Attack PICO SWAES using CW

ChipWhisperer Setup

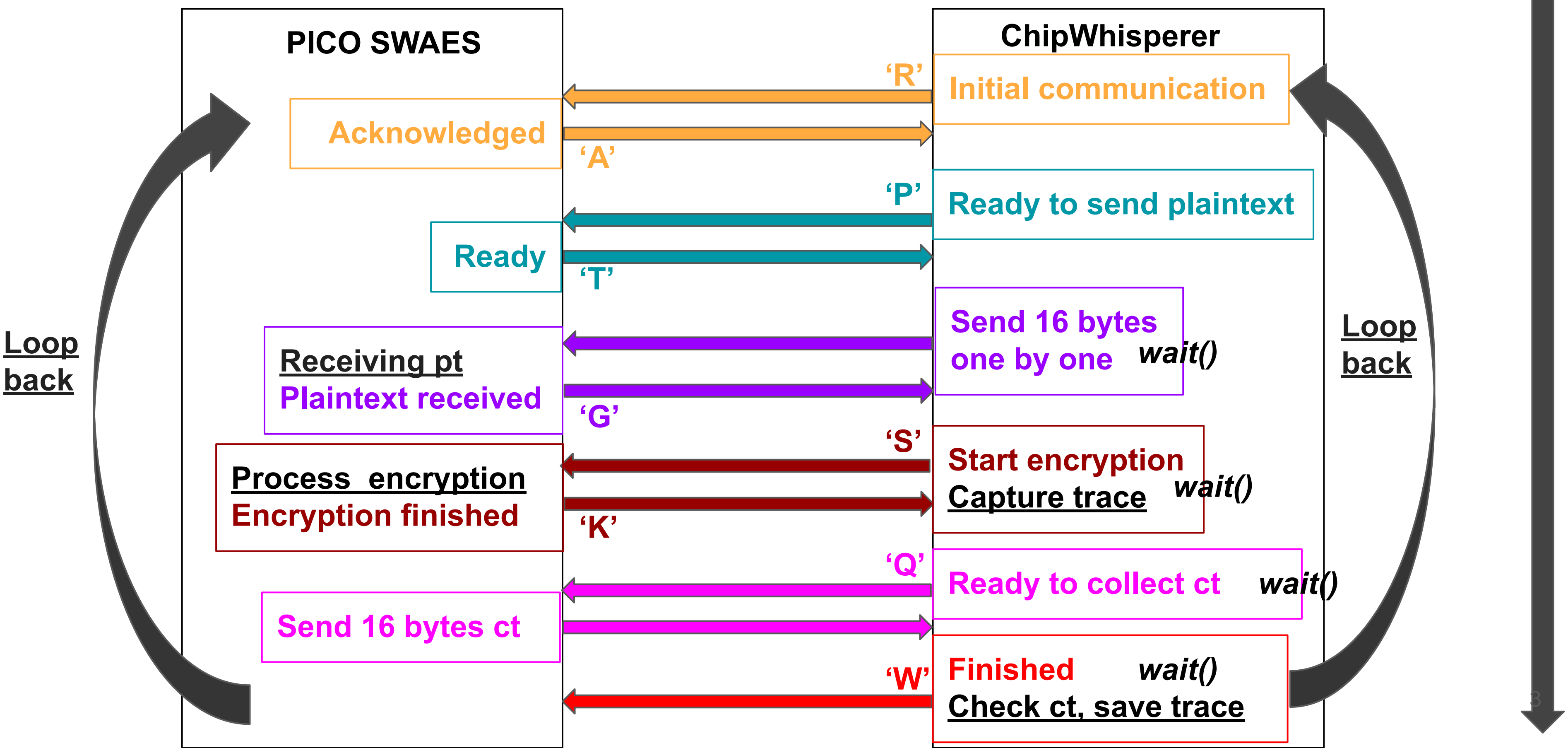
- *CW Clock : 4Mhz*
- *CW ADC Sampling rate : 16Mhz*
- *Samples per trace : 24400*
- *# of traces : 40k*
- *Time per traces to capture : 3 sec*

Attack Region and Time

- *Trigger = 1*
  1st round sbox
  Trigger = 0
- *Attack time per byte: 20 mins*

Communication between PICO SWAES and CW

Command order



PICO SWAES

ChipWhisperer

‘R’ Initial communication

Acknowledged ‘A’

‘P’ Ready to send plaintext

Ready ‘T’

Send 16 bytes one by one *wait()*

Receiving pt

Plaintext received ‘G’

‘S’ Start encryption

Capture trace *wait()*

Process encryption

Encryption finished ‘K’

‘Q’ Ready to collect ct *wait()*

Send 16 bytes ct

‘W’ Finished *wait()*

Check ct, save trace

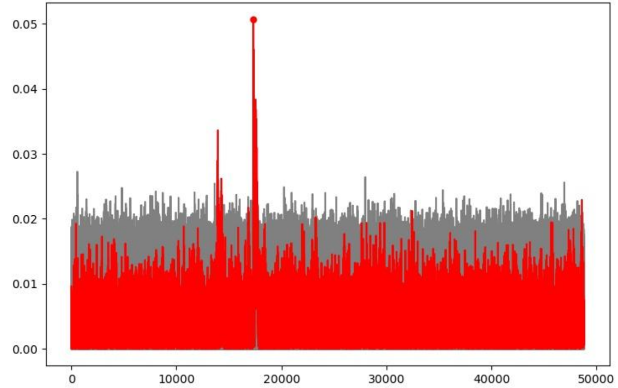
Loop back

Loop back

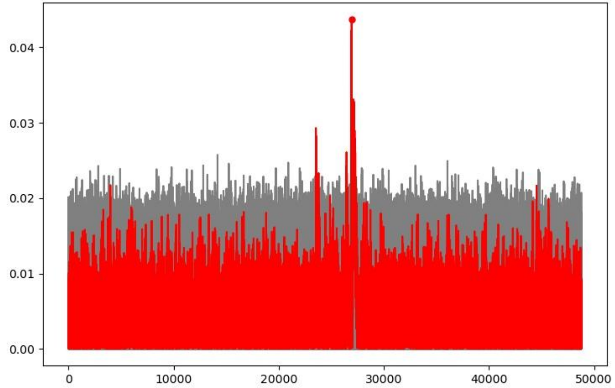
0-48800 samples

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

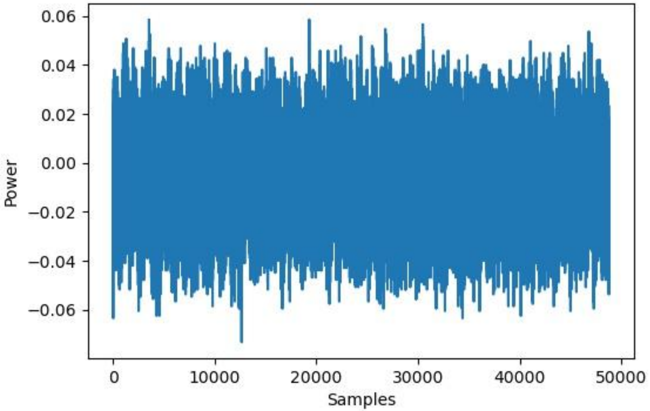
Subkey 0, Correlation 0.050702 at sample point 17319



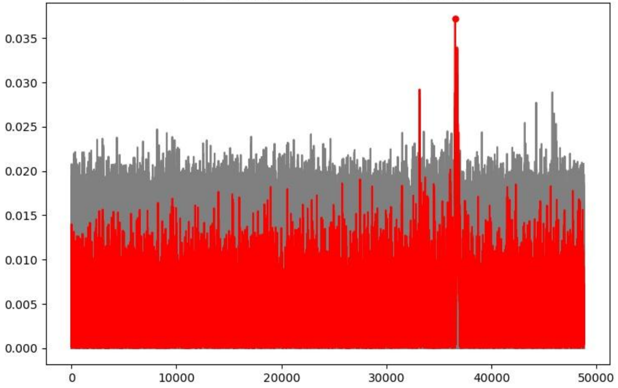
Subkey 4, Correlation 0.043747 at sample point 26941



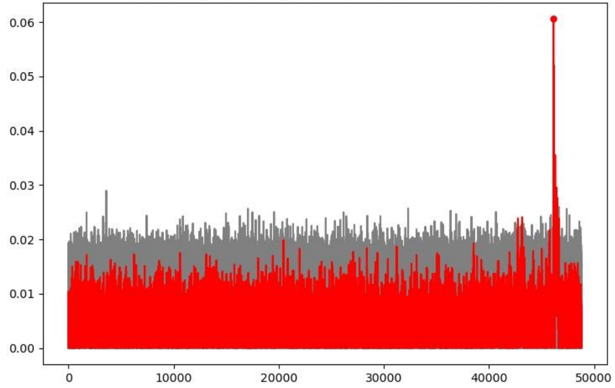
SWAES PICO CW Power Traces Plot



Subkey 8, Correlation 0.037191 at sample point 36535

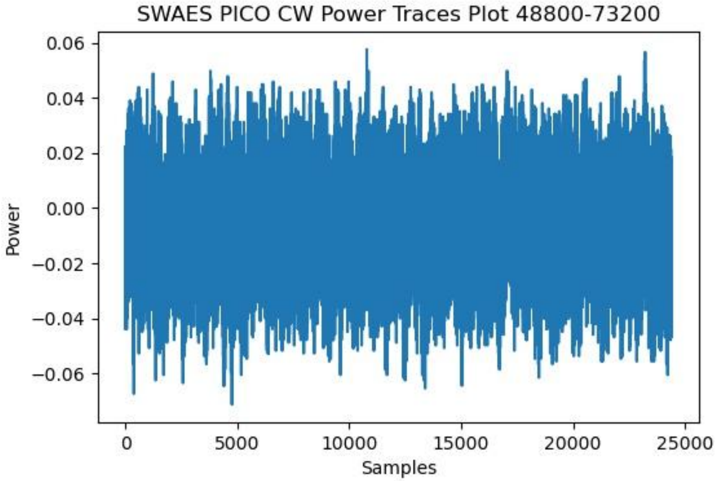


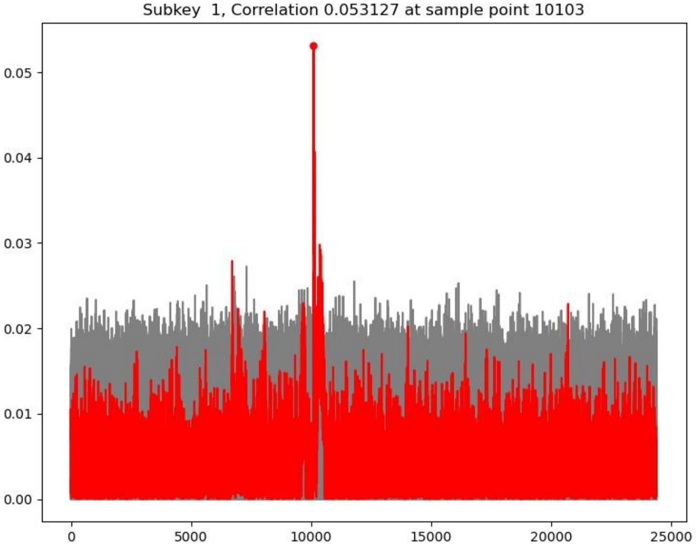
Subkey 12, Correlation 0.060589 at sample point 46139

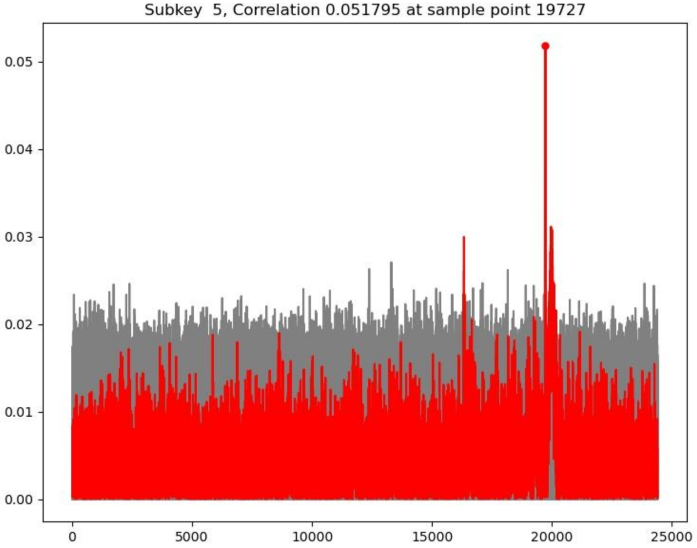


48800-73200 samples

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

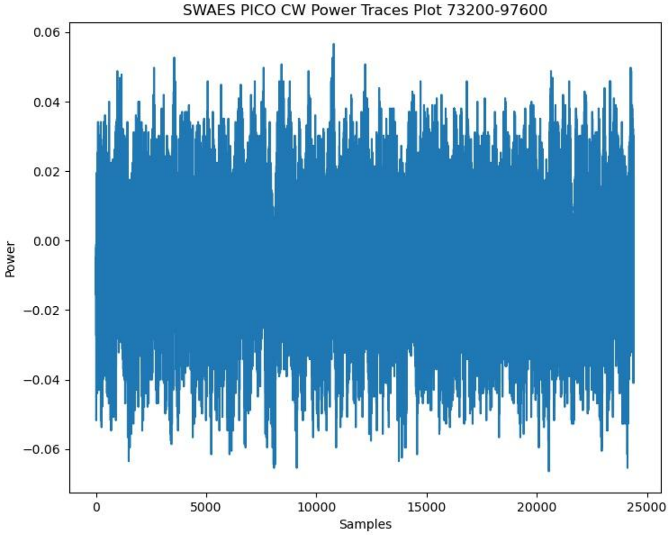

SWAES PICO CW Power Traces Plot 48800-73200

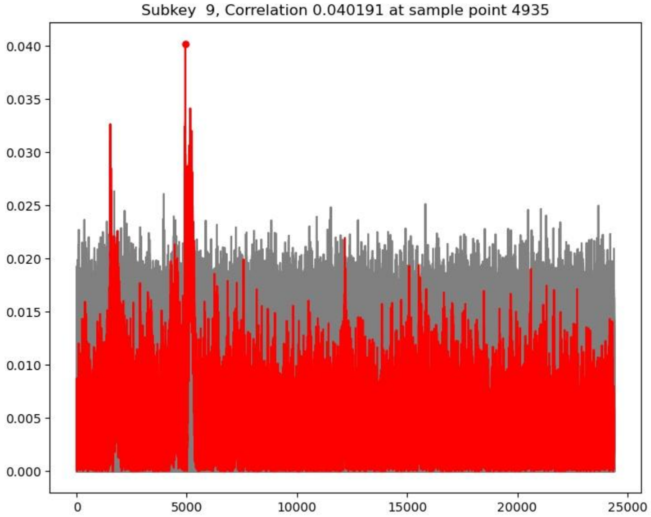

Subkey 1, Correlation 0.053127 at sample point 10103

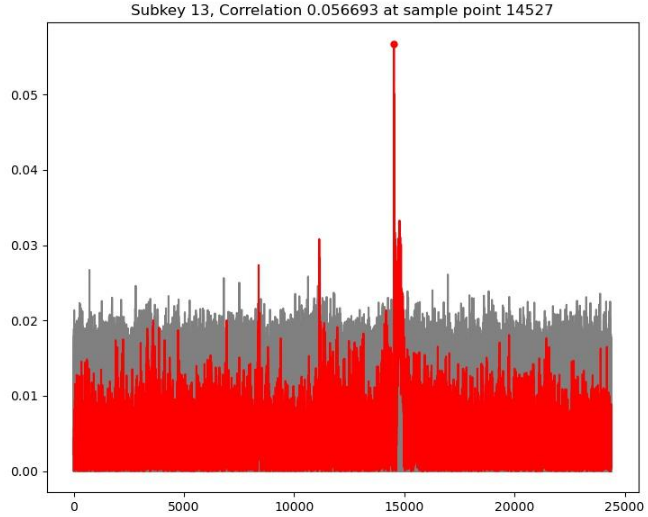

Subkey 5, Correlation 0.051795 at sample point 19727

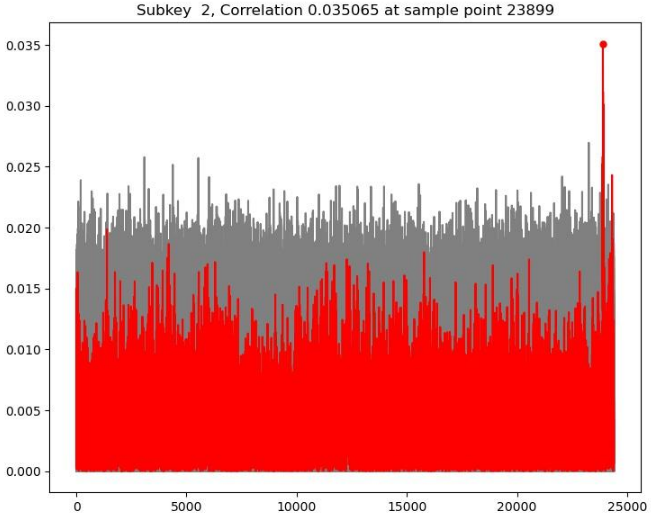
73200-97600 samples

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15


SWAES PICO CW Power Traces Plot 73200-97600

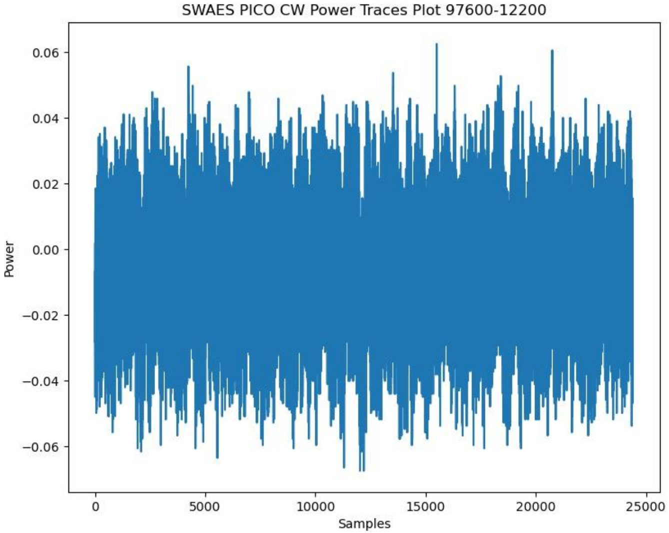

Subkey 9, Correlation 0.040191 at sample point 4935

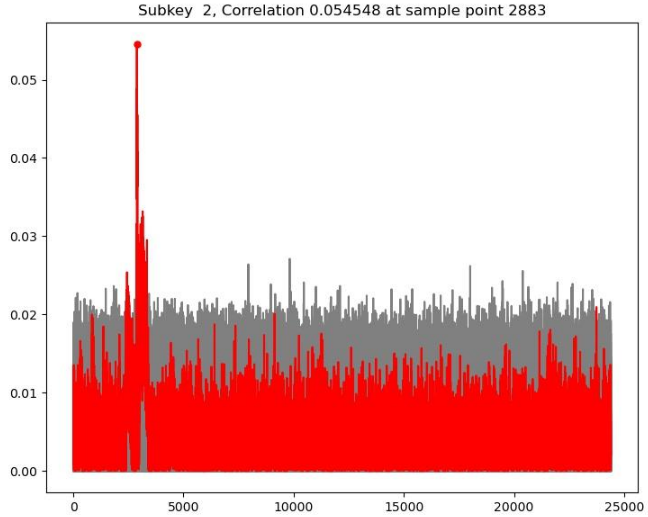

Subkey 13, Correlation 0.056693 at sample point 14527

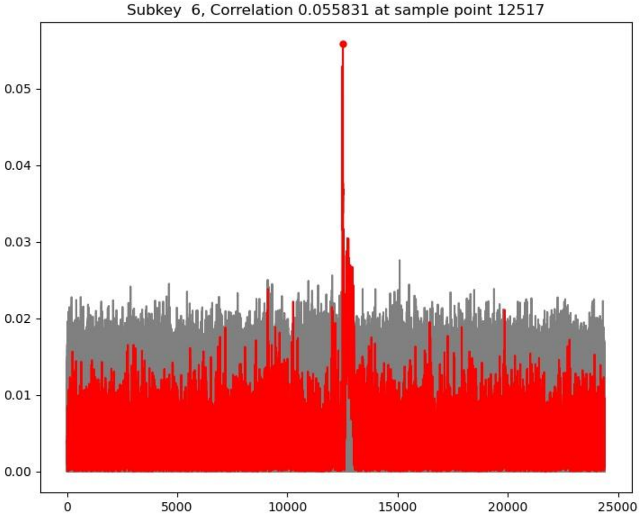

Subkey 2, Correlation 0.035065 at sample point 23899

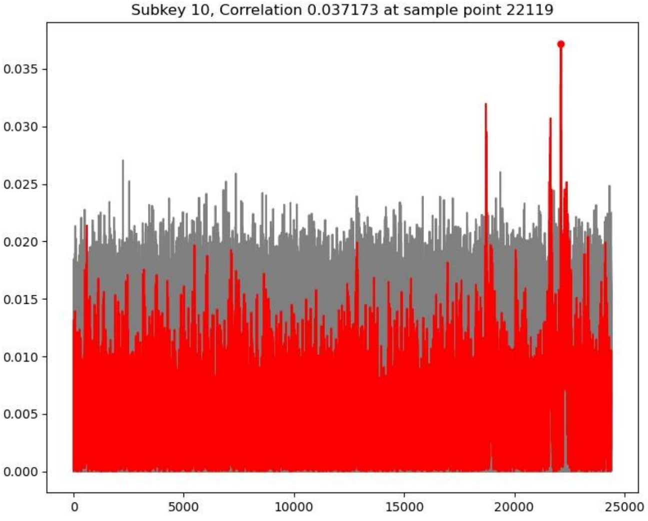
97600-12200 samples

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15



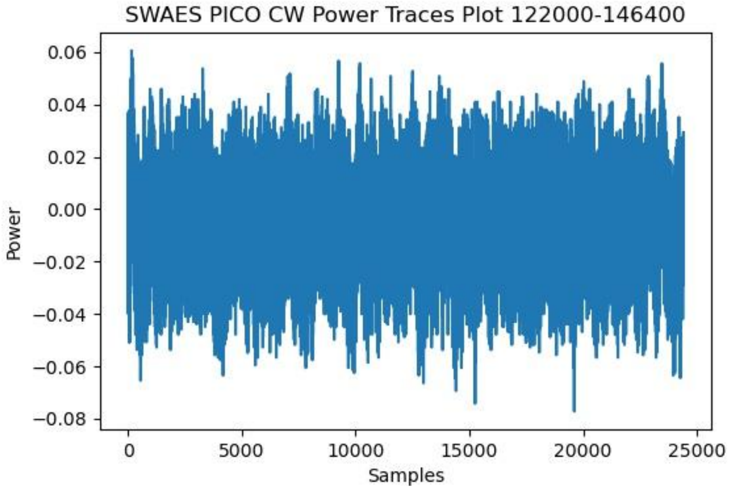




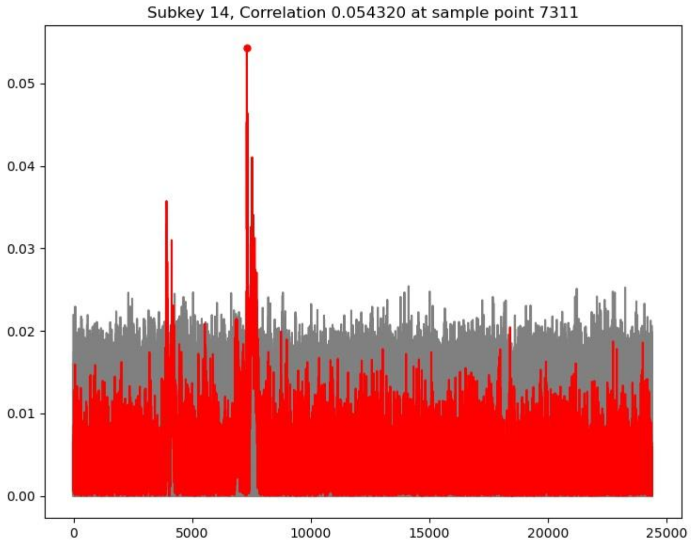


12200-146400 samples

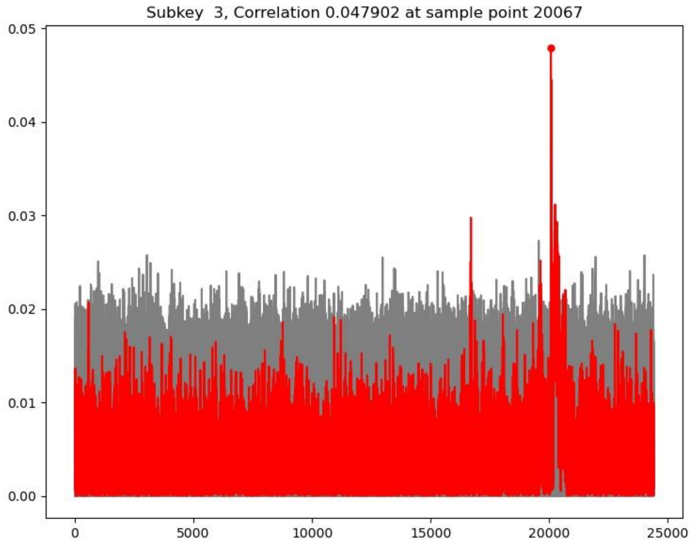
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15



SWAES PICO CW Power Traces Plot 122000-146400



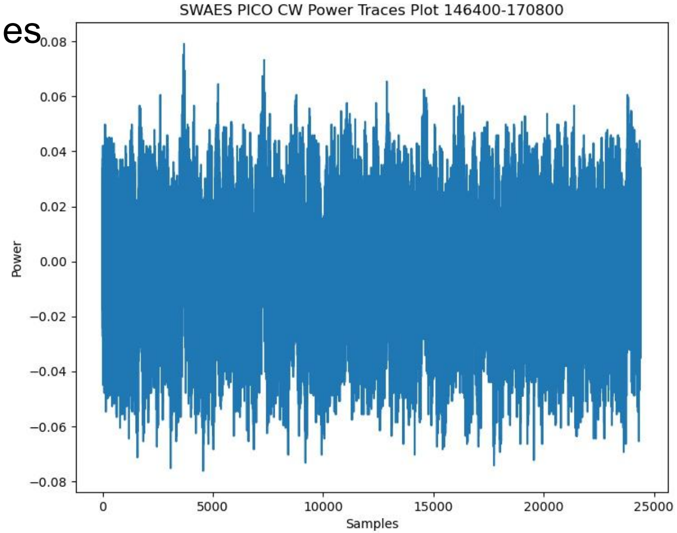
Subkey 14, Correlation 0.054320 at sample point 7311

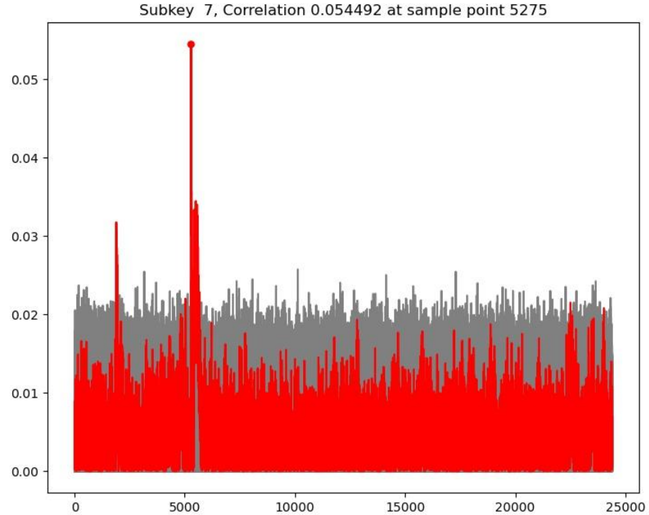


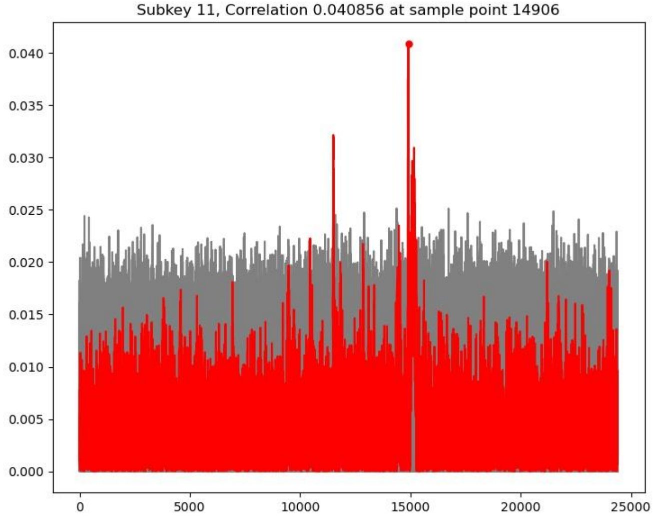
Subkey 3, Correlation 0.047902 at sample point 20067

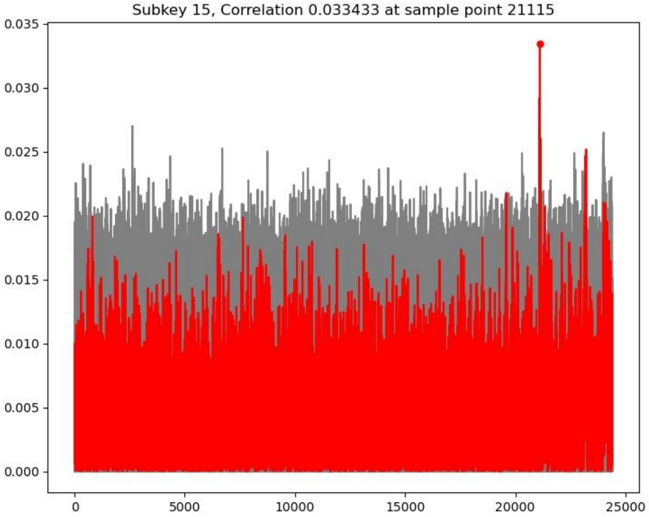
146400-170800 samples
Byte 3, 7

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15


SWAES PICO CW Power Traces Plot 146400-170800


Subkey 7, Correlation 0.054492 at sample point 5275


Subkey 11, Correlation 0.040856 at sample point 14906


Subkey 15, Correlation 0.033433 at sample point 21115