8/7/2019

**False negative experiment**

Bootstrapping Experiment on the false negative case:

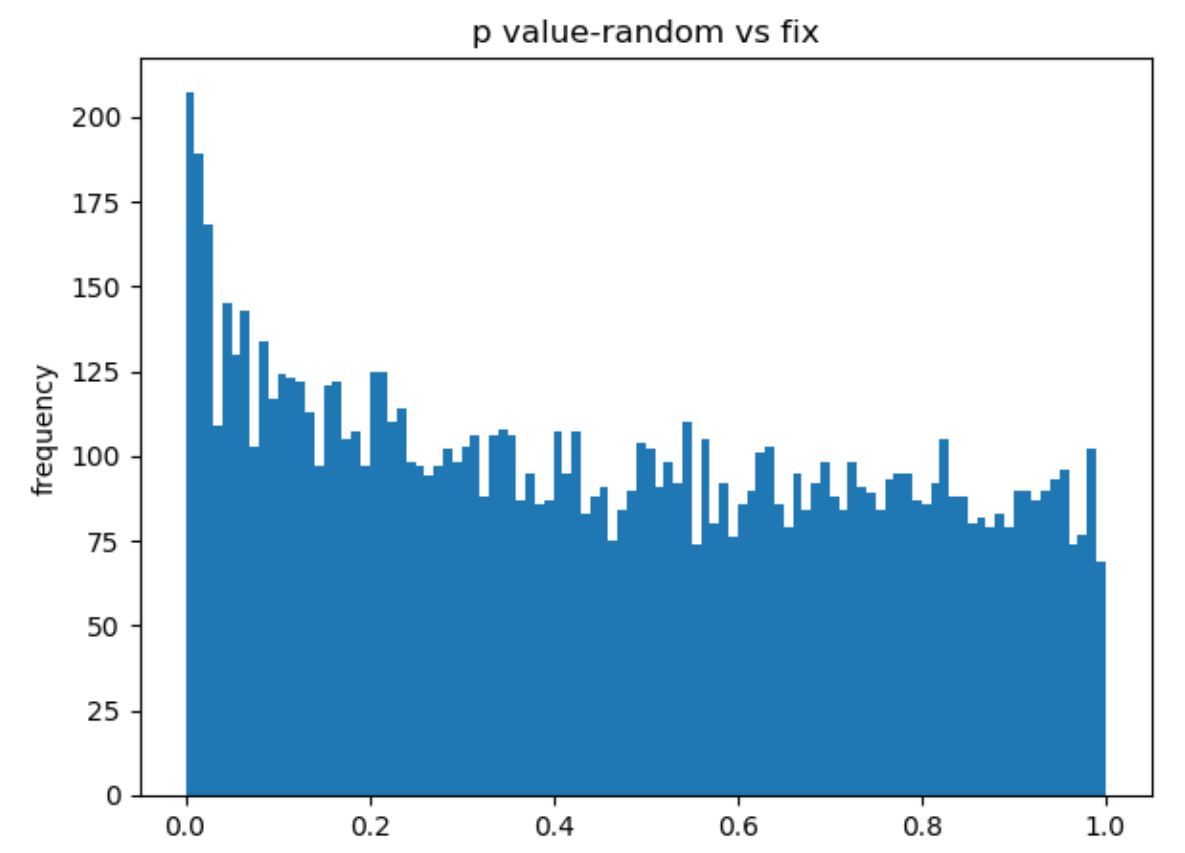
**Case1:**

(1) Parameters:

Bootnum: 10000 Traces: 1000 Fix\_value: 5 SNR:0.0001

obsv rand vs fix-t:-0.488886265183 p:0.6250295276

obsv rand vs rand-t:0.372845713999 p:0.709303098945



Comparison with the uniform distribution

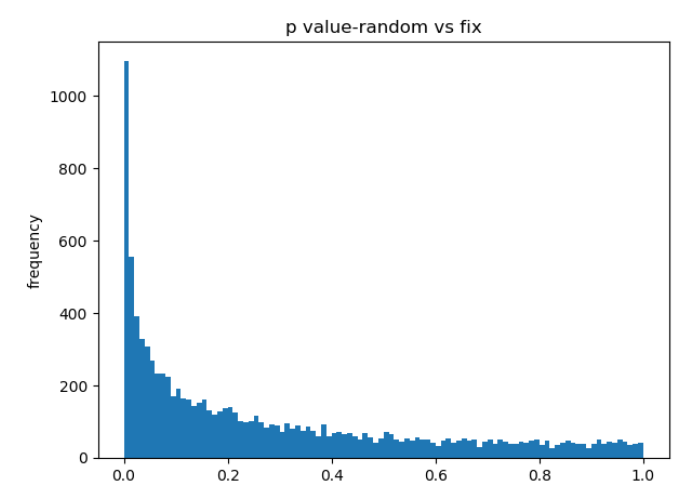
p\_ks:8.85876096521e-22

**Case2:**

(1) Parameters:

Bootnum: 10000 Traces: 1000 Fix\_value: 5 SNR:0.001

obsv rand vs fix-t:1.35005743038 p:0.177303356346

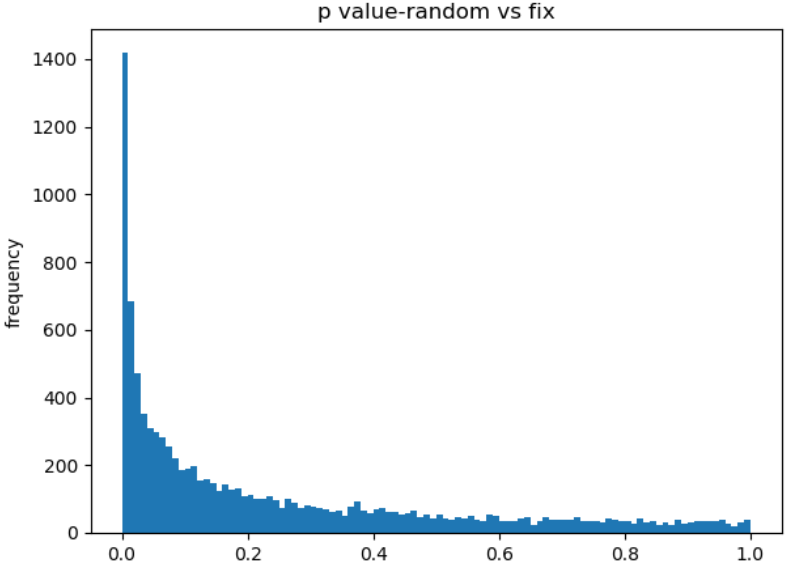


**p\_ks:9.88131291682e-324**

**Case2:**

(1) Parameters:

Bootnum: 10000 Traces: 1000 Fix\_value: 5 SNR:0.01

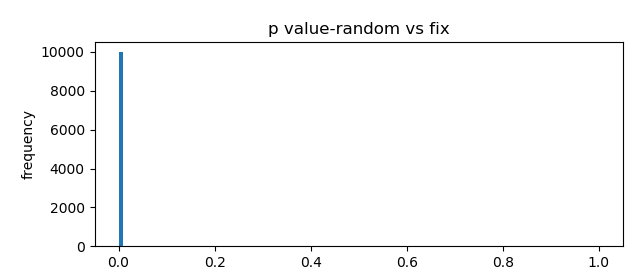


p\_ks:9.88131291682e-324

**Case3:**

(1) Parameters:

Bootnum: 10000 Traces: 1000 Fix\_value: 5 SNR:0.1



**p\_ks:9.88131291682e-324**

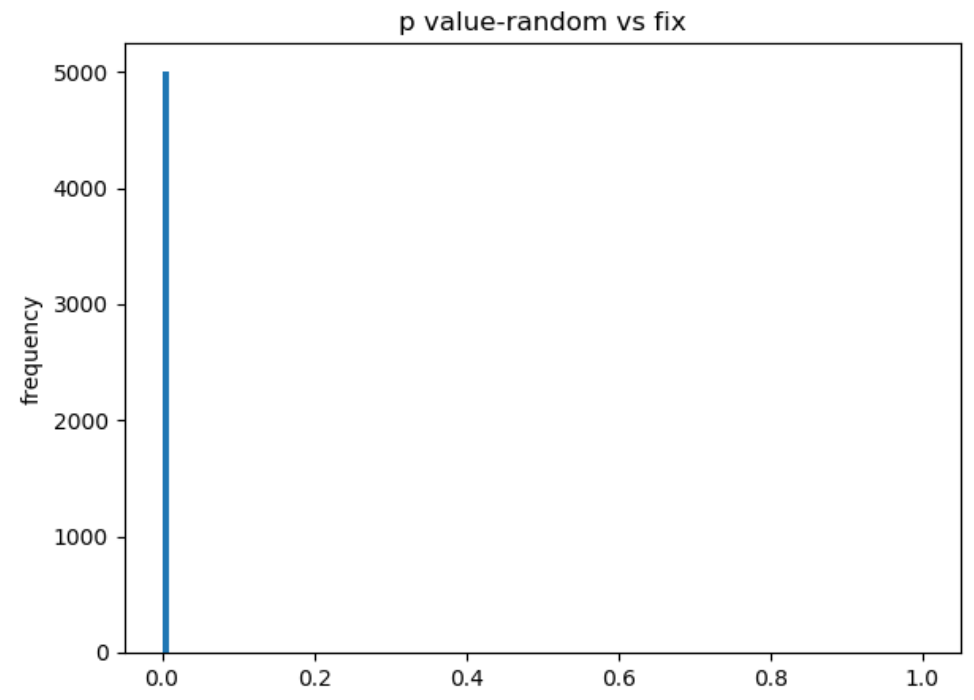
**Case4:**

(1) Parameters:

Bootnum:5000 Traces: 1000 Fix\_value: 5 SNR:0.1

obsv rand vs fix-t:6.8019422624 p:1.77498413636e-11

p\_ks:9.88131291682e-324

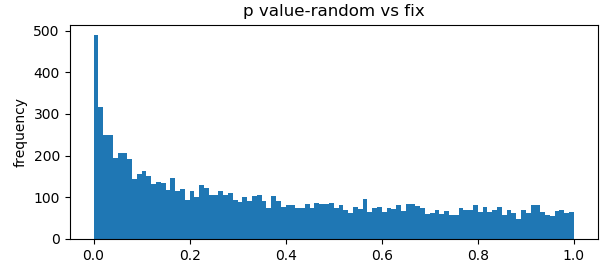


**Number of boots influence on the false negative identification:**

In the folder: Z:\simulation-trace\useful\_result\false\_negative\bootnum

**Case1:**

Parameter: Bootnum:10000 Tracenum: 1000 Fix value: 5 SNR: 0.001

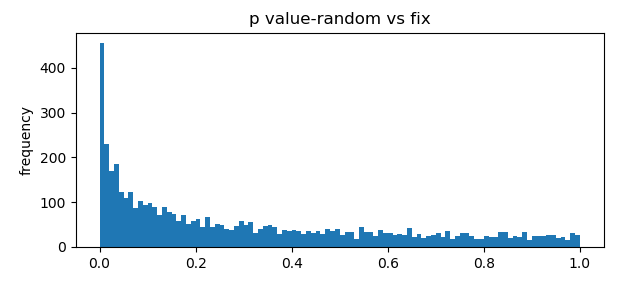


**p\_ks:2.05812107252e-149**

**p\_t:4.57170991485e-177**

**Case2:**

Parameter: Bootnum:5000 Tracenum: 1000 Fix value: 5 SNR: 0.001



obsv rand vs fix-t:1.19524049846 p:0.232276736032

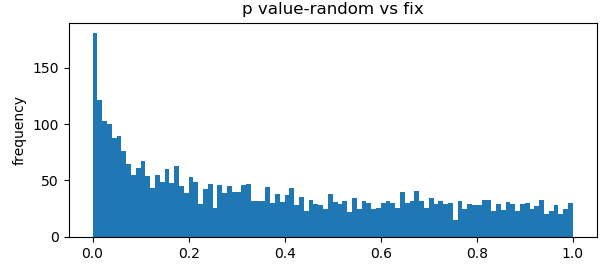
p\_ks:3.66161956374e-180

p\_t:5.59790262272e-209

**Case3:**

Parameter: bootnum: 4000 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



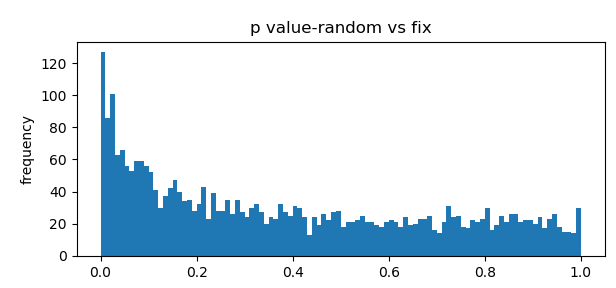
p\_ks:2.76199637855e-49

p\_t:2.2257995978e-55

**Case4:**

Parameter: bootnum: 3000 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



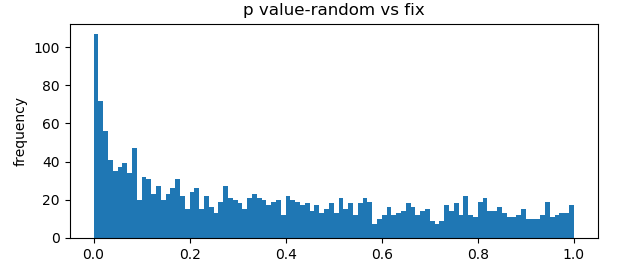
p\_ks:2.79530919292e-42

p\_t:1.92079178417e-45

Case2:

Parameter: bootnum: 2000 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908

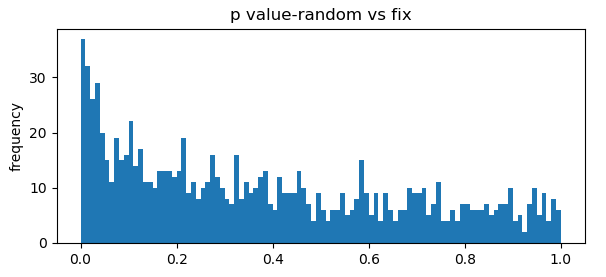


**p\_ks:2.90980931714e-29**

**p\_t:1.23889598505e-32**

**Case2:**

Parameter: bootnum: 1000 Tracenum: 1000 Fix value: 5 SNR: 0.001



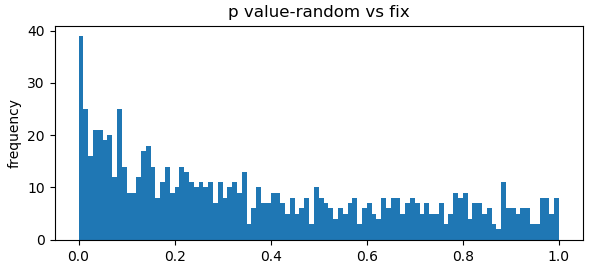
obsv rand vs fix-t:0.912542315826 p:0.361703464908

p\_ks:1.07637280113e-23

p\_t:5.67028334132e-29

Case2:

Parameter: bootnum: 900 Tracenum: 1000 Fix value: 5 SNR: 0.001



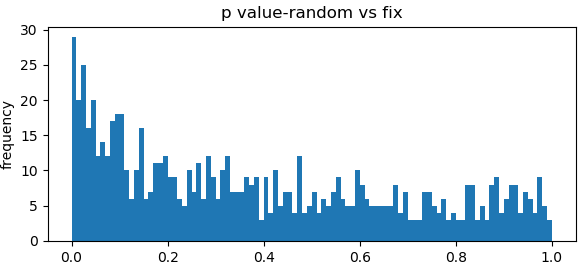
obsv rand vs fix-t:0.912542315826 p:0.361703464908

p\_ks:2.01879786488e-16

p\_t:2.1461190642e-15

Case2:

Parameter: bootnum: 800 Tracenum: 1000 Fix value: 5 SNR: 0.001



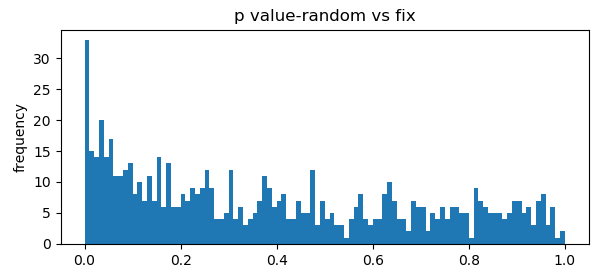
obsv rand vs fix-t:0.912542315826 p:0.361703464908

p\_ks:6.79979943396e-11

p\_t:2.77282171659e-13

Case2:

Parameter: bootnum: 700 Tracenum: 1000 Fix value: 5 SNR: 0.001



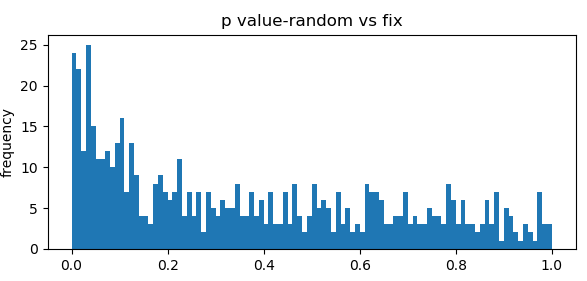
p\_ks:9.26257861141e-08

p\_t:1.48375040553e-09

Case2:

Parameter: bootnum: 600 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



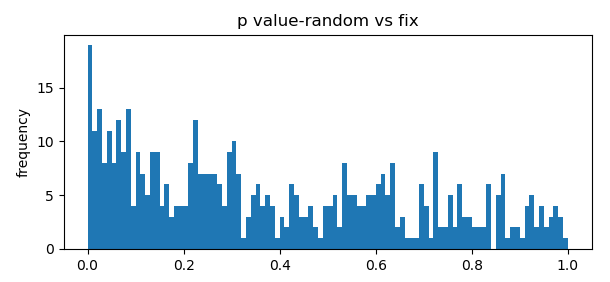
p\_ks:1.59961604383e-08

p\_t:2.4528806709e-10

Case2:

Parameter: bootnum: 500 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



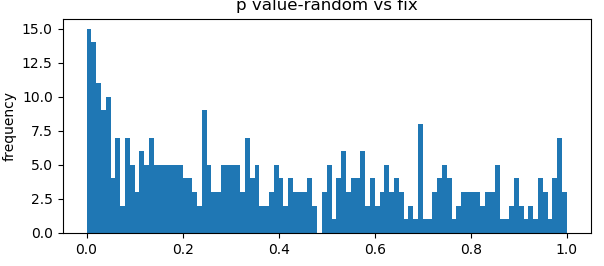
p\_ks:2.98603050634e-09

p\_t:1.73813189146e-08

Case2:

Parameter: bootnum: 400 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



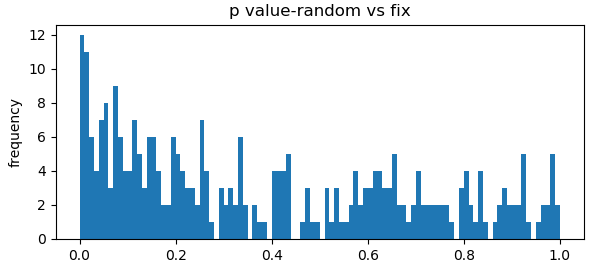
p\_ks:1.0914598327e-05

p\_t:6.12620908971e-07

Case2:

Parameter: bootnum: 400 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



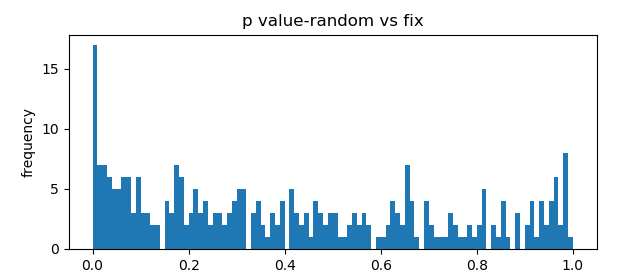
p\_ks:0.000140761917517

p\_t:0.000131605864041

Case2:

Parameter: bootnum: 300 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



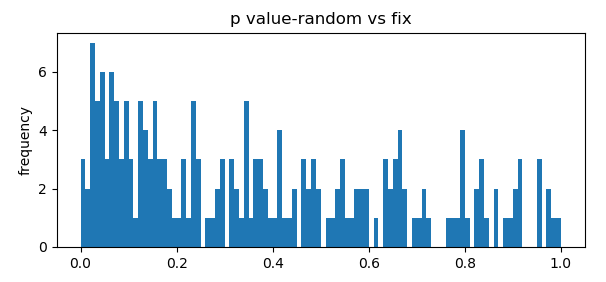
p\_ks:0.00148917968856

p\_t:0.00492803250096

Case2:

Parameter: bootnum: 200 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



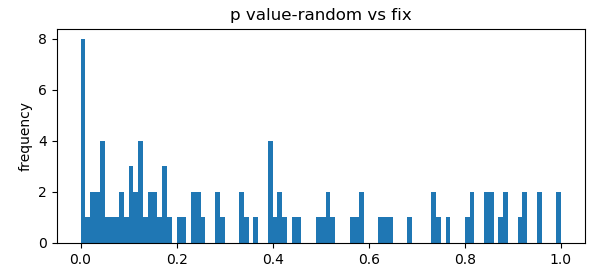
p\_ks:0.0104424546443

p\_t:0.00119074767392

Case2:

Parameter: bootnum: 100 Tracenum: 1000 Fix value: 5 SNR: 0.001

obsv rand vs fix-t:0.912542315826 p:0.361703464908



p\_ks:0.00303124516675

p\_t:0.00311906487789

**False positive experiment**

Look into the variance of the t-value:

**case1:**

obsv rand vs rand-t:5.64302806446 p:1.90924791203e-08

t\_value variance:1.00768807896

boot average:5.59439235376

**case2**:

obsv rand vs rand-t:4.57161882505 p:5.13600132717e-06

t\_value variance:0.984055225375

boot average:4.56111556214

**case3:**

obsv rand vs rand-t:-4.87921913284 p:1.14938738474e-06

t\_value variance:1.00854475588

boot average:4.91337386539

**case4:**

obsv rand vs rand-t:5.28109226026 p:1.42392121547e-07

t\_value variance:1.02918773345

boot average:5.30598073151

**True Positive case:**

obsv rand vs rand-t:-22.4054219976 p:2.0864524912e-90

t\_value variance:1.26937603218

boot average:22.4160419527

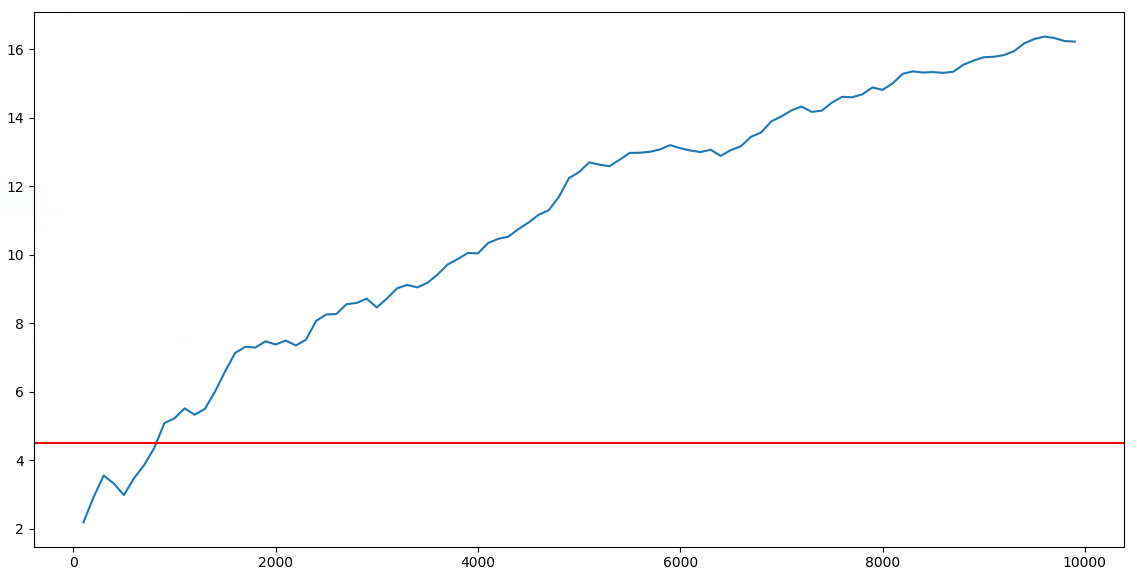
**Bootstrapping the number of traces:**

For the trace set:

fix\_noise\_10k.txt

rand\_noise\_10k.txt

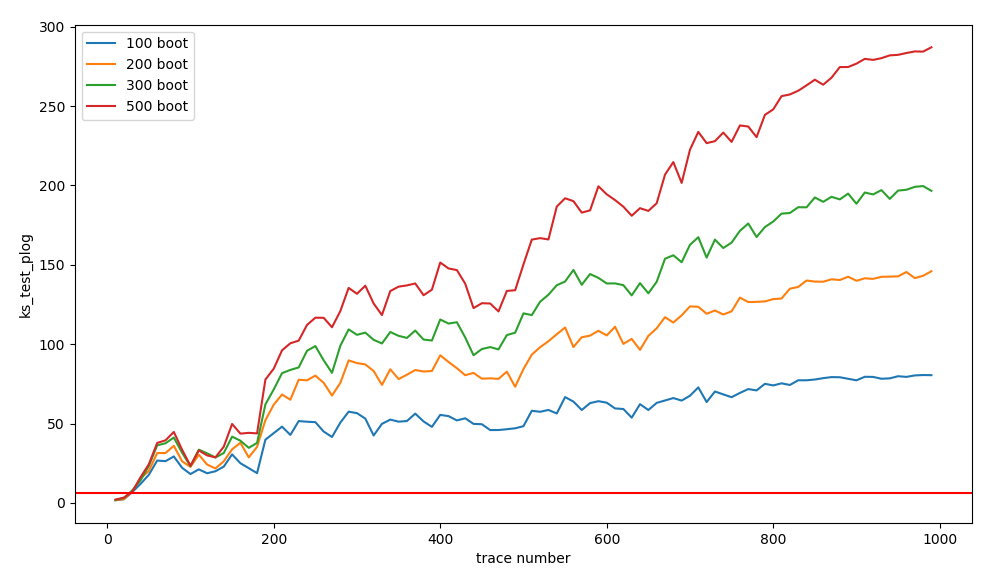
Read in the traces and read



The point which pass the threshold is: 819

As we can see, we will not be able to detect leakage within 800 traces.

Within the 800 traces, we do boot strapping on different number of traces, and use the distribution of the bootstrapping p\_value to predict the side channel leakage. When the log of p\_value is higher than the threshold which is 6.3, we can find that with only 30 traces, you will be able to identify the leakage.

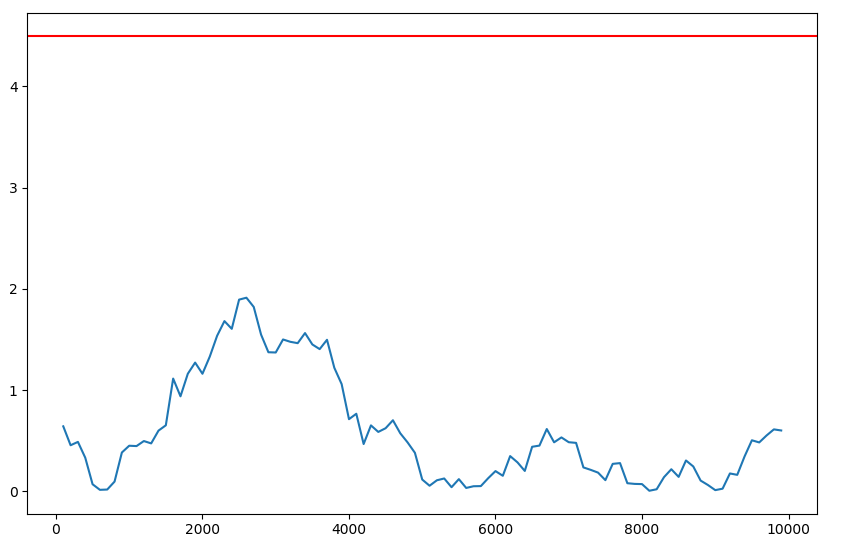


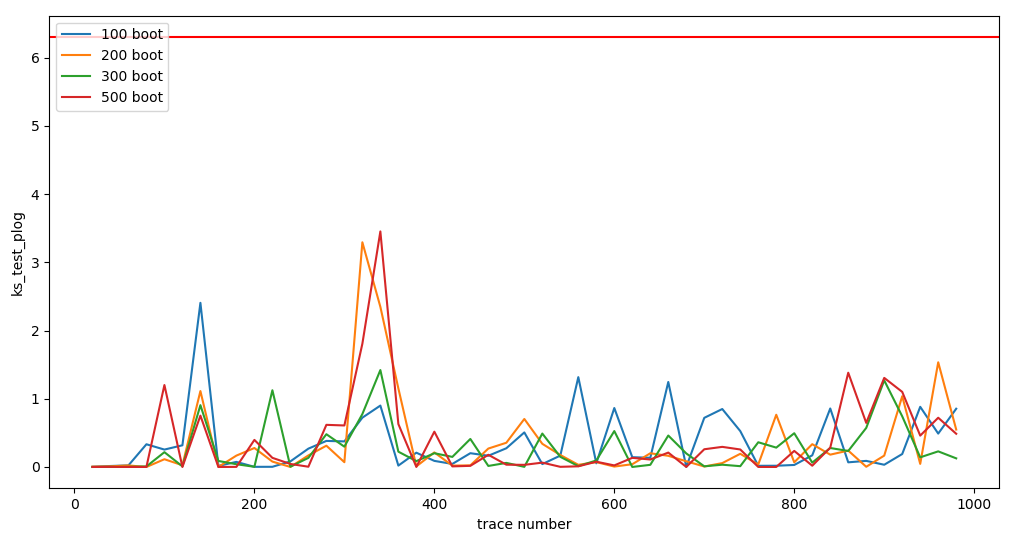
**Random vs Random experiment comparison**

For the trace set: **( result in the folder: Z:\simulation-trace\fn\_rr\_evolution)**

rand\_noise\_trace10000.txt

rand2\_noise\_trace10000.txt

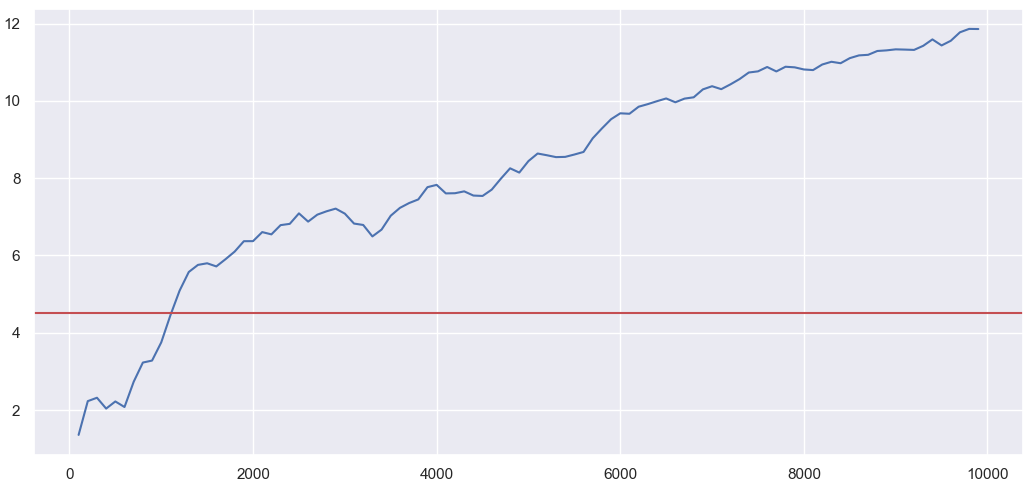
Read in the traces and read 



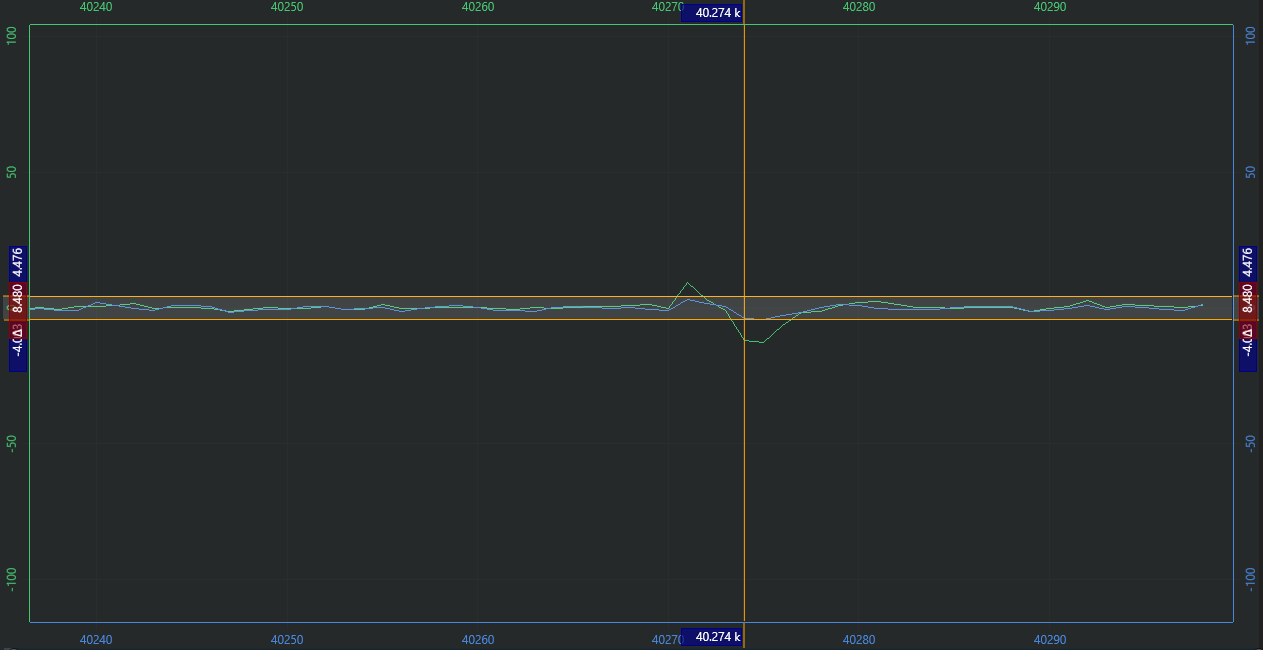
**Experiment on the olimex board:**

This is an AES naïve protected implementation. In total there are 0-100000 samples in the traces. I choose the sample-40274 as a case study. In this sample, it doesn’t leak at 1000 traces, the t value is 4.0.

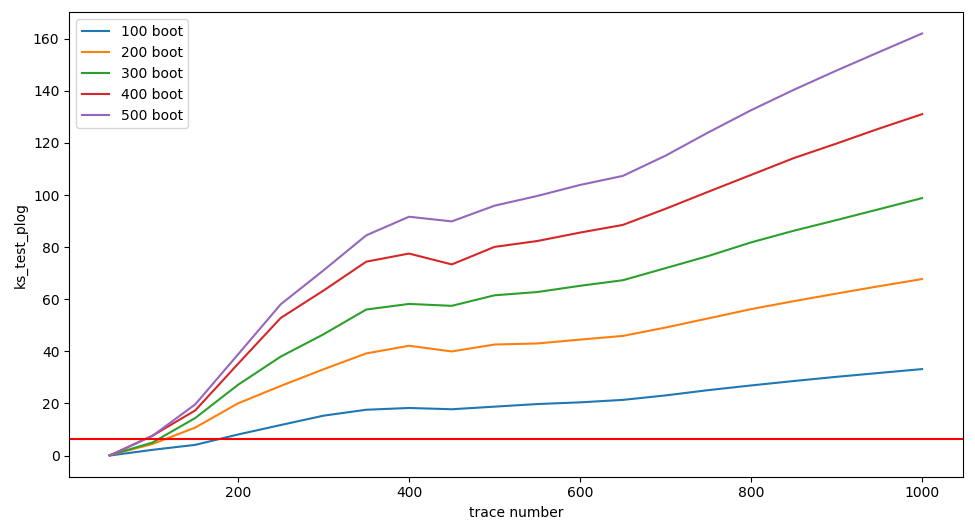
On the sample[40274], we have this evolution regarding the t-value(y: tvalue, x-number of traces)



At this position, it will not leak until 1000 traces.



In this point, the blue line is the one is the t-peak at the sample 40274 when there are 1000 traces. And then green is the t-peak at the sample 40274 when there are 5000 traces. So we can see that this is a leaky point, have false positive when traces not that much.



**Experiment on the False Positive:**

For a simulated trace set with 1000 random traces and random 1000 traces. This random vs random set of traces, the t-value is 5.28109118925, this is a false positive case.

We divide this set of traces into slices, one slice has 200 traces. Implement boot strapping on each of the traces.

Bootnum is 600. If any of them is bad traces, we will say it may be false positive.

**Case-1:**

obsv rand vs rand-t: 5.28109226026 p:1.42392121547e-07

p\_ks: [0.9991232928974864, 7.564659756359237e-104, 1.1675129652988354e-119, 3.5576778774448364e-96, 1.4155729037640332e-06]

p\_ks\_log: [3.80916057e-04 1.03121211e+02 1.18932738e+02 9.54488334e+01, 5.84906776e+00]

**Case-2:**

obsv rand vs rand-t:4.52894493253 p:6.27771186284e-06

p\_ks:[2.5357626243502377e-48, 3.557677877444533e-96, 2.1488576015462665e-109, 0.9991232928974862, 7.90883130611672e-18]

p\_ks\_log:[4.75958914e+01, 9.54488334e+01, 1.08667792e+02, 3.80916057e-04, 1.71018877e+01]

**Case-3:**

obsv rand vs rand-t:5.26827223072 p:1.52578176953e-07

p\_ks:[0.0004029766550936929, 1.2891161543822386e-122, 3.689788882097665e-44, 2.618614238830309e-65, 2.3505317403494346e-54]

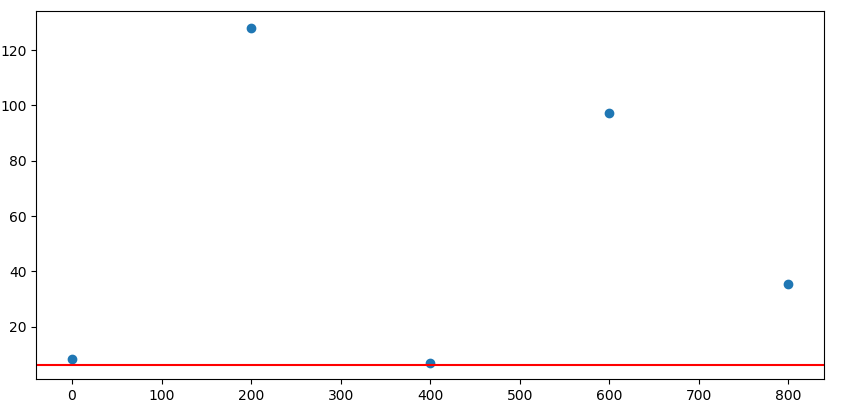
p\_ks\_log:[ 3.39472011 121.88970795 43.43299848 64.58192847 53.62883388]

**Case-4:**

**Slice200: (no bad case)**

obsv rand vs rand-t:-5.46359617967 p:5.24938938259e-08

p\_ks:[3.437075242665017e-09, 1.2237640044103214e-128, 8.984816380192807e-08, 4.579208761301225e-98, 3.592240263396201e-36]

p\_ks\_log:[ 8.46381096 127.91230233 7.04649079 97.33920956 35.44463462]

**Slice100: (has bad case)**

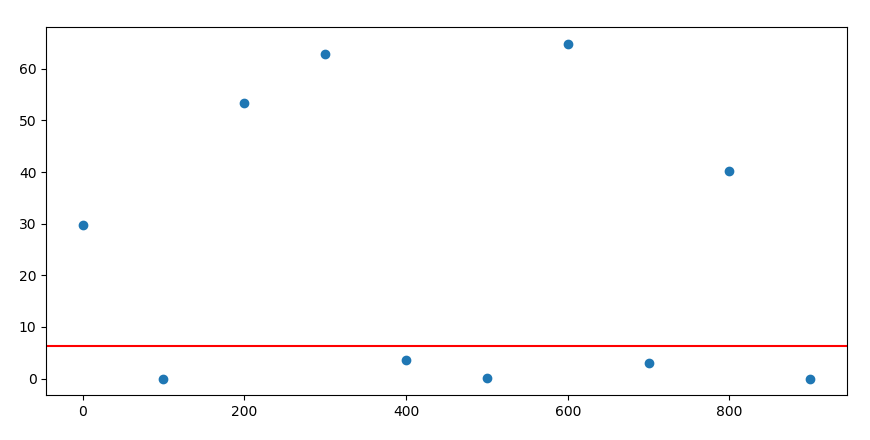
obsv rand vs rand-t:-5.46359617967 p:5.24938938259e-08

p\_ks:[3.093013007529419e-27, 0.8712150443724264, 1.3057257146205775e-53, 1.749869060567244e-65, 8.926787010740584e-05, 0.6778926173429699, 3.1288558839604628e-62, 0.04129590531905744, 2.3023797898886694e-42, 0.9999164542876107]

p\_ks\_log:[2.65096183e+01 5.98746337e-02 5.28841480e+01 6.47569944e+01

4.04930483e+00 1.68839096e-01 6.15046144e+01 1.38409301e+00

4.16378230e+01 3.62849576e-05]



**Compare with true positive case:**

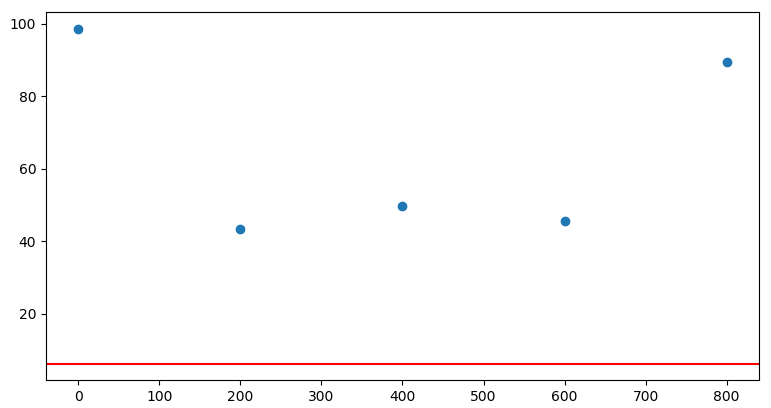
**Case1:**

**obsv rand vs rand-t:-5.59149578035 p:2.56575267349e-08**

**Slice200: (no bad case)**

p\_ks:[3.2937826275359153e-99, 3.689788882097665e-44, 1.7852692861302625e-50, 1.7727907426067927e-46, 2.9935960446893755e-90]

p\_ks\_log:[98.48230507 43.43299848 49.74829627 45.75134252 89.5238068 ]



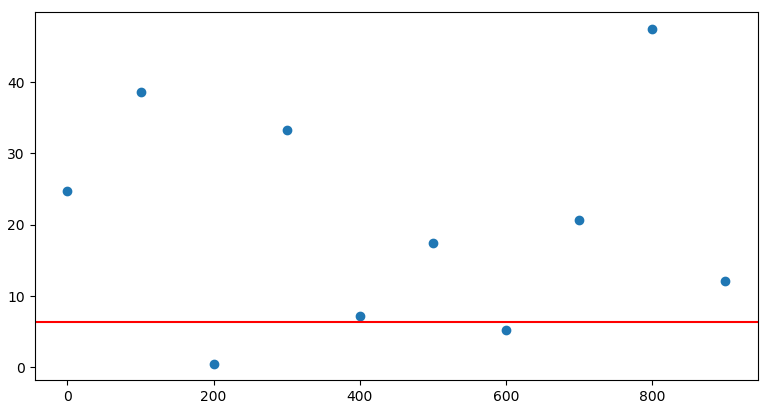
**Slice100: (also have bad case)**

obsv rand vs rand-t:-5.59149578035 p:2.56575267349e-08

p\_ks:[1.6318490584577587e-25, 2.7426771275077172e-39, 0.3075158125869262, 5.584926298120324e-34, 5.64235435215078e-08, 3.996891504061668e-18, 5.37196746513371e-06, 1.8834807293526534e-21, 3.611111303999259e-48, 6.764260626635851e-13]

p\_ks\_log:[24.78732001 38.56182532 0.51213255 33.25298255 7.24853964 17.39827764

5.26986663 20.72503882 47.44235913 12.16977967]



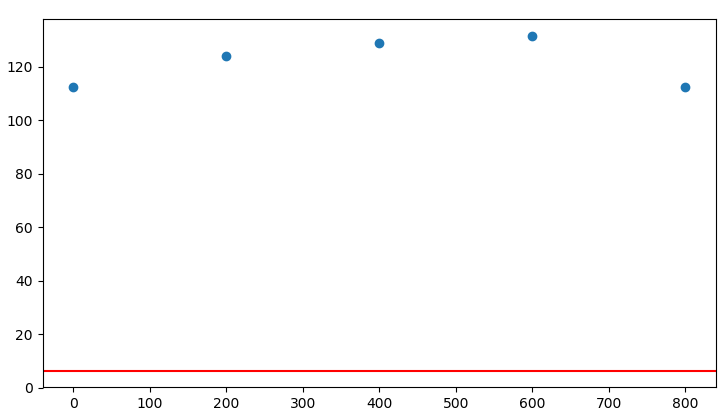
**Case2:**

**obsv rand vs rand-t:-10.9556695361 p:3.7781633767e-27**

**Slice200:**

p\_ks: [4.8983059250936263e-113, 9.462292379701568e-125, 1.6424821153005704e-129, 3.812149925119005e-132, 4.8983059250936263e-113]

p\_ks\_log: [112.30995409 124.02400364 128.78449935 131.41883003 112.30995409]

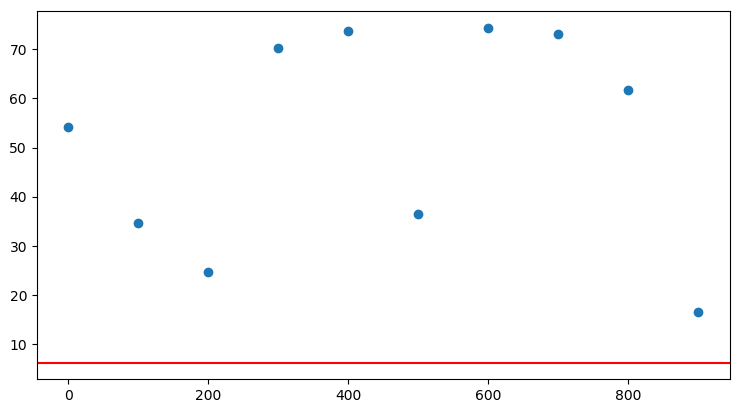


**Slice100:**

obsv rand vs rand-t:-10.9556695361 p:3.7781633767e-27

p\_ks: [6.788112300065515e-55, 2.548206883545998e-35, 1.871965978080394e-25, 5.233201774039631e-71, 1.7619277462384402e-74, 3.0547333974457096e-37, 5.534380968170295e-75, 9.935175642810039e-74, 1.8443287297256352e-62, 3.1828093356817983e-17]

p\_ks\_log: [54.16825098 34.59376532 24.72770205 70.28123252 73.75401191 36.51502669, 74.25693095 73.00282445 61.73416167 16.49718938]



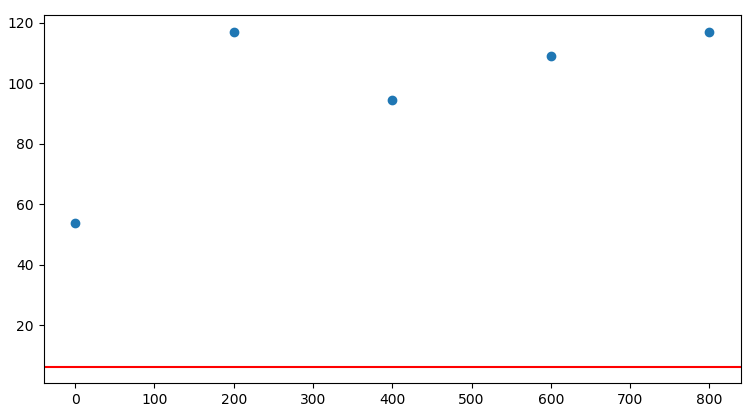
**Case3:**

**obsv rand vs rand-t:-7.61343959335 p:4.08928757823e-14**

**Slice200:**

p\_ks:[2.3505317403494346e-54, 1.436178424807275e-117, 4.7481292350596555e-95, 8.520784865583226e-110, 1.436178424807275e-117]

p\_ks\_log:[ 53.62883388 116.8427916 94.32347747 109.0695204 116.8427916 ]

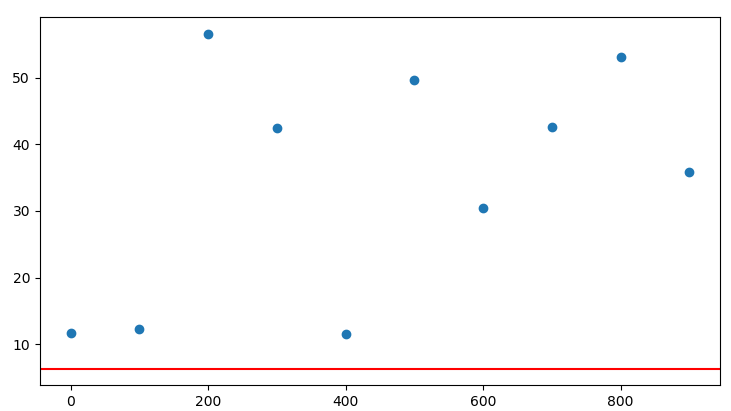


**Slice100:**

p\_ks:[2.246968244054414e-12, 5.481553834222951e-13, 2.7401717501221924e-57, 4.009757454367801e-43, 3.567994423538566e-12, 1.815916936403143e-50, 3.8130382386986677e-31, 2.5839831935110035e-43, 7.99647353432644e-54, 1.5472858422516345e-36]

p\_ks\_log:[11.64840307 12.26109632 56.56222222 42.3968819 11.44757583 49.74090402

30.41872884 42.58771032 53.0971015 35.81042945]



**Case which have one false positive and then change one set to fix value**

**Random trace vs fix random trace:**

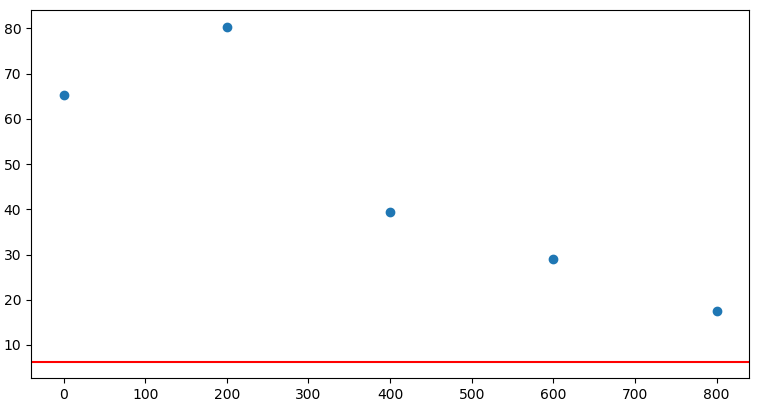
**False positive** obsv rand vs rand-t:4.57161882505 p:5.13600132717e-06

**200-slice**

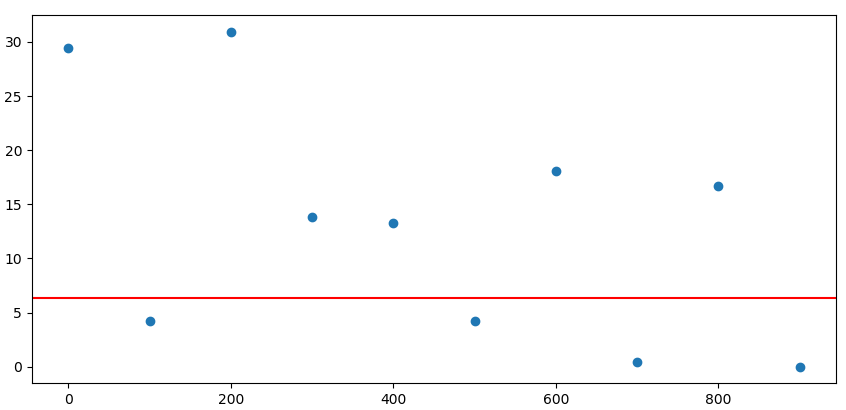
obsv rand vs rand-t:4.57161882505 p:5.13600132717e-06

p\_ks:[6.268815770936441e-66, 5.020945020321976e-81, 3.4727381178332274e-40, 8.146045602801461e-30, 2.59178798996368e-18]

p\_ks\_log:[65.20281449 80.29921453 39.45932797 29.08905316 17.58640053]



**100-slice**



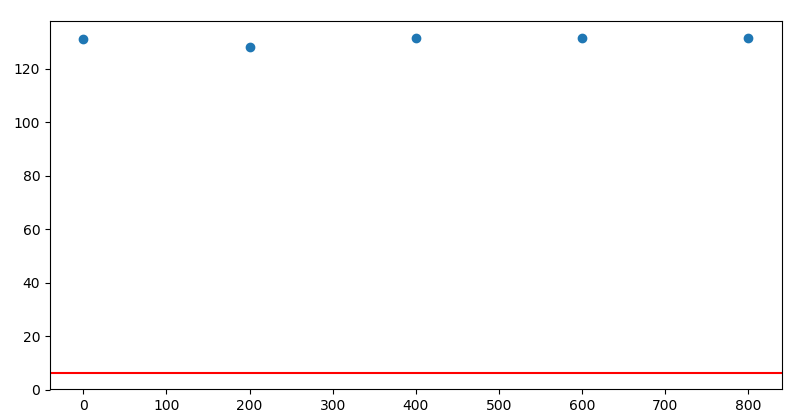
**True Positive: change the one random set to fix set.**

obsv rand vs rand-t:-13.1674822079 p:1.25150297099e-36

**200-slice**

p\_ks:[1.0521386152238108e-131, 1.2237640044103214e-128, 3.812149925119005e-132, 3.812149925119005e-132, 3.812149925119005e-132]

p\_ks\_log:[130.97792704 127.91230233 131.41883003 131.41883003 131.41883003]

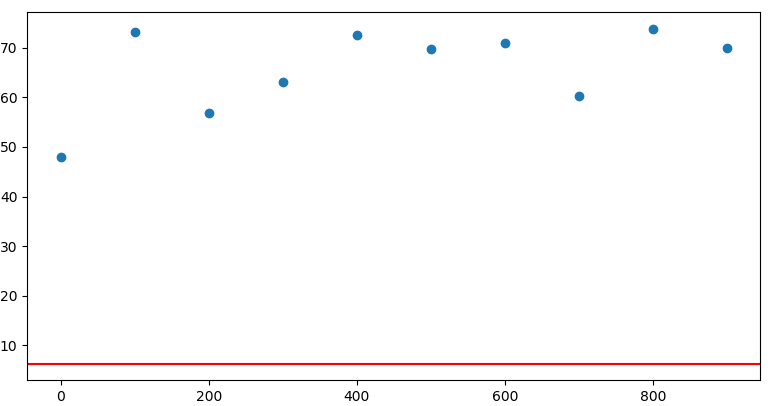


**100-slice**

p\_ks:[1.2562914340807531e-48, 5.5873414510150385e-74, 1.650407344247869e-57, 7.579138634244978e-64, 3.132129995394915e-73, 1.6146229377868164e-70, 9.585635537303159e-72, 4.332509070093073e-61, 1.7619277462384402e-74, 9.196700418812299e-71]

p\_ks\_log:[47.9009096 73.25279479 56.78240885 63.12038015 72.50416022 69.79192888

71.01837909 60.36326052 73.75401191 70.03636796]



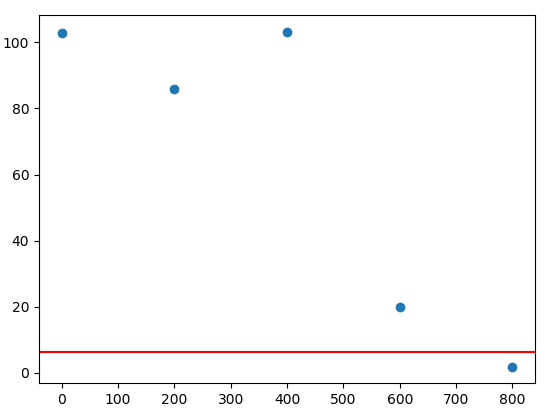
**Case2:**

False Positive: obsv rand vs rand-t:5.37823108564 p:8.40376526606e-08

**200-slice**

p\_ks:[1.8596455940159415e-103, 1.2112821065343148e-86, 7.564659756359237e-104, 1.7265224683578717e-20, 0.014667785895916509]

p\_ks\_log:[102.73056981 85.9167547 103.1212106 19.76282777 1.83363544]



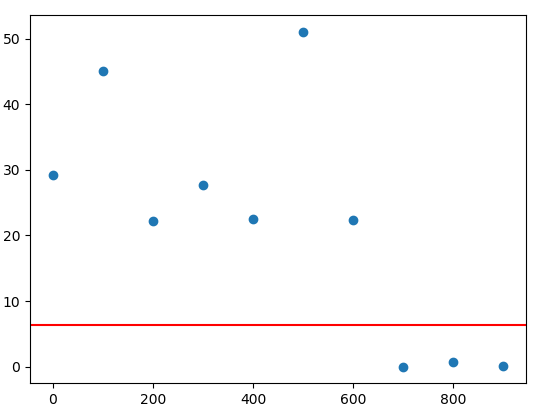
**100-slice**

p\_ks:[7.263054197225627e-30, 7.812705081008992e-46, 6.765381233041863e-23, 1.8552357129437928e-28, 3.5717280602971435e-23, 1.031065769243342e-51, 4.9181081051005737e-23, 0.9999727936949891, 0.1691767404986982, 0.6778926173429702]

p\_ks\_log:[2.91388807e+01 4.51071986e+01 2.21697077e+01 2.77316009e+01

2.24471216e+01 5.09867136e+01 2.23082019e+01 1.18157089e-05

7.71659347e-01 1.68839096e-01]



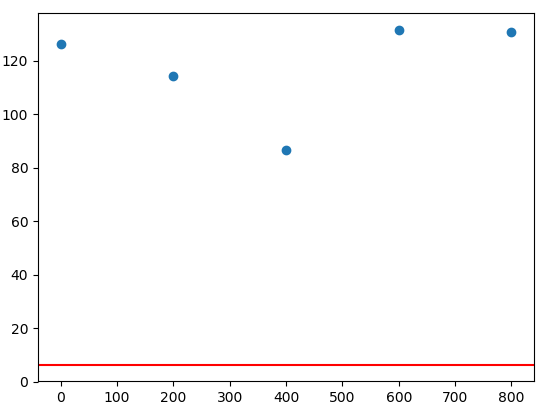
**True Positive: change the one random set to fix set.**

obsv rand vs rand-t:-10.5073084988 p:1.445422976e-24

**200-slice**

p\_ks:[6.656131992027875e-127, 4.372728073518541e-115, 2.3321048966235707e-87, 3.812149925119005e-132, 2.898923788459267e-131]

p\_ks\_log:[126.17677807 114.35924753 86.63225192 131.41883003 130.5377632 ]

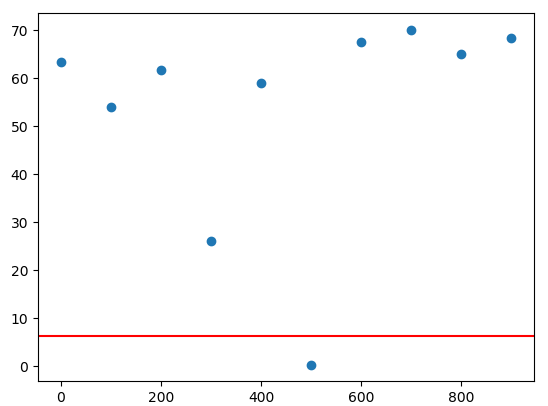


**100-slice**

p\_ks:[4.4370492845933355e-64, 1.1138581284834956e-54, 1.8443287297256352e-62, 6.189030099416482e-27, 9.824790500187441e-60, 0.4261152760490878, 2.448364975607311e-68, 9.196700418812299e-71, 1.0174230772558232e-65, 4.6320205511431185e-69]

p\_ks\_log:[63.35290575 53.95317012 61.73416167 26.20837741 59.0076767 0.3704729

67.61112384 70.03636796 64.99249842 68.33422952]



**Case3**

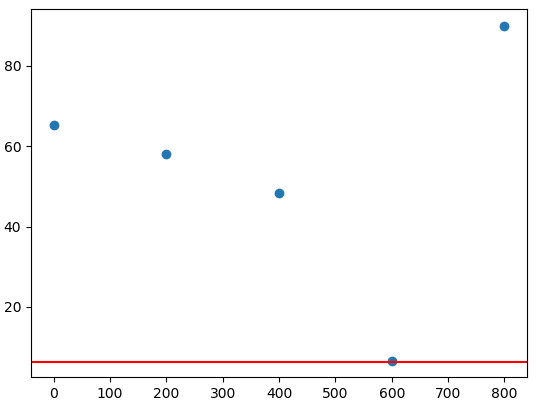
**False Positive**

obsv rand vs rand-t:5.01631489306 p:5.73305287628e-07

**200-slice**

p\_ks:[6.268815770936441e-66, 1.1289692650117905e-58, 4.0040583517035474e-49, 2.3146035666458489e-07, 1.2924765156347273e-90]

p\_ks\_log:[65.20281449 57.94731788 48.3974996 6.63552338 89.88857734]

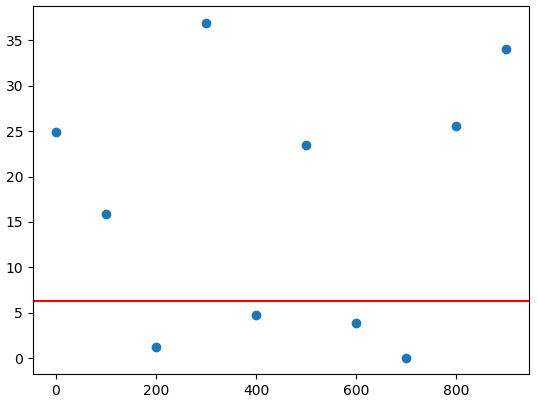


**100-slice**

p\_ks:[1.337042099630385e-25, 1.2453559687752253e-16, 0.06308380791938048, 1.3493412750344823e-37, 1.8016534854743396e-05, 3.702773190198229e-24, 0.00011790491168606678, 0.8280929309885813, 2.449054865162297e-26, 8.342187534574905e-35]

p\_ks\_log:[24.87385492 15.90470649 1.2000821 36.86987819 4.74432873 23.43147289

3.9284681 0.08192092 25.61100149 34.07872005]



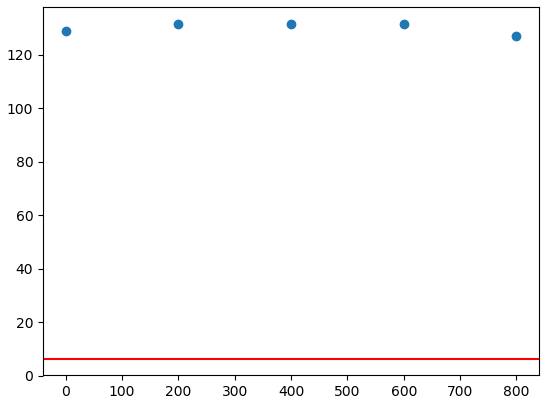
**True Positive**

obsv rand vs rand-t:-13.148696293 p:1.54685056177e-36

**200-slice**

p\_ks:[1.6424821153005704e-129, 3.812149925119005e-132, 3.812149925119005e-132, 3.812149925119005e-132, 9.056035163877316e-128]

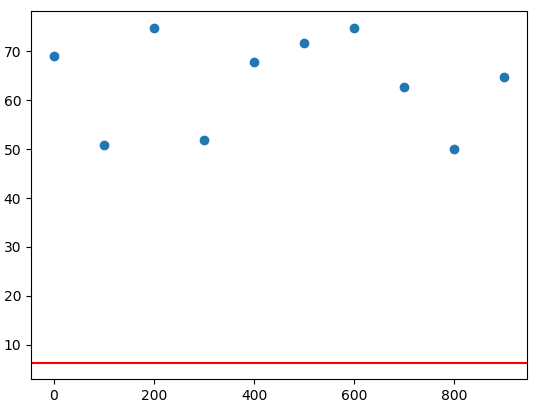
p\_ks\_log:[128.78449935 131.41883003 131.41883003 131.41883003 127.0430619 ]



**100-slice**

p\_ks:[8.68631279209662e-70, 1.667189657300754e-51, 1.7316020128535686e-75, 1.4936092688776157e-52, 1.406910311748921e-68, 1.7403837190405937e-72, 1.7316020128535686e-75, 2.2049289698617128e-63, 1.128560245106482e-50, 1.749869060567244e-65]

p\_ks\_log:[69.06116454 50.77801499 74.76155192 51.825763 67.85173359 71.75935499 74.76155192 62.6566054 49.94747525 64.75699445]



**Compare with True Positive Case with small value**

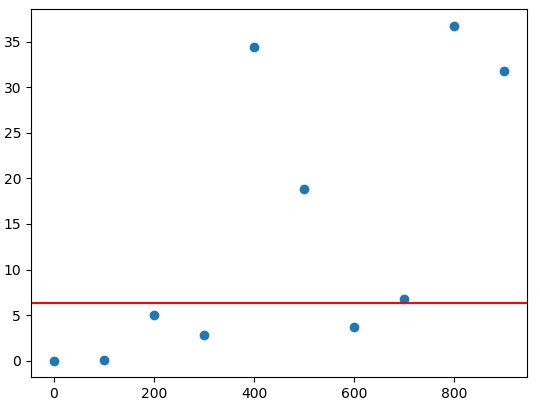
**Case1:**

obsv rand vs rand-t:4.53687841348 p:6.05096039572e-06

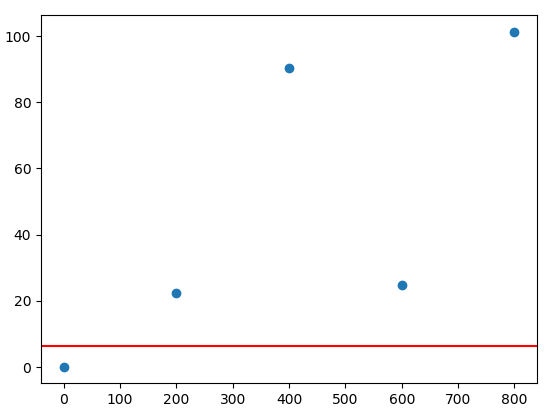
**100-slice**

p\_ks:[0.9634284310693951, 0.8907421420833641, 9.77621755201305e-06, 0.0013633182104698196, 3.7874065043627696e-35, 1.426809202586228e-19, 0.00020328230160267772, 1.795587801275457e-07, 2.031235601682271e-37, 1.8801488140757117e-32]

p\_ks\_log:[1.61805417e-02 5.02480002e-02 5.00982914e+00 2.86540276e+00, 3.44216581e+01 1.88456341e+01 3.69190043e+00 6.74579335e+00, 3.66922397e+01 3.17258078e+01]



**200-slice**



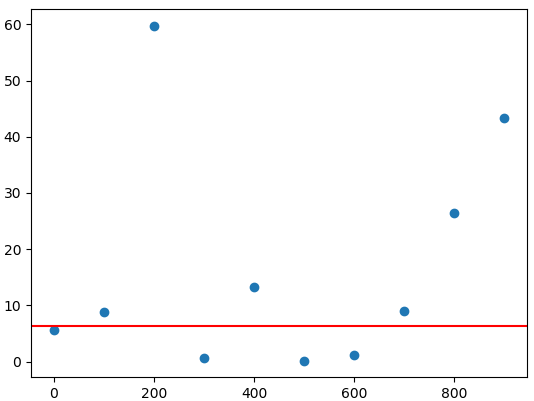
**Case2:**

obsv rand vs rand-t:4.9761421554 p:7.04287182112e-07

**100-slice**

p\_ks:[2.33294378663062e-06, 1.532156826660911e-09, 2.072268645350059e-60, 0.26827913081835786, 4.827360709973276e-14, 0.6778926173429702, 0.06308380791938034, 1.019302168273736e-09, 3.093013007529353e-27, 4.412870625448152e-44]

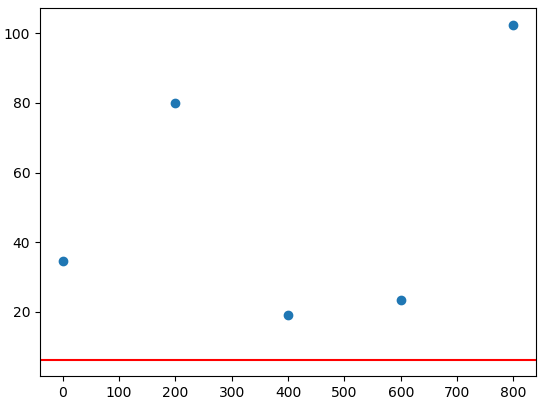
p\_ks\_log:[ 5.63209573 8.81469678 59.68355394 0.57141311 13.31629025 0.1688391

1.2000821 8.99169705 26.50961825 43.3552788 ]

**200-slice**

p\_ks:[1.7444807094813664e-35, 1.11070557290306e-80, 8.320450752765771e-20, 4.414719649413244e-24, 4.563854832455122e-103]

p\_ks\_log:[ 34.75833383 79.95440105 19.07985315 23.35509687 102.34066818]



**Case3:**

obsv rand vs rand-t:5.42698895313 p:6.43729617988e-08

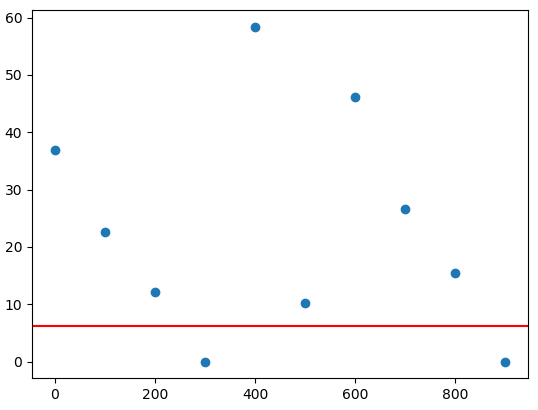
**100-slice**

p\_ks:[1.3493412750344823e-37, 2.5913926297932387e-23, 6.951570459957562e-13, 0.9997800013626197, 4.617120489185555e-59, 6.55113784748743e-11, 8.028248792215038e-47, 2.183348690813274e-27, 3.6443589628374206e-16, 0.9634284310693951]

p\_ks\_log:[3.68698782e+01 2.25864668e+01 1.21579171e+01 9.55547056e-05

5.83356288e+01 1.01836833e+01 4.60953792e+01 2.66608769e+01

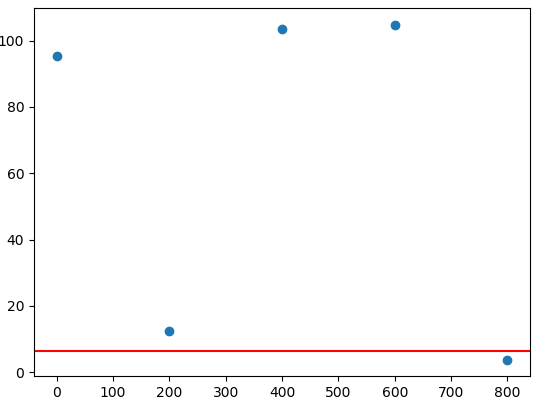
1.54383789e+01 1.61805417e-02]



**200-slice**

p\_ks:[3.557677877444533e-96, 4.490815894804724e-13, 3.0719168961076267e-104, 2.036267141245769e-105, 0.00016844786141381846]

p\_ks\_log:[ 95.44883338 12.34767475 103.51259054 104.69116525 3.7735345 ]



**Case4:**

obsv rand vs rand-t:5.20392281778 p:2.15472573258e-07

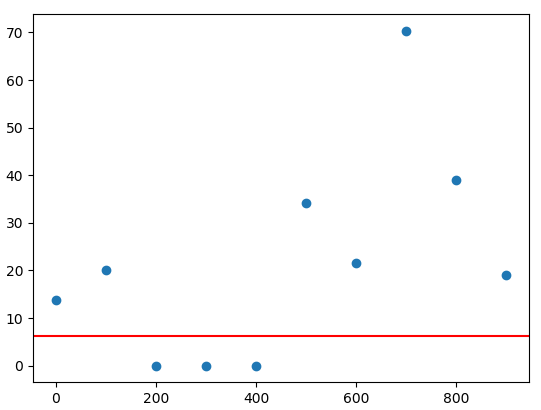
**100-slice**

p\_ks:[1.3808841089159557e-14, 9.734957468594514e-21, 0.9979744006422696, 0.9999164542876107, 0.9940781816198302, 8.34218753457455e-35, 2.398911766136538e-22, 5.233201774039631e-71, 9.231500941655981e-40, 1.0629399590441579e-19]

p\_ks\_log:[1.38598428e+01 2.00116659e+01 8.80598795e-04 3.62849576e-05

2.57945815e-03 3.40787201e+01 2.16199857e+01 7.02812325e+01

3.90347277e+01 1.89734913e+01]

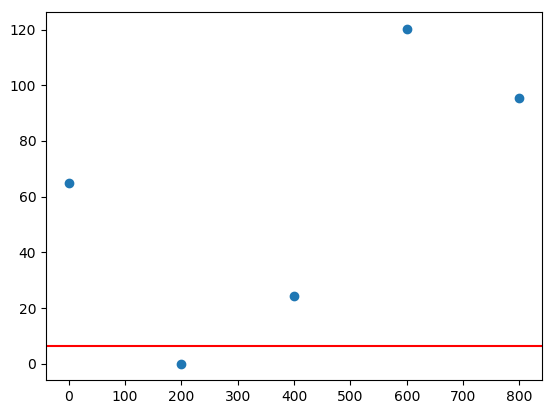


**200-slice**

p\_ks:[1.2823249459651644e-65, 0.9979216691369992, 5.019251725210255e-25, 6.374173790335909e-121, 3.557677877444533e-96]

p\_ks\_log:[6.48920019e+01 9.03546886e-04 2.42993610e+01 1.20195576e+02

9.54488334e+01]



**Look at if there is behavior in the evolution of bootstrapping**

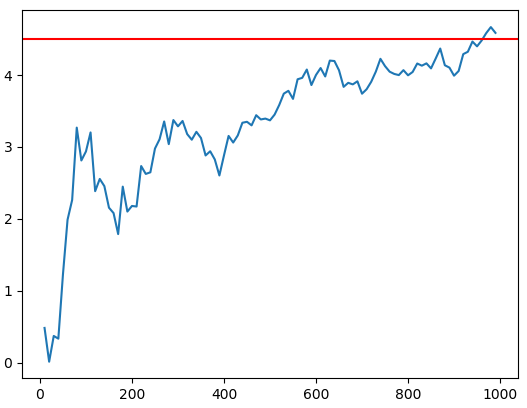
**FP\_evolution:**

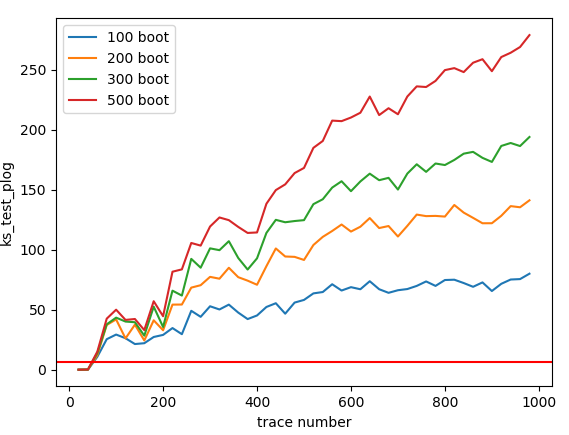
F1 = open('rr\_1000traces\_snr1\_f5-2019-07-30\_15\_09/4.5327166168Rand1Noise\_1000traces\_1SNR\_f5.txt','r')

F1 = open('rr\_1000traces\_snr1\_f5-2019-07-30\_15\_09/4.5327166168Rand2Noise\_1000traces\_1SNR\_f5.txt','r')

(result in the folder: Z:\simulation-trace\fp\_evolution)

obsv rand vs rand-t:4.58720068791 p:4.77407816337e-06





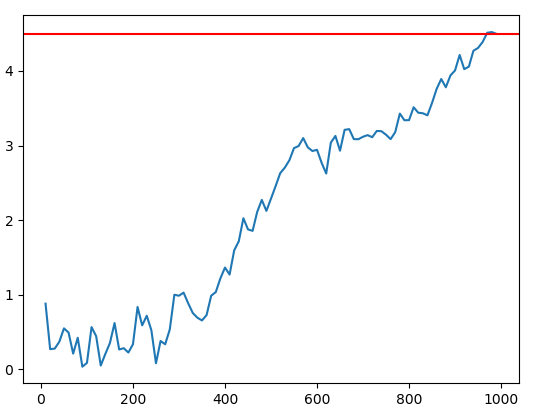
**TP\_evolution:**

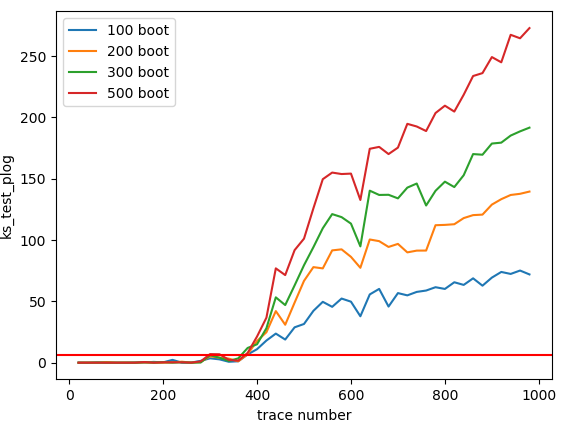
F1 = open('Z:/simulation-trace/TP\_SmallValue\_set/1RandNoise\_1000traces\_0.01SNR\_f5.txt','r')

F1 = open('Z:/simulation-trace/TP\_SmallValue\_set/1FixNoise\_1000traces\_0.01SNR\_f5.txt','r')

(result in the folder: Z:\simulation-trace\tp\_SmallValue\_evolution)

obsv rand vs rand-t:-4.49635589053 p:7.31644367216e-06

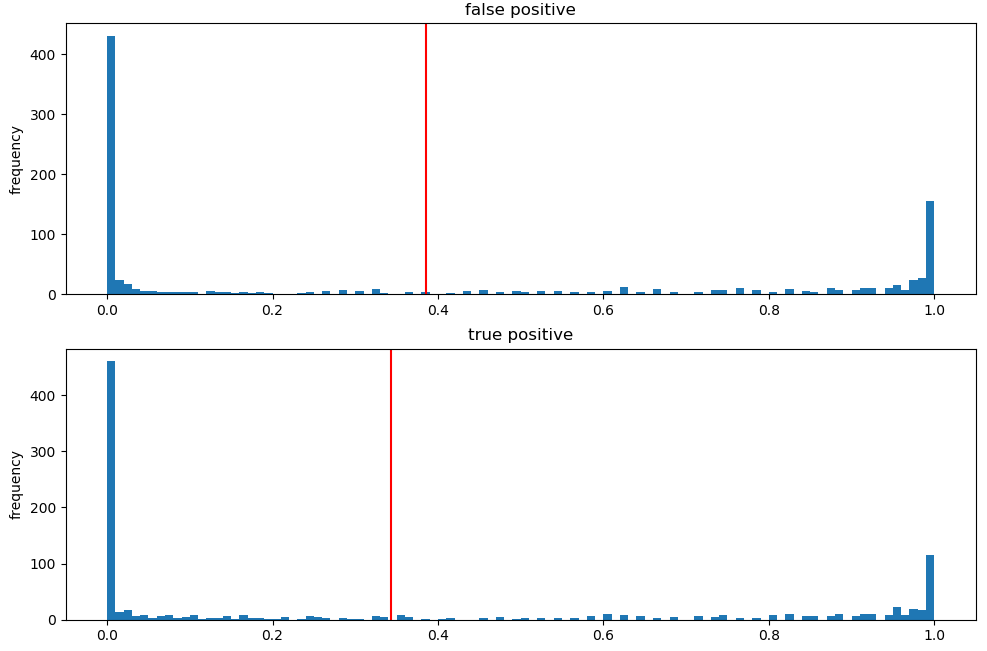




**False Positive experiment 2:**

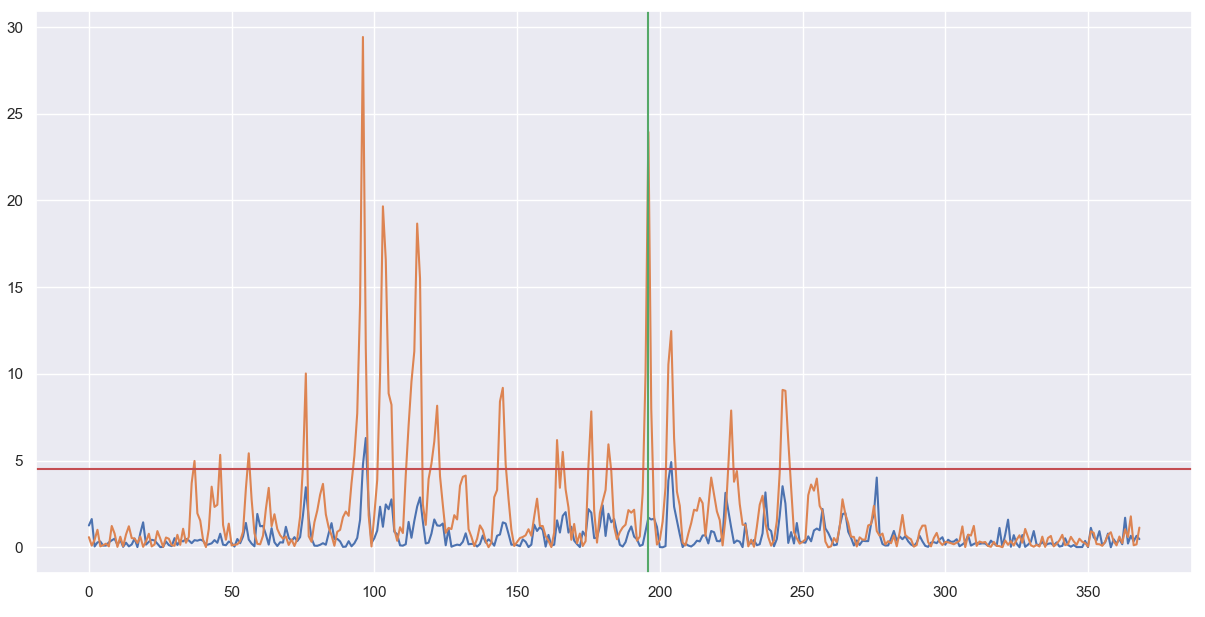
Random select slices from the traces set, and look the distribution of the bootstrapping ks-p value, check if there is difference of or bias of the distribution.

Distribution of the ks p-value:

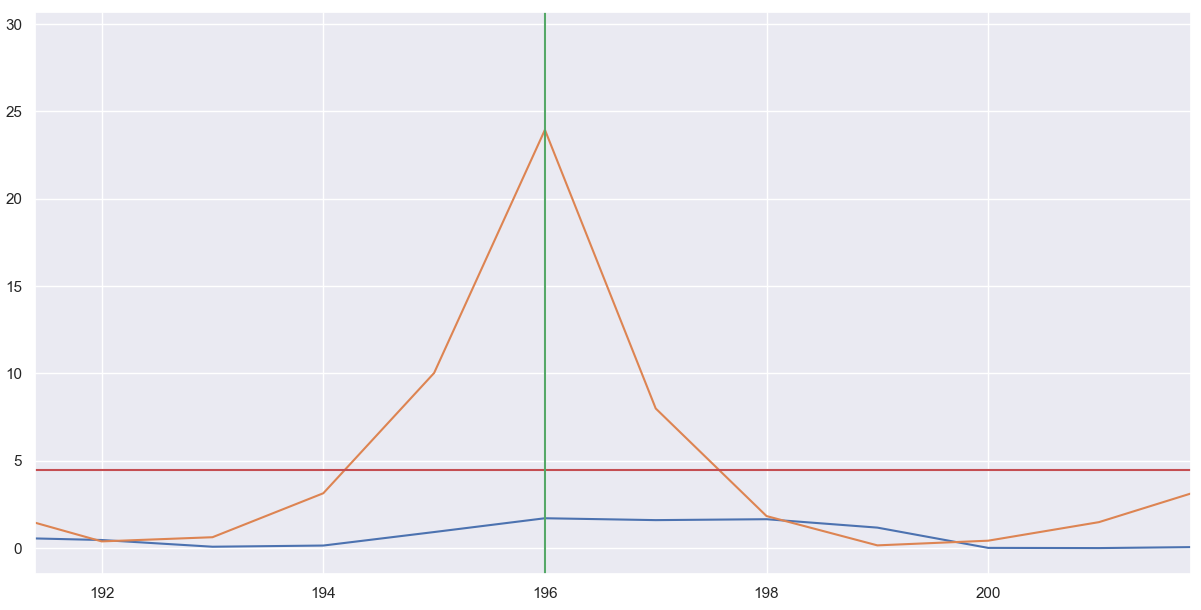


**Experiment on DPAD AES unprotected version**

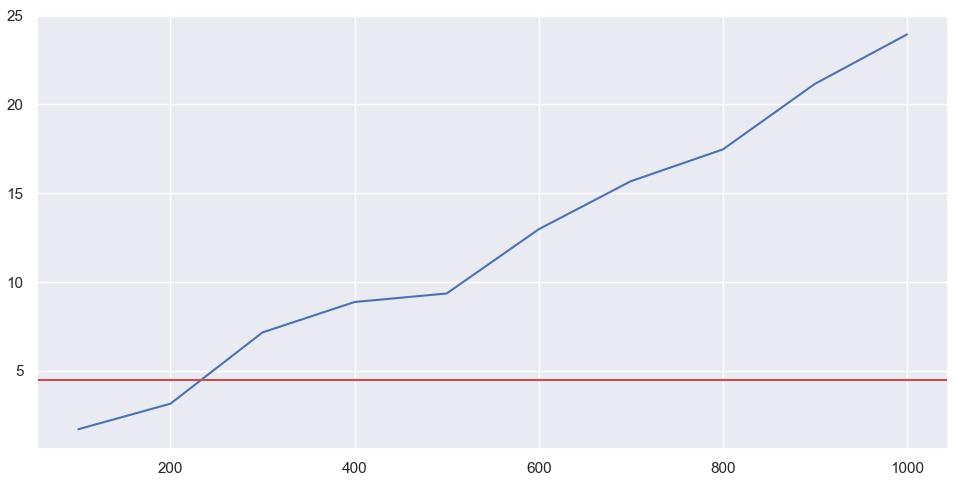
Use the sample-196 as an example: (blue line is: 100 traces, orange line: 1000 traces)



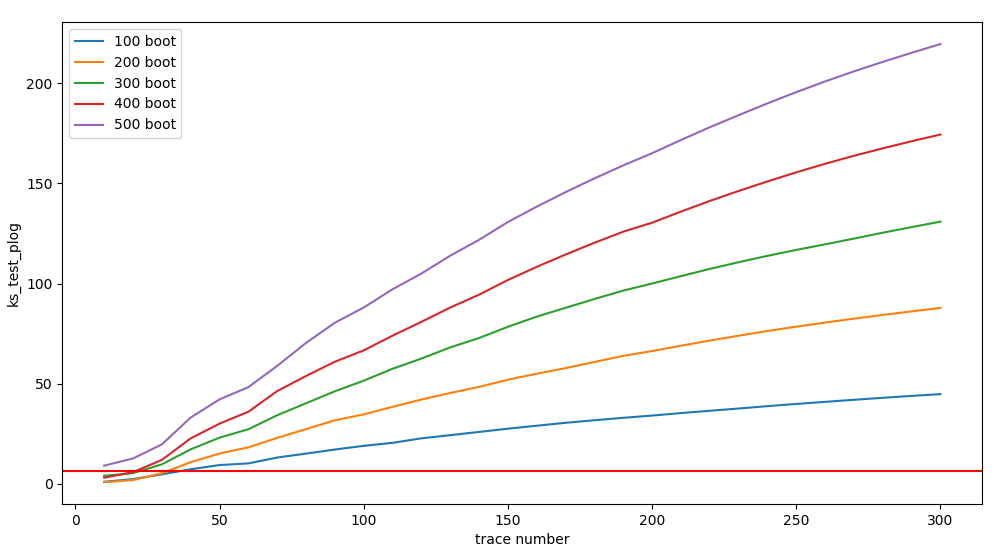
Zoom-in in the sample-196



Plot the t-value value revolution over the number of traces:



In this positive, it started detect leak after 234 traces.

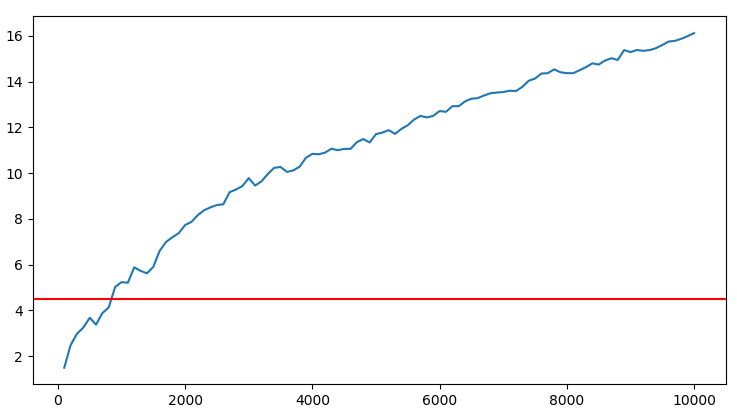


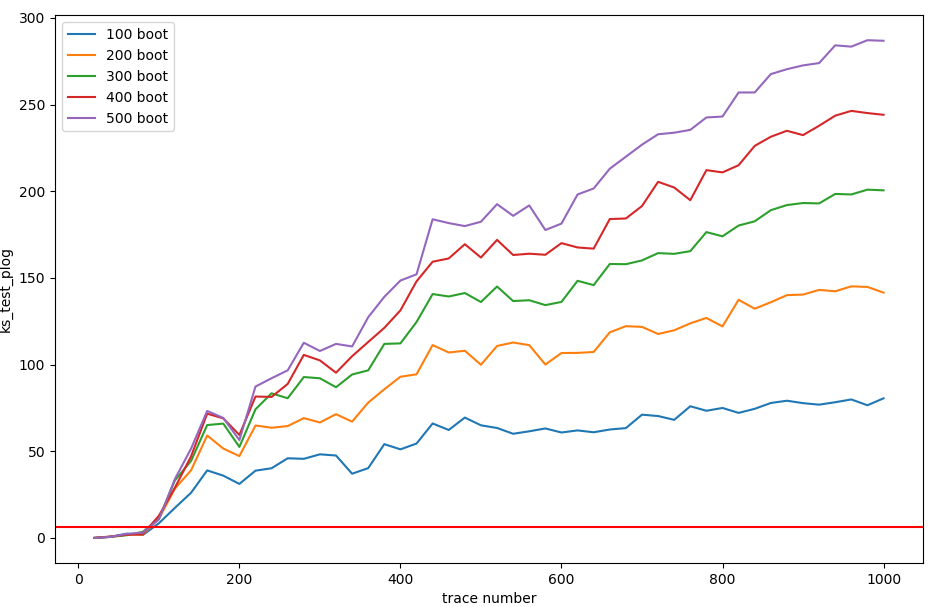
The highest number of trace needed is 36 for 100 number of boot

**Experiment on Fix vs Fix of simulated traces**

2 Fix vs Fix set, the first set the fix value the hamming weight is 5. For the second fix value hamming weight is 4.

It will not pass the threshold until 840 traces





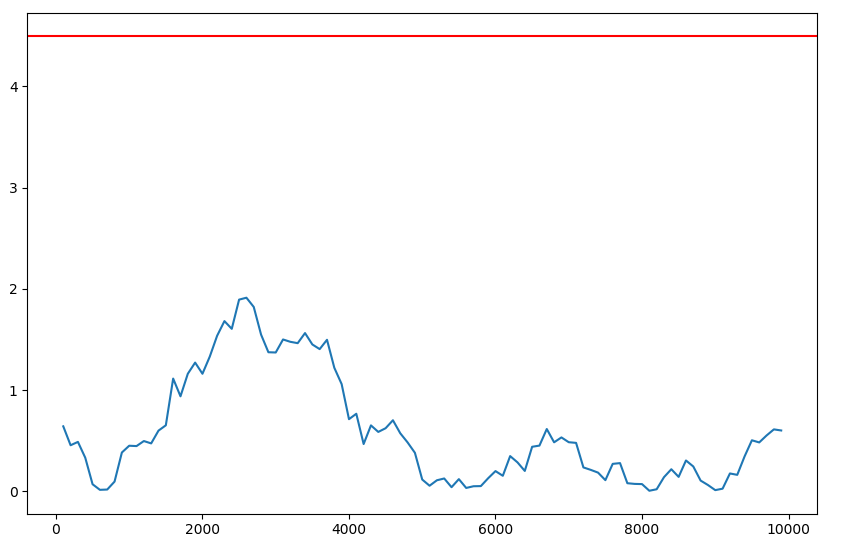
It will start detect leakage at around 90 traces.

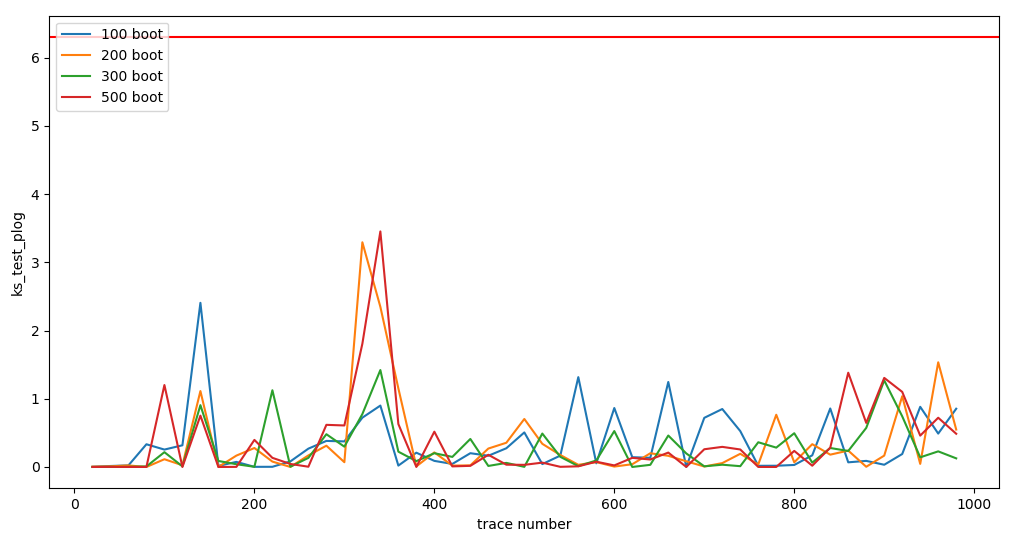
**Random vs Random experiment comparison**

For the trace set: **( result in the folder: Z:\simulation-trace\fn\_rr\_evolution)**

rand\_noise\_trace10000.txt

rand2\_noise\_trace10000.txt

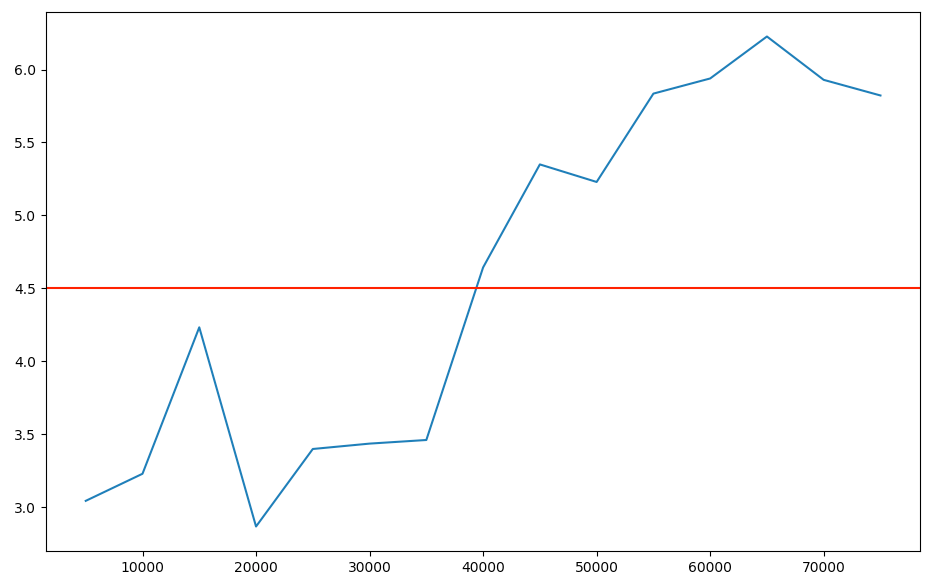
Read in the traces and read 

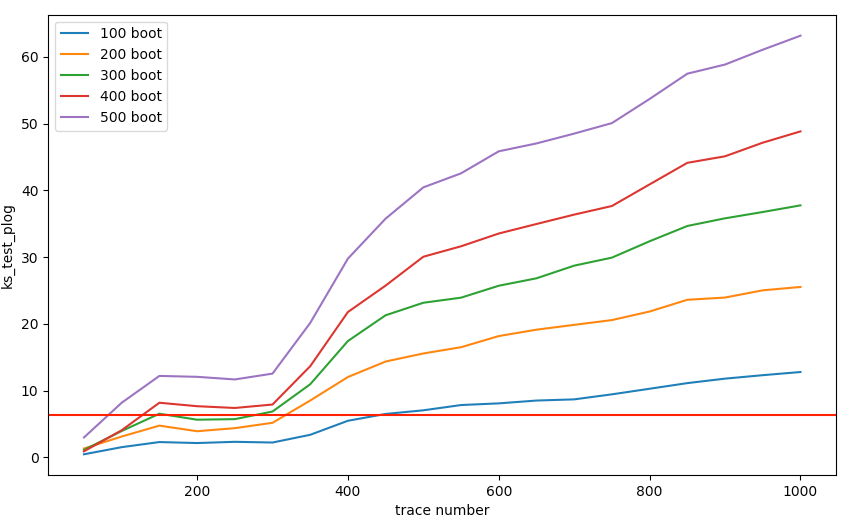


**Experiment on DPAD AES protected version**

Use the sample-83(base\_sample: 40) as an example:

TVLA evolution: in this sample, leakage will not be detected until 40000





The highest number of trace needed is 420 for 100 number of boot