451	1C 0.4601	AB 0.4486	AF 0.4427	9C 0.4462	3E 0.4507	E7 0.4555	79 0.4533	17 0.4587	71 0.4454	F1 0.4485	3E 0.4572	34 0.4414	24 0.4691
6	CE 0.4419	81 0.4506	FB 0.4420	61 0.4572	AD 0.4485	89 0.4398	AA 0.4458	D5 0.4485	AF 0.4477	16 0.4526	FB 0.4552	07 0.4380	50 0.4468	49 0.4558	5F 0.4410	6E 0.4551
7	4F 0.4405	D5 0.4497	66 0.4390	BF 0.4508	5E 0.4469	A5 0.4391	8D 0.4440	E5 0.4474	7E 0.4437	B9 0.4460	E6 0.4532	BF 0.4364	43 0.4423	9C 0.4514	15 0.4409	80 0.4550
8	0F 0.4394	C2 0.4472	42 0.4388	FC 0.4508	F6 0.4434	5B 0.4353	21 0.4403	E4 0.4473	0C 0.4433	C3 0.4450	5A 0.4480	EA 0.4338	23 0.4379	DB 0.4467	CB 0.4407	A9 0.4496
9	EB	A5	85	51	5A	F9	67	DF	61	9D	2B	86	12	FE	E2	EF

SUCCESS

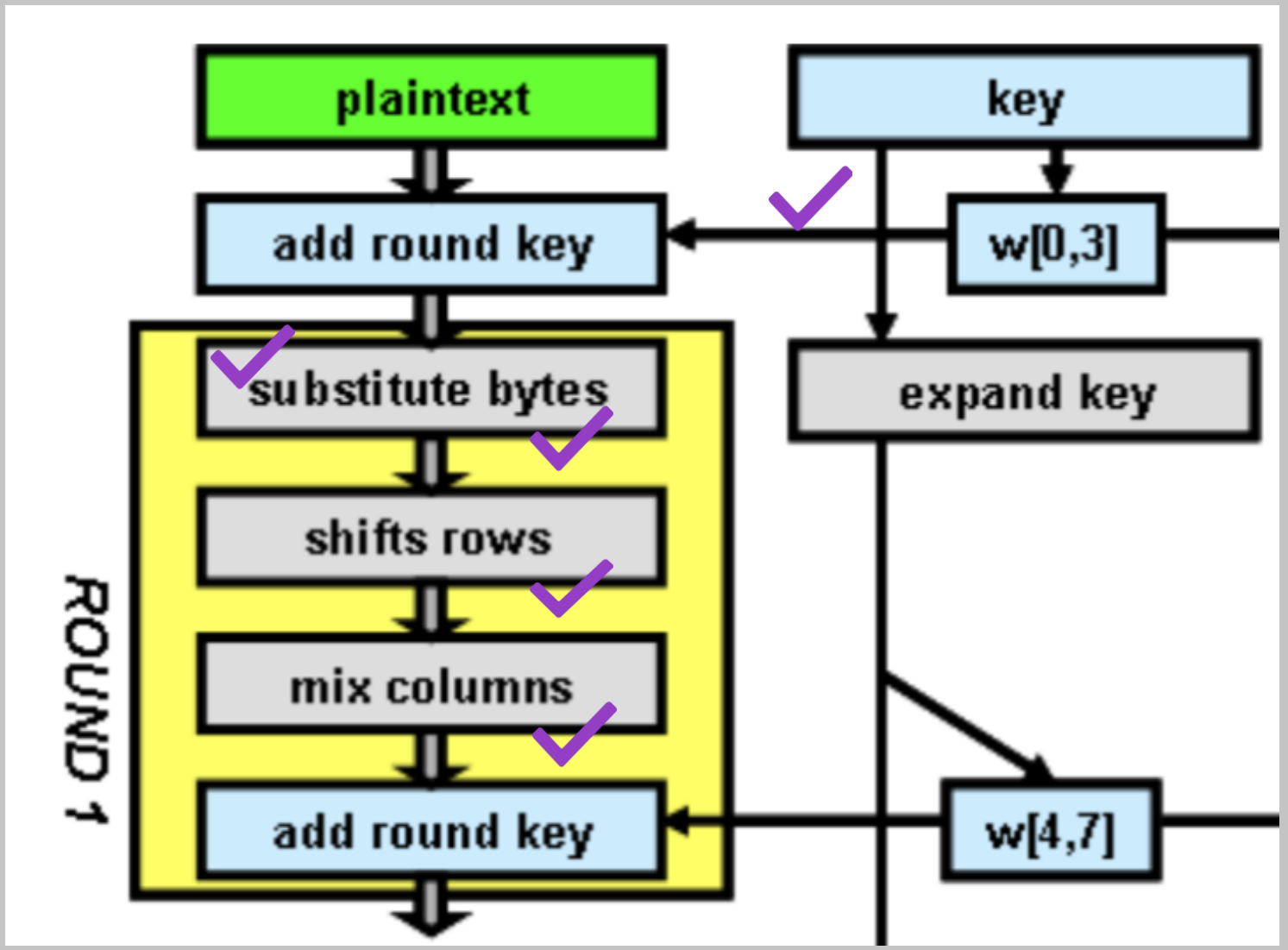
내용 ㅡ
CPA To AES
키 획득

High
Peak





내용 ㅡ
앞으로..


plaintext
key
add round key
w[0,3]
substitute bytes
expand key
shifts rows
mix columns
add round key
w[4,7]
ROUND 1

내용 ㅡ
앞으로..

01 위의 대응 기법 적용

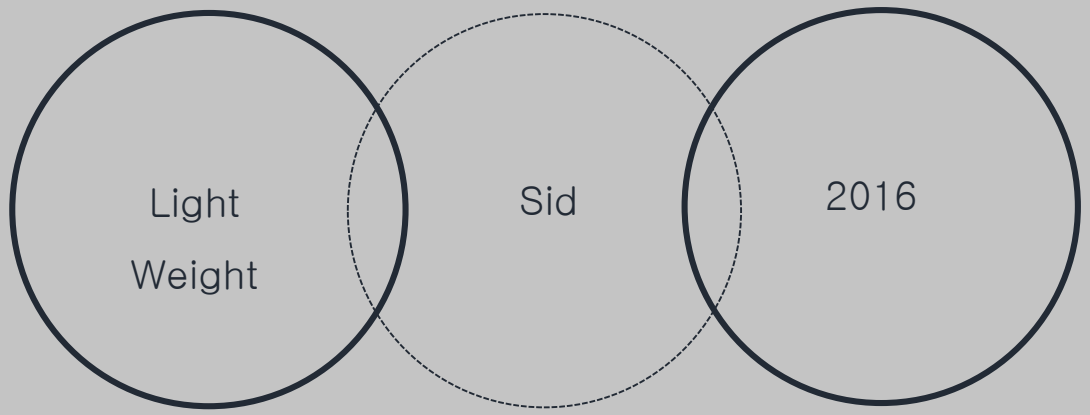
02 경량 블록 암호 알고리즘 CHAM 분석

03 부채널분석과 그에 대한 대응기법 적용, 효율 확인

읽어주셔서
감사합니다

고맙습니다

내용 ㅡ
전력분석



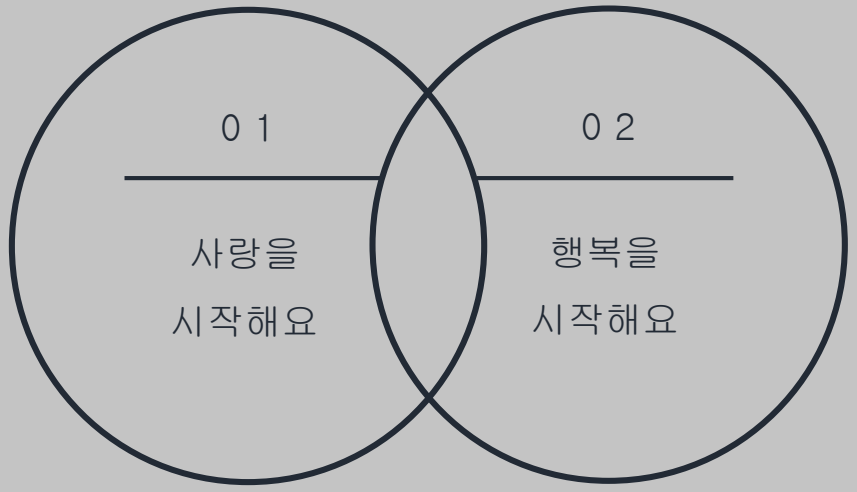
내용 ㅡ

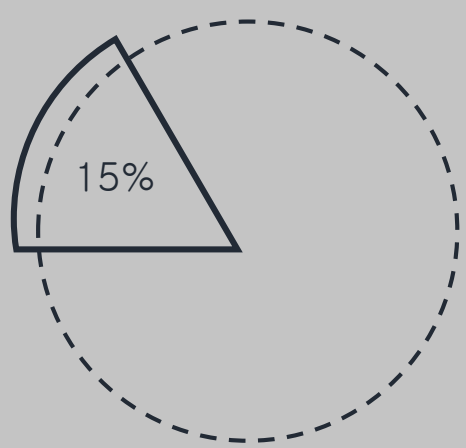
01

사랑을
시작해요

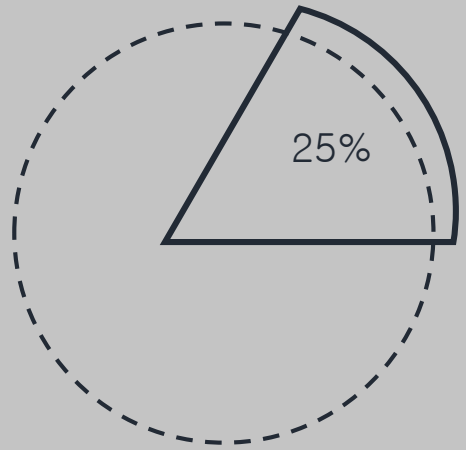
02

행복을
시작해요


0 1
사랑을
시작해요
0 2
행복을
시작해요


15%

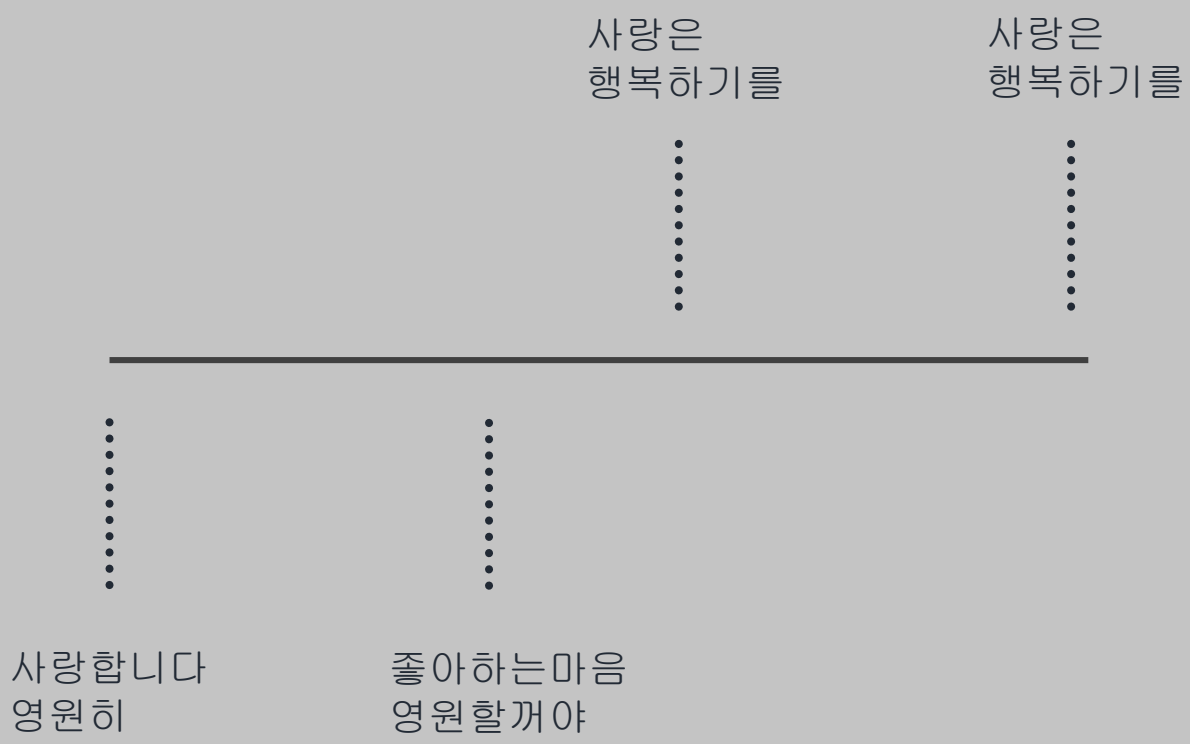

35%


25%


사랑이
간다


사랑이
간다

내용 ㅡ



내용 ㅡ

내용 ㅡ

01 나는 오늘도 유쾌하다고
말을하고 싶었다
이유는 모르겠다
그런데 졸립다

02 왕별이는 어느내용
적을까 항상 고민이
설레인다 음 어려워
그렇지 어려워

03 오늘은 좀 컬러감이
특이해서 맘에드는데
여러분들도
괜찮나요 홍홍

04 항상 사랑해주셔서
감사합니다
여러가지로 발전하려고
노력하는중

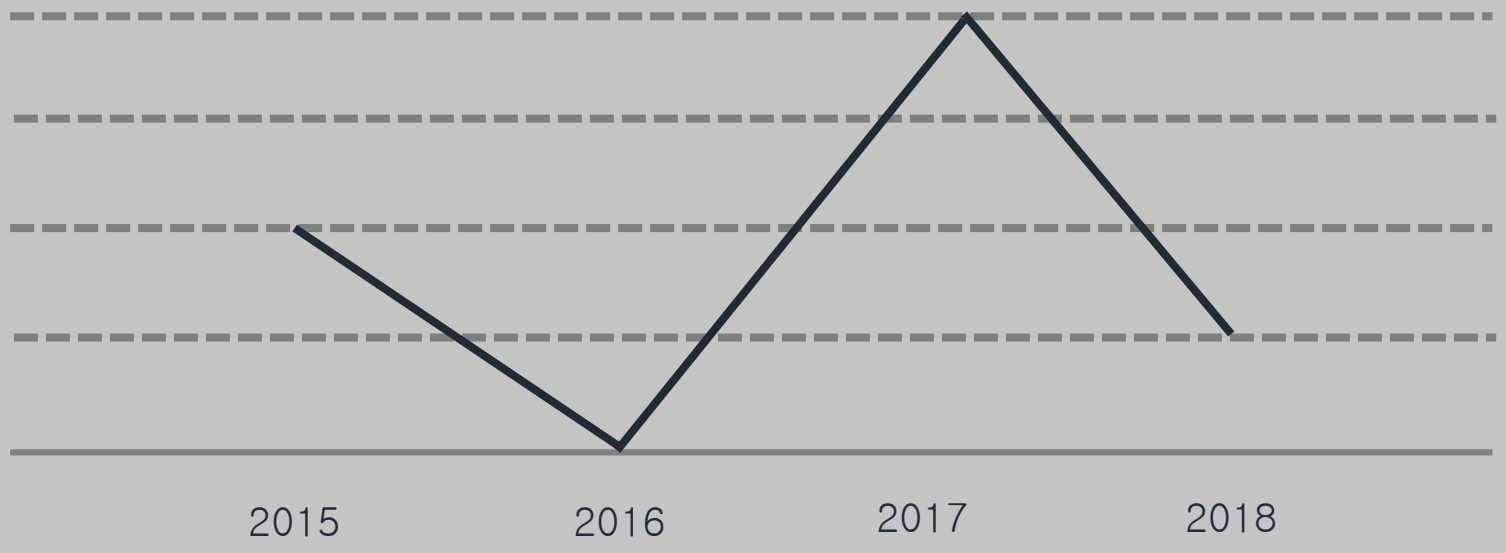
내용 ㅡ

01 긴 기다림에 끝에 당신이 오겠지요 네 오세요
이 내용은 길게 적을수 있게 만든것입니다
그러니 잘 사용해주시면 감사하겠습니다

02 긴 기다림에 끝에 당신이 오겠지요 네 오세요
이 내용은 길게 적을수 있게 만든것입니다
그러니 잘 사용해주시면 감사하겠습니다

03 긴 기다림에 끝에 당신이 오겠지요 네 오세요
이 내용은 길게 적을수 있게 만든것입니다
그러니 잘 사용해주시면 감사하겠습니다

내용



내용

내용 ㅡ

왕별입니다 오늘도 너무나
과제와 회사발표로 힘드실것같은
여러분들을 위해서 만들었습니다
전문적이고 깔끔한 스타일을

만들었기 때문에 필요하게 잘 사
용
해주셨으면 좋겠습니다.
저는 여백을 좋아하기 때문에
그렇게 잘 사용해주십시오.

내용 ㅡ

왕별입니다 오늘도 너무나
과제와 회사발표로 힘드실것같은
여러분들을 위해서 만들었습니다
전문적이고 깔끔한 스타일을

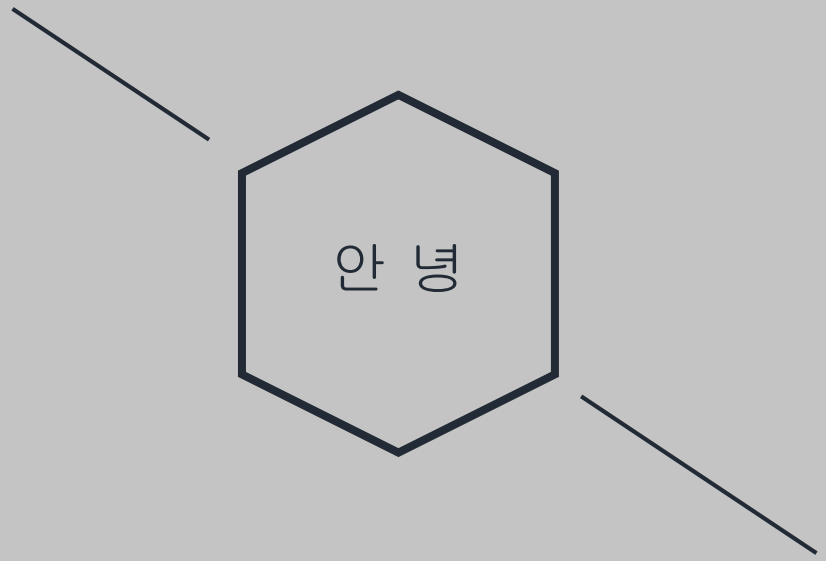
만들었기 때문에 필요하게 잘 사
용
해주셨으면 좋겠습니다.
저는 여백을 좋아하기 때문에
그렇게 잘 사용해주십시오.

내용 ㅡ

블로그
행복해라

희망을
품어본다

희망을
품어본다



여러분들을 위해서 만들었습니다
전문적이고 깔끔한 스타일을

왕별입니다 오늘도 너무나
과제와 회사발표로 힘드실것같은

읽어주셔서
감사합니다

김왕별 비행이
누구나 적어요