Avoiding Falsely Passing a Device in TVLA Testing

Gilbert Goodwill
Senior Manager, DPA

2017-05-19

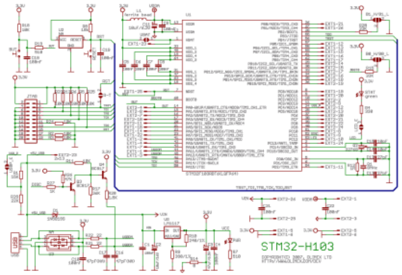
TVLA Background

- Test Vector Leakage Assessment (TVLA)
  - Conformance testing methodology for side-channel resistance
- Uses known key and data to predict sensitive intermediates
  - Instead of attempting various attacks against an unknown key
- Bounded data collection and analysis time
- Evaluate leakage using Welch's t-Test
  - Allows setting of confidence interval, e.g., 99.999%
- Includes specific and non-specific tests
  - Specific tests map directly to attacks
  - Non-specific tests amplify leaks, accelerating testing

Signal Finding

- TVLA requires signal finding, which may be a new evaluation skill

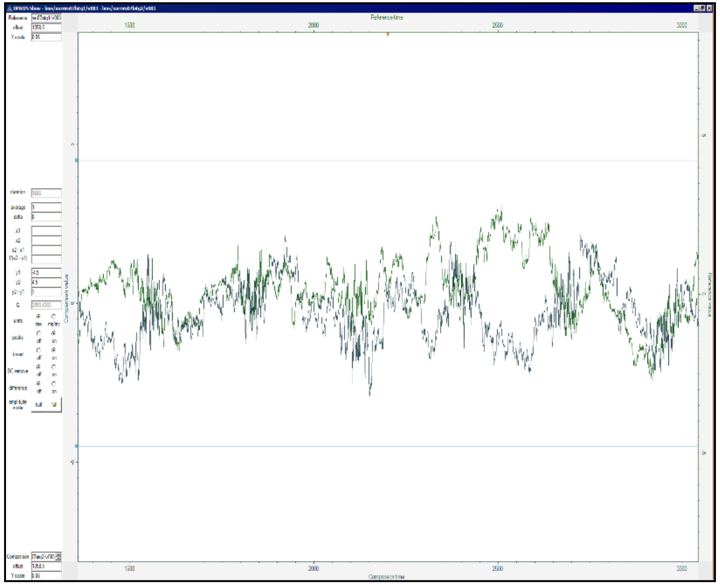
- To facilitate evaluation, vendors should provide
  - Schematics
  - Taps
  - Trigger signals



- Signal finding may use
  - Power taps or EM probes
  - Tuner (analog or digital)
  - Demodulation
  - Filtering

Absence of Signal is Not Absence of Leakage

- An individual t-Test may show no leakage
  - No indication of statistically significant difference between partitions of collected data



- On its own this does not necessarily mean there is no leakage
  - Even for sensitive non-specific (“fixed-vs.-random”) tests

- Test setup must be confirmed to be capable of recording leakage

Common Sources of Error: Equipment Setup

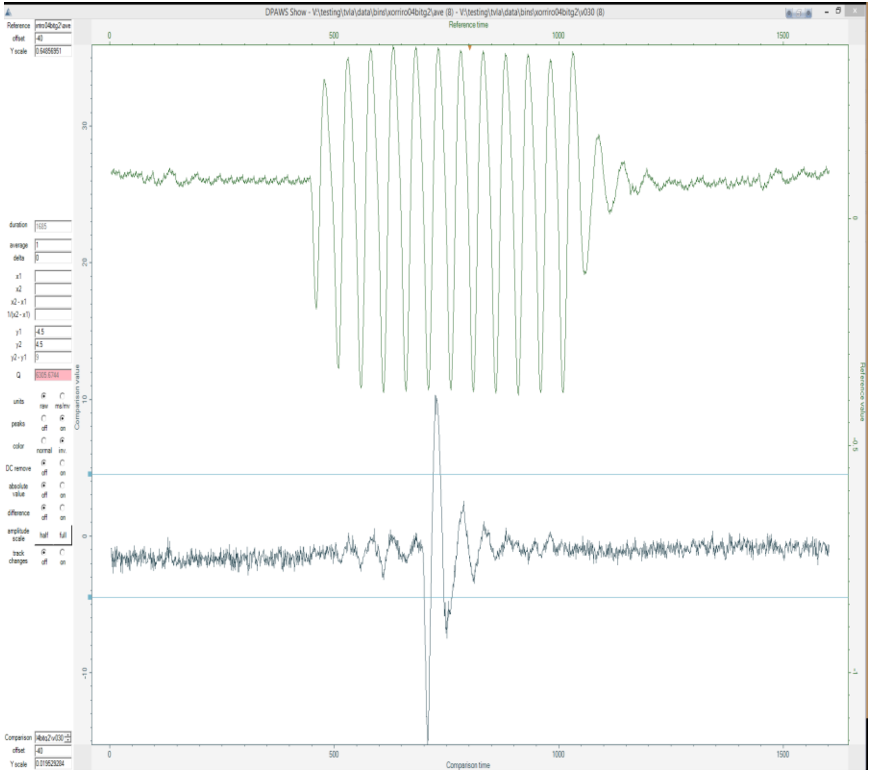
- Disconnected wires
- Amplifiers not turned on
- Probe position moved
- Insufficient data collection parameters
  - Sample rate
  - Bandwidth
  - Tuning
  - Filtering
- …

Common Sources of Error: Post-Processing

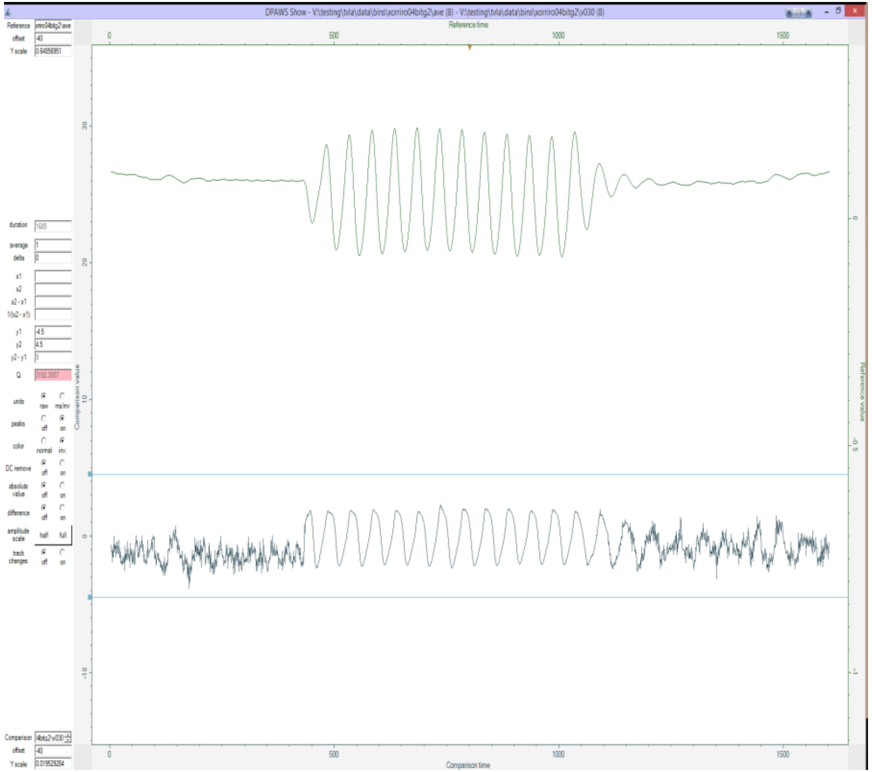
- Location of operations in time is not correct
    - Too much jitter in operation location in trace
    - Bulk mode (multiple operations per scope trace) issues:
        - Incorrect length of operation
        - Incorrect number of operations per trace

- Incorrect associating of data being processed and traces, “off-by-one”
    - Individual operations located correctly
    - Incorrect data used for making predictions
    - Leakage will grow up until an extra or missing operation

Incorrectly Handled Operation Jitter

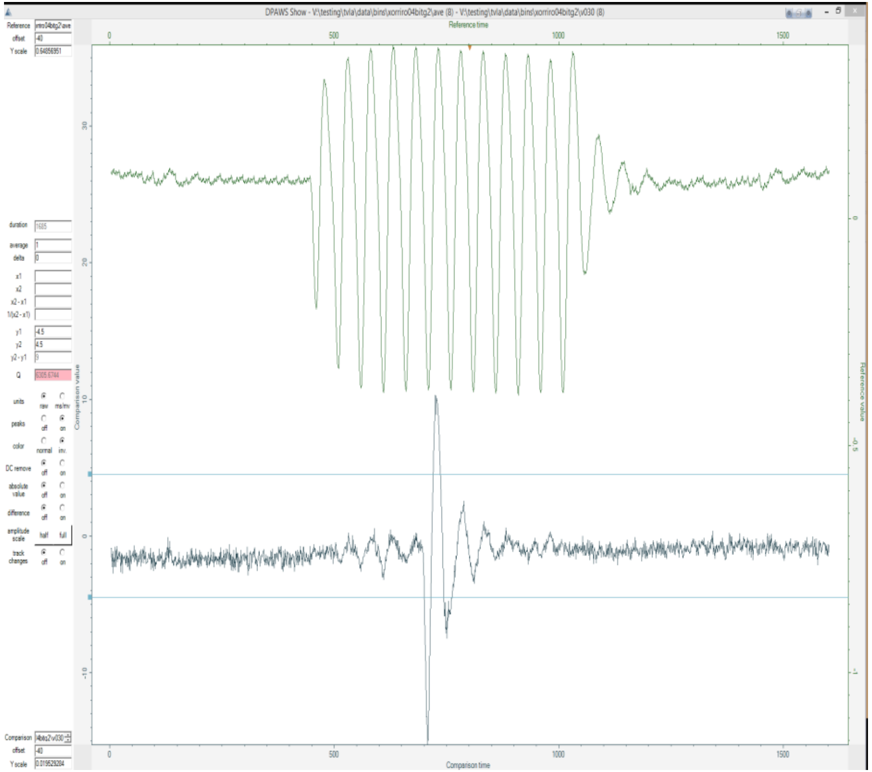

DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

Reference: ırriro04bitg2\ave
offset: -40
Y scale: 0.64856951
duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 6305.6744
units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on
Comparison: l4bitg2\v030
offset: -40
Y scale: 0.019529284


DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

Reference: ırriro04bitg2\ave
offset: -40
Y scale: 0.64856951
duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 3192.3007
units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on
Comparison: l4bitg2\v030
offset: -40
Y scale: 0.019529284

Incorrectly Specified Operation Length



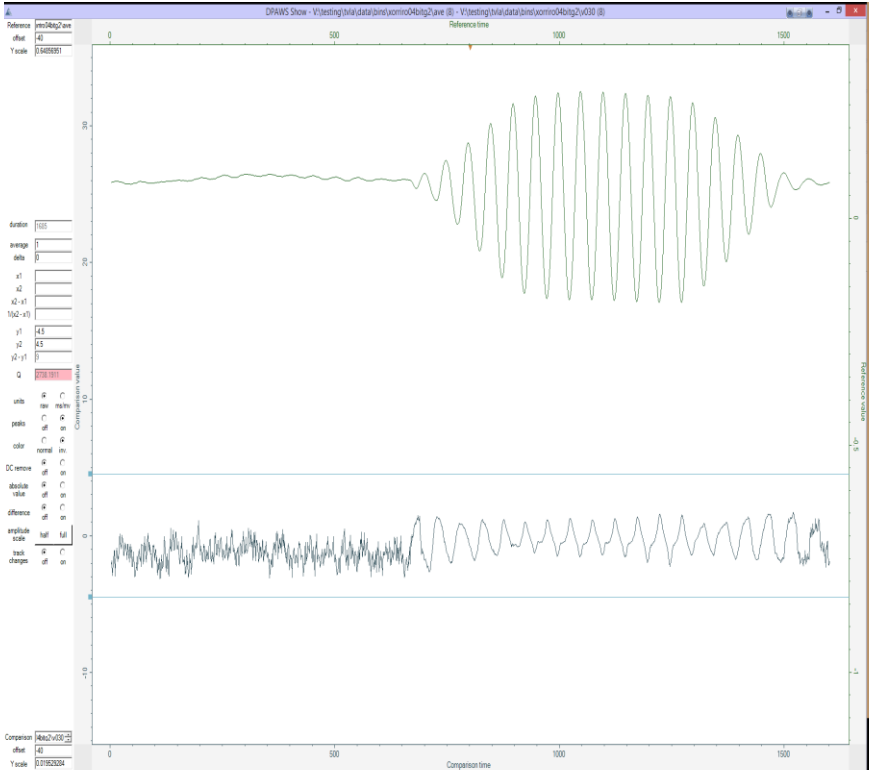
DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

Reference: xriro04bitg2\ave
offset: -40
Y scale: 0.64856951

duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 6305.6744

units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on

Comparison: 4bitg2\v030
offset: -40
Y scale: 0.019529284



DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

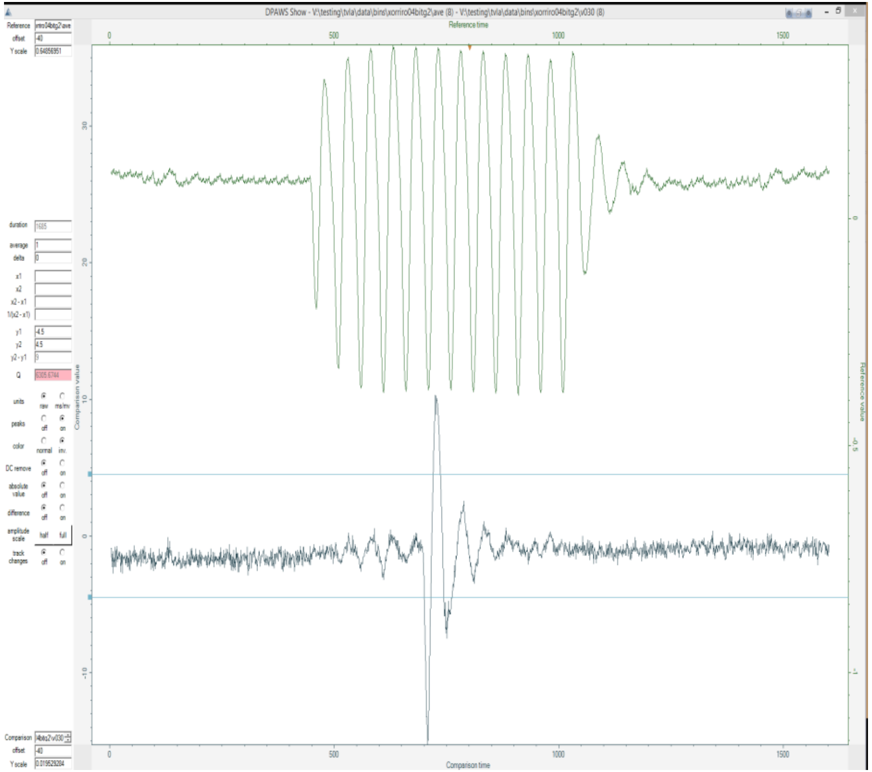
Reference: xriro04bitg2\ave
offset: -40
Y scale: 0.64856951

duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 2738.1911

units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on

Comparison: 4bitg2\v030
offset: -40
Y scale: 0.019529284

“Off-by-One”



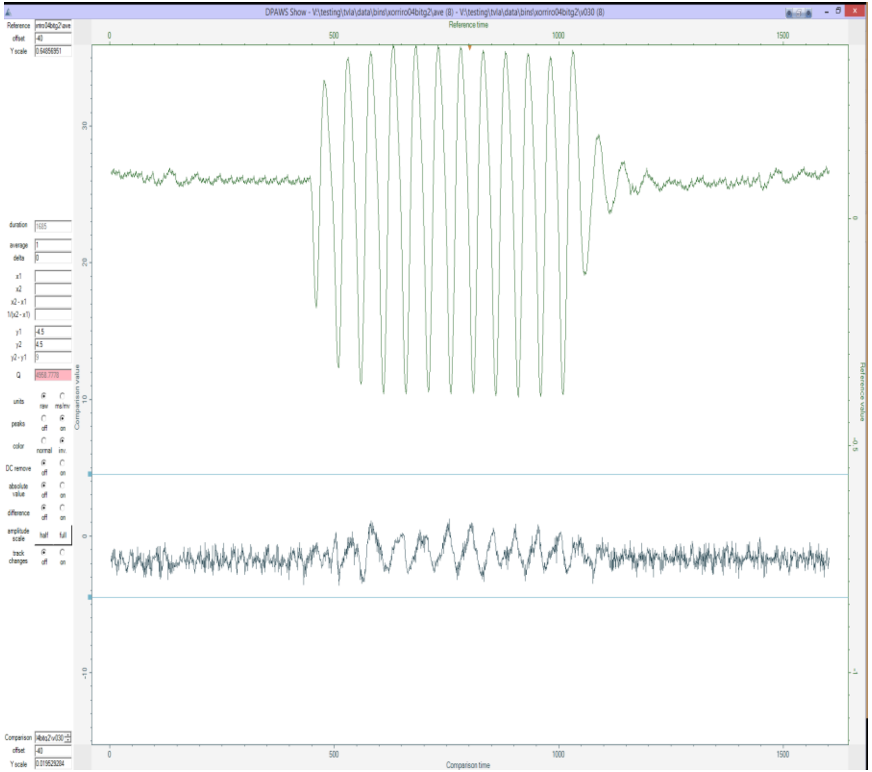
DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

Reference: rriro04bitg2\ave
offset: -40
Y scale: 0.64856951

duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 6305.6744

units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on

Comparison:)4bitg2\v030
offset: -40
Y scale: 0.019529284



DPAWS Show - V:\testing\tvla\data\bins\xorriro04bitg2\ave (8) - V:\testing\tvla\data\bins\xorriro04bitg2\v030 (8)

Reference: rriro04bitg2\ave
offset: -40
Y scale: 0.64856951

duration: 1685
average: 1
delta: 0
x1:
x2:
x2 - x1:
1/(x2 - x1):
y1: -4.5
y2: 4.5
y2 - y1: 9
Q: 4958.7778

units: ● raw ○ ms/mv
peaks: ○ off ● on
color: ○ normal ● inv.
DC remove: ● off ○ on
absolute value: ● off ○ on
difference: ● off ○ on
amplitude scale: half full
track changes: ● off ○ on

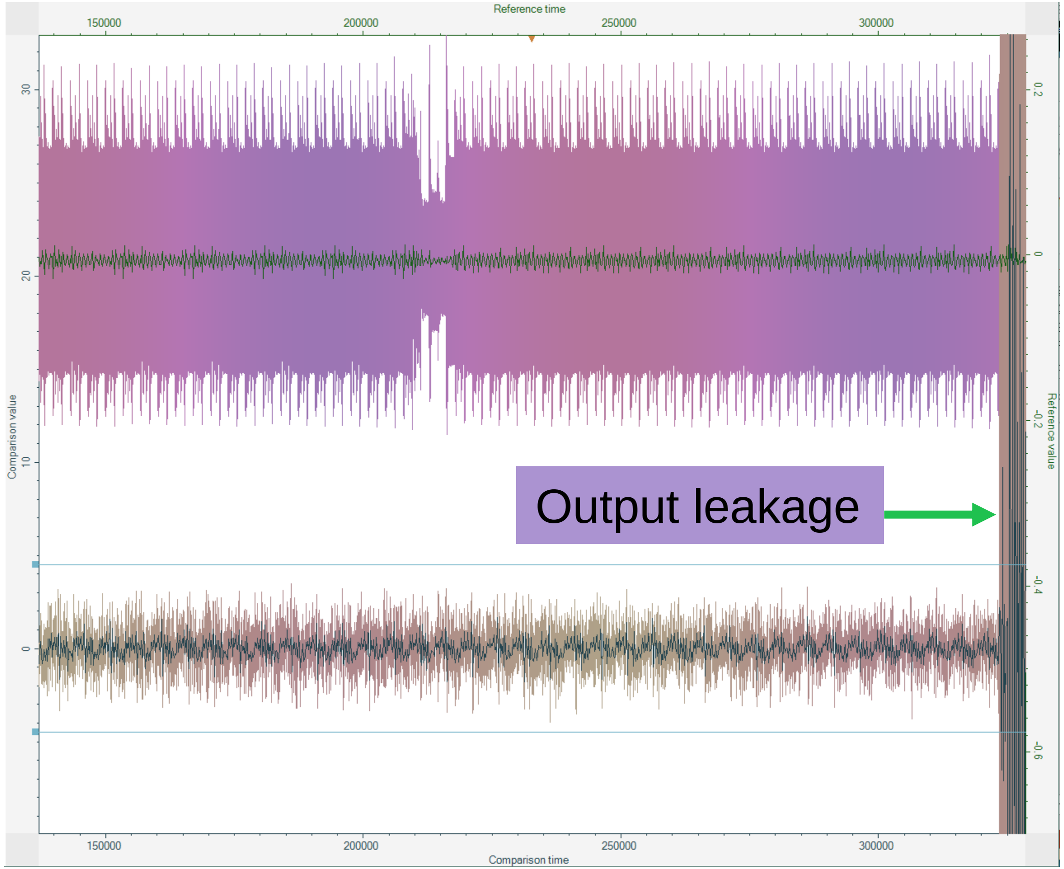
Comparison:)4bitg2\v030
offset: -40
Y scale: 0.019529284

Signal calibration using known leakage

- Calibration signal needed to confirm setup is capable of showing leakage

- Input or output leakage *at the cryptographic processing* provides this
  - I/O leakage on its own is not enough, need to see input/output from crypto.
  - Temporal ranges must match beginning/end of cryptographic operation
  - Cipher text is generally unprotected and leaks a lot

Output leakage as calibration



Output leakage

Calibration signals, beyond simple I/O

- If inputs or outputs provided masked, may need access to the shares

- Compare results to those when disabling
  - Random number generator so masks are fixed
  - Countermeasures

Summary

- TVLA results must confirm setup is capable of detecting leakage
  - Signal finding has been successful
  - Test setup is functioning
  - Post-processing has correctly identified operations

- Beware of TVLA results without corresponding calibration
  - Must show leakage from same setup for an unprotected quantity